Pre IMO 2013 TdN - Pomeriggio

Titolo nota 29/05/2013

N7 Trovare tutte le coppie di interi coprimi a, b tali che esistono finiti interi n t.c.

$$n^2 \mid a^n + b^n$$

R: $a+b = 2^k$, $\{a, b\} = \{1, 2\}$.

Dim. [$a+b = 2^k$ allora $\nexists$ n t.c.]

Step 1 $(a, n) = (b, n) = 1$ $\quad p \mid a \quad p \mid n \Rightarrow p \mid b$

Step 2 n è per forza dispari. Altrimenti ($n = 2k$)

$$4 \mid n^2 \mid a^{2k} + b^{2k}$$

$$4 \mid (a^k)^2 + (b^k)^2$$

a, b dispari, ma allora $(a^k)^2 + (b^k)^2 \equiv 2 \pmod 4$ assurdo.

Step 3 $a+b = 2^k$ $\quad n \neq 1$ ma allora $\exists$ p.p.p. che divide n $\quad p$

$$p^2 \mid a^n + b^n$$

$$a^n \equiv -b^n \pmod p \rightsquigarrow \left(\frac{a}{b}\right)^{2n} \equiv (-1)^2 \pmod p$$

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

$ord_p\left(\frac{a}{b}\right) \mid (2n, p-1) = 2$

$a^n \equiv b^n \ (p) \rightsquigarrow 2a^n \equiv 0 \ (p)$ $\qquad p=2$ no!

$\frac{a}{b} \equiv -1 \ (p)$ $\qquad a+b \equiv 0 \ (p)$ $\qquad p \mid a+b = 2^k$

$\lightning$

$a=2, b=1$

$n^2 \mid 2^n + 1^n$ $\qquad p$ è p.p.p. di n

$\Rightarrow \quad p \mid 2+1=3 \qquad p=3$

$n = 3k$

$9k^2 \mid 8^k + 1^k \Rightarrow k^2 \mid 8^k + 1^k$

$\Downarrow \ k \neq 1$

l.p.p. $\mid 8+1 = 9$

$3 \mid k$

$v_3(9k^2) \leq v_3(8^k + 1^k)$

$\| \qquad\qquad \|$

$2 + 2v_3(k) \qquad v_3(8+1) + v_3(k) =$

$= 2 + v_3(k)$

$2 + 2v_3(k) \leq 2 + v_3(k) \Rightarrow v_3(k) \leq 0$

$a=1 \quad b=2 \rightsquigarrow \quad n=1$

$n=3$.

Lemma (LTE-w) $p \mid a+b \qquad (p,a)=1 \qquad (p,b)=1$

$$p \mid \frac{a^p+b^p}{a+b} \qquad \text{ma} \qquad p^2 \nmid \frac{a^p+b^p}{a+b}$$

Cor. (LTE) $p \mid a-b \qquad (p,a)=1 \qquad (p,b)=1$

$$v_p\left(a^n-b^n\right) = v_p(a-b) + v_p(n).$$

2ª prova

CLAIM. $\exists \{p_1, p_2, \dots, p_k\}$ primi dispari distinti t.c.

$$(p_1 p_2 \cdots p_k)^2 \mid a^{p_1 p_2 \cdots p_k} + b^{p_1 p_2 \cdots p_k} \quad (= n_k)$$

$k=1$ $\quad p_1^2 \mid a^{p_1}+b^{p_1}$ come lo trovo

$a+b \neq 2^k \qquad p_1 \mid a+b \quad \Rightarrow \quad p_1^2 \mid a^{p_1}+b^{p_1}$.

