WC 13 - TdN

Titolo nota 30/01/2013

Problema 4.

$$\frac{a^2+b^2+c^2}{3(ab+bc+ca)} \notin \mathbb{Z}$$

Se questo fosse un intero, si avrebbe

$$a^2+b^2+c^2 = 3k(ab+bc+ca) \qquad k \in \mathbb{Z}$$

$$a^2+b^2+c^2+2ab+2bc+2ca = (a+b+c)^2$$
$$= (3k+2)(ab+bc+ca).$$

$$p \mid 3k+2 \qquad 2^n \equiv (-1)^n \pmod 3$$

Esiste un primo congruo a 2 modulo 3 che divide $3k+2$ con un esponente dispari

$$p \mid 3k+2 \qquad p \mid ab+bc+ca \qquad p \mid a+b+c$$

$$a+b+c \equiv 0 \pmod p$$
$$c \equiv -(a+b) \pmod p$$

$$ab+bc+ca \equiv 0 \pmod p$$
$$ab+b(-a-b)+(-a-b)a \equiv 0 \pmod p$$
$$-(a^2+ab+b^2) \equiv 0 \pmod p.$$

Posso supporre a, b, c primi fra loro.
a, b primi fra loro.

In particolare $p \nmid a$ $p \nmid b$

$x = a/b$ $\qquad x^2 + x + 1 \equiv 0 \pmod p$.

$\boxed{p \neq 2}$ $\qquad x = -\frac{1 \pm \sqrt{1-4}}{2} = \frac{-1 \pm \sqrt{-3}}{2}$.

-3 è un quadrato modulo p?

$\left(\frac{-3}{p}\right) = \pm 1$

p, q

$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ se almeno uno dei due è $\equiv 1 \mod 4$.

$\left(\frac{-3}{p}\right) = \left(\frac{p}{-3}\right)$ $\qquad p \equiv 1 \pmod 3$.

$\left(\frac{a}{p}\right) = \pm 1$?

$x \to ax$ $\qquad (a, p) = 1$.

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$x \to -3x$ $\qquad (x \to 3x)$

$p = 3k+1$

3	6	9.	$3k$
2	5	8	$3k-1$
1	4	7	$3k-2$

Es n. 5

$p \equiv 3 \pmod 4$

$$\prod_{1 \le x < y \le \frac{p-1}{2}} (x^2+y^2)$$

$\underline{x^2+y^2}$

-1 non è un quadrato.

a quadrato $\Leftrightarrow$
$-a$ non è un quadrato.

$x^2+y^2=t^2 \quad \Leftrightarrow \quad x^2+y^2=1$

$x=tx' \quad y=ty'$

$(tx')^2+(ty')^2=t^2$

$x'^2+y'^2=1$

$x^2+y^2=-t^2 \quad \Leftrightarrow \quad x^2+y^2=-1.$

$x^2+y^2=1 \qquad y^2=1-x^2$

$$\sum_{x=1}^{p} \left(\frac{1-x^2}{p}\right) = ?$$

$\left(\frac{a}{p}\right)=1 \quad \Leftrightarrow \quad a^{(p-1)/2} \equiv 1 \pmod p$

$$\sum_{x=1}^{p} \left(\frac{1-x^2}{p}\right) \equiv \sum_{x=1}^{p} (1-x^2)^{(p-1)/2} \pmod p$$

$$\equiv \sum_{x=1}^{p} 1 - \sum_{x=1}^{p} \left(\frac{p-1}{2}\right) x^2 + \dots + - \sum_{x=1}^{p} x^{p-1}$$

$$\equiv p \quad \pm 0 \cdots \pm 0 \qquad - (p-1)$$
$$\equiv 1 \pmod p \qquad = 1$$

$x \not\equiv 0$, $x \not\equiv 1$, $x \not\equiv -1$ $\qquad p-3$ valori

$\frac{p-3}{2}$ danno quadrati, $\frac{p-7}{2}$ non danno quadrati.

Nella mia limitazione $\left(1 \leq x < y \leq \frac{p-1}{2}\right)$

$\frac{p-3}{4}$ danno quadrati, $\frac{p-7}{4}$ non danno quadrati.

Le coppie $(x<y)$ sono $\frac{p-3}{8}$.

a meno che non si possa risolvere

$$x^2+x^2 \equiv 1 \pmod p$$
$$2x^2 \equiv 1 \pmod p$$

$$\frac{p-3}{8} = \left(\frac{p-3}{4}\right) \Big/ 2$$

In questo caso ho $\left(\frac{p-3}{4} - 1\right) \Big/ 2 = p-7/8$

In un caso viene la formula

$$\prod_{1 \leq x < y \leq \frac{p-1}{2}} (x^2+y^2) \equiv \prod_{t=1}^{(p-1)/2} (-t^2)^{p+1/8} (t^2)^{p-7/8} =$$

$$= (-1)^{p+1/8} \prod_{t=1}^{(p-1)/2} (t^2)^{(p-3)/4}$$