$k \Rightarrow k+1$

$$n_k^2 \mid a^{n_k}+b^{n_k}$$

$$n_{k-1}^2 p_k^2 \mid a^{n_{k-1} p_k} + b^{n_{k-1} p_k}$$

$$p_k \mid a^{n_{k-1}} + b^{n_{k-1}}$$

$$\left(\frac{\left(a^{n_{k-1}}\right)^{p_k} + \left(b^{n_{k-1}}\right)^{p_k}}{a^{n_{k-1}} + b^{n_{k-1}}}, \; a^{n_{k-1}} + b^{n_{k-1}} \right) = p_k$$

$$p_k^2 \nmid A_k \qquad \left(\frac{A_k}{p_k}, n_k\right) = 1$$

$$p_k \mid A_n$$

$$\frac{A_k}{p_k} > 1 \qquad A_k \text{ disp.} \Rightarrow \exists\, p_{k+1} \notin \{p_1, \dots, p_k\}$$

$$p_{k+1} \mid A_n .$$

$$\frac{A^{p_k} + B^{p_k}}{A + B} > p_k$$

$$\left(A^{p_k} + B^{p_k}\right) > p_k (A + B) \qquad \max\{|A|, |B|\} \geq 3$$

$$A > B \qquad A > 0$$

$$\left(A^{p_k - 1} - B A^{p_k - 2} + \dots + B^{p_k - 1}\right) > p_k$$

$$\left(A^{p_k - 2}(A - B) + \cancel{A^{p_k - 1} B^2 (A - B)} - \cancel{+} + B^{p_k - 1}\right) \geq$$

$$\geq \left(A^{p_k - 2} + B^{p_k - 1}\right) > 3^{p_k - 2} = (1 + 2)^{p_k - 2} \geq 1 + 2p_k - 4 =$$

$$= p_k + (p_k - 3) \geq p_k .$$

Esercizio 5

$$\frac{m+n}{3} - \frac{3mn}{m+n} = \frac{2011}{3}$$

$$3(m+n)^2 - 9mn = 2011\,(m+n)$$

$d = (m,n)$ $\quad m = ad \quad n = bd$

$$3d\,(a^2 - ab + b^2) = 2011\,(a+b)$$

$3 \mid a+b \;\to\; 9 \mid a+b$

$$d = k\,\frac{a+b}{9}$$

$$k\,(a^2 - ab + b^2) = 3 \cdot 2011$$

$a^2 - ab + b^2 = \cancel{3}, \boxed{3 \cdot 2011}$ $\qquad a^2 - ab + b^2 \geq ab$

$k = 1 \qquad 9d = a+b$

Poss. supporre $a \leq b$ $\qquad a^2 - ab + b^2 \leq b^2$ $\qquad \boxed{b \geq 78}$

$a + b \geq 81 \qquad d \geq 9$

$b = 9d - a$

$*$ $\quad a^2 - 9ad + 27d^2 - 2011 = 0$

$$\Delta = 8044 - 27d^2 \qquad (\Delta \geq 0)$$

$$d \leq 17$$

Considerando mod p $\quad p = 5, 7$

restano solo i casi $\quad d = 7, 8, 13.$ $\qquad (d \geq 9)$

$d = 13 \qquad m = 377 \qquad n = 1144.$

Esercizio 6

$$1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv p + (p-1)! \pmod{p^2}$$

p primo dispari

$$i^{p-1} \equiv 1 \pmod{p} \qquad 1 \leq i \leq p-1.$$

$$a_i = i^{p-1} - 1 \equiv 0 \pmod{p}$$

$$(p-1)!^{p-1} - 1 = \prod_{i=1}^{p-1} i^{p-1} - 1 = \prod_{i=1}^{p-1} (1 + a_i) - 1$$

$$= \cancel{1} + \sum_{i=1}^{p-1} a_i + \sum_{i<j} a_i a_j + \dots \qquad \cancel{-1}$$

$$\equiv \sum_{i=1}^{p-1} a_i \pmod{p^2}$$

$$\text{LHS} = p-1 + \sum_{i=1}^{p-1} a_i \equiv (p-1)!^{p-1} + p - 2 \pmod{p^2}$$

$$\overset{?}{\equiv} p + (p-1)! \pmod{p^2}$$

Mi serve $(p-1)!^{p-1} \equiv (p-1)! + 2 \pmod{p^2}$

Wilson: $(p-1)! \equiv -1 \pmod{p}$

$$(p-1)! = -1 + kp$$

$$(p-1)!^{p-1} \equiv 1 - (p-1)kp \equiv 1 + kp \equiv 2 + (-1+kp) \pmod{p^2}$$

$$\rho(x) = \overline{(x-1)}\,\overline{(x-2)} \cdot \dots \cdot \overline{(x-(p-1))} =$$

$$= x^{p-1} + c_{p-2} x^{p-2} + \dots + c_1 \cdot x + (p-1)!$$

$$c_k = (-1)^k \cdot \sigma_k^{p-1}(1, 2, 3, \dots, p-1)$$

$$\sigma_k^{p-1}(x_1, \dots, x_{p-1}) = \sum_{i_1 < i_2 < \dots < i_k} \prod_{j=1}^{k} x_{i_j}$$

$$\sigma_k^{p-1}(1, \dots p-1) \begin{cases} 0 \pmod{p} & \text{per } 1 \le k \le p-2 \\ -1 \pmod{p} & \text{per } k = p-1 \end{cases}$$

$$0 = \sum_{n=1}^{p-1} \rho(n) = \sum_{n=1}^{p-1} n^{p-1} + \underbrace{c_{p-2} \sum_{n=1}^{p-1} n^{p-2} + \dots +}_{\text{multipli di } p^2} \sum_{n=1}^{p-1} (p-1)!$$

$$\sum_{n=1}^{p-1} n^k \equiv 0 \pmod p \quad \text{per } 1 \le k \le p-2$$

$$0 \equiv \sum_{n=1}^{p-1} n^{p-1} + (p-1)\cdot(p-1)! \equiv \underbrace{p\cdot(p-1)!}_{p(p-1)} - (p-1)! + \sum \equiv$$

$$\equiv -p - (p-1)! + \sum \pmod{p^2}$$

Esercizio 8 $\quad \phi(5^m-1) = 5^n-1 \quad \Rightarrow \quad (m,n) > 1.$

Sol (per assurdo): supponiamo $(m,n)=1$.

$$(5^m-1, 5^n-1) = 5^{(m,n)} - 1 = 5-1 = 4$$
$$(x^m-1, x^n-1) = x^d - 1 \qquad d=(m,n)$$

Divisori primi di 5^m-1.

$p^2 \mid 5^m-1 \qquad p \mid \phi(5^m-1) = 5^n-1 \qquad p \mid 4 \qquad p=2$

$$5^m-1 = 2^\alpha p_2 \cdots p_k \qquad \alpha \ge 2$$

Se fosse $5^m-1 = 2^\alpha \qquad \phi(5^m-1) = \frac{5^m-1}{2}$

$(5^n-1, 5^m-1) = 5^n-1 \mid 4 \qquad n \le 1.$

Allora c'è un $p_i \neq 2$ $\rightarrow$ nella ϕ c'è $p_i - 1$

Quindi $2^\alpha \mid 5^n-1 \rightarrow \alpha \le 2$ $\qquad \boxed{\alpha = 2}$

Ricapitolando $\quad 5^m-1 = 4\cdot p_2 \cdots p_k$

$$5^n-1 = 2\,(p_2-1)\cdots(p_k-1)$$

Oss. m deve essere DISPARI (se pari $5^m \equiv 1 \pmod 8$)

$$5^{m+1} \equiv 5 \pmod{p_i}$$

esponente pari

5 è un quadrato mod p_i $\qquad \left(\frac{5}{p_i}\right) = +1$

$RQ \Rightarrow \left(\frac{p_i}{5}\right) = +1 \qquad p_i \equiv \cancel{1}, 4 \pmod 5$

Se fosse $p_i \equiv 1 \pmod 5$ $\quad 5 \mid p_i - 1 \mid \phi(5^n - 1) = 5^n - 1$

NO

Quindi $p_2, \dots, p_k$ sono tutti $\equiv 4 \equiv -1 \pmod 5$

$$-1 \equiv 5^n - 1 = 4 p_2 \cdots p_k \equiv (-1)^k \pmod 5$$

k dispari.

$$5^n - 1 = 2 (p_2 - 1) \cdots (p_k - 1) \equiv 2 \cdot 3^{k-1} \pmod 5$$

$k - 1 = 2t \qquad 3^2 \equiv -1 \pmod 5$

$$-1 \equiv 5^n - 1 \equiv 2 (-1)^t \pmod 5$$

ASSURDO