TEORIA DEI NUMERI 3 MEDIUM

Titolo nota 09/09/2019

VARI PROBLEMI

- $\dfrac{a^2+b^2}{1+ab} = k$ intero $\Rightarrow$ k è un $\square$ (IMO 88/6)
  a, b interi >0
- $\dfrac{a^2+b^2+1}{ab} = k \in \mathbb{Z} \Rightarrow k=3$ $(a,b>0)$
- $a^m b^n = (a+b)^2+1$ con $m, n, a, b > 0$
- Trova min n per cui esistono infiniti razionali $a_1, \dots, a_n$ con
  $a_1 + \dots + a_n$ intero, $\dfrac{1}{a_1} + \dots + \dfrac{1}{a_n}$ intero

Reciprocità quadratica

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & a \text{ quadrato mod } p \\ -1 & a \text{ non è quadrato mod } p \\ 0 & p \mid a \end{cases}$$

Teo Siano p, q primi dispari, $p \neq q$. Allora

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Ovvero • Se almeno uno fra p e q è $\equiv 1 \ (4)$,

allora $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$

• Se $p \equiv q \equiv 3 \ (4)$ $\qquad \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

Oss Funziona anche con p, q primi negativi,

ad esempio $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$, e quindi

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & \text{se } p \equiv 1 \ (3) \\ -1, & \text{se } p \equiv 2 \ (3) \end{cases}$$

$$\left(\frac{1002}{13}\right) = \left(\frac{2 \cdot 501}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{501}{13}\right)$$

$$= \left(\frac{2}{13}\right) \cdot \left(\frac{167}{13}\right) \cdot \left(\frac{3}{13}\right)$$

$$\left(\frac{2}{13}\right) \cdot \left(\frac{-2}{13}\right) \cdot \left(\frac{13}{3}\right)$$

$$= \left(\frac{-1}{13}\right)\cdot\left(\frac{2}{13}\right)^2\cdot\left(\frac{1}{3}\right) = +1$$

Lemma

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv \pm 1\ (8) \\ -1, & p \equiv \pm 3\ (8) \end{cases}$$

Dim elementare

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \quad (p)$$

$$1 = (-1)(-1)$$

$$2 = 2\cdot(-1)^2$$

$$3 = (-3)(-1)^3$$

$$\vdots$$

$$\frac{p-1}{2} = \pm\left(\frac{p-1}{2}\right)(-1)^{\frac{p-1}{2}}$$

moltiplico tutto $\quad 1+2+\dots+\frac{p-1}{2}$

$$\left(\frac{p-1}{2}\right)! \equiv 2\cdot 4\cdot\dots\cdot(p-1)\cdot(-1)^{\left(\frac{p-1}{2}\cdot\frac{p+1}{2}\right)\cdot\frac{1}{2}} \pmod p$$

$$\equiv 2^{\frac{p-1}{2}}\cdot\left(\frac{p-1}{2}\right)!\ (-1)^{\frac{p^2-1}{8}} \mod p$$

$$\Rightarrow\ 2^{\frac{p-1}{2}}\cdot(-1)^{\frac{p^2-1}{8}} \equiv 1\ (p)$$

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}}\ (p) \quad\Rightarrow\quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \qquad \square$$

Dim meno elementare $\quad 2^{\frac{p-1}{2}}$, ma

$2 = -(1+i)^2\, i$, e quindi

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-i)^{\frac{p-1}{2}}\cdot(1+i)^{p-1} \quad (p)$$

$$\equiv (-i)^{\frac{p-1}{2}}\ \frac{(1+i)^p}{1+i} \quad (p)$$

$$\equiv (-i)^{\frac{p-1}{2}} \frac{1+i^p}{1+i} \mod p$$

Basta controllare i casi per $p \mod 8$ $\square$

Oss $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 (4) \\ -1, & p \equiv 3 (4) \end{cases}$

Dimostriamo un altro caso speciale

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

Supponiamo che $\left(\frac{-3}{p}\right) = 1$. Allora la quantità

$$\zeta_3 = \frac{-1+\sqrt{-3}}{2}$$ ha senso modulo p

fissiamo $a \in \mathbb{Z}$ t.c. $a^2 \equiv -3 (p)$ e definiamo $\zeta_3 := 2^{-1} \cdot (-1+a)$

$$\zeta_3^2 + \zeta_3 + 1 \equiv 0 \quad (p)$$

$\Rightarrow$ l'equazione $X^2+X+1 \equiv 0 \ (p)$ ha 2 sol. mod p

$\Rightarrow$ ——— $X^3 - 1 \equiv 0 \ (p)$ ha 3 ———

$\Rightarrow$ $p \equiv 1 \ (3)$ $\qquad \text{ord}_p(\zeta_3) = 3 \mid p-1$

[Il n° di soluz di $x^k \equiv 1 \ (p)$ è $(p-1, k)$]

Viceversa: $p \equiv 1 \ (3) \Rightarrow X^3 \equiv 1 \ (p)$ ha 3 soluz.

$\rightarrow g^0, g^{\frac{p-1}{3}}, g^{\frac{p-1}{3}\cdot 2}$

dove g = gen. mod p

$\Leftrightarrow$ $(x-1)(x^2+x+1) \equiv 0 \ (p)$ ha 3 soluz. mod p

$\Leftrightarrow$ $x = \dfrac{-1 \pm \sqrt{-3}}{2}$ esistono mod p, cioè

$-3 = \square$ mod p

$\ulcorner$ Sia b una soluz. di $x^2+x+1 \equiv 0 \ (p)$

Sia $a = 2b+1$. Allora $a^2 \equiv 4b^2+4b+1$

$\equiv 4(-b-1)+4b+1 \equiv -3 \ (p)$ $\lrcorner$

Esempio

(RMM 2013) $p_1 = 2^{\overset{q_1}{a}}-1$, $\underset{p_2}{\underset{\shortparallel}{2^{\overset{q_2}{2a+1}}-1}}$, $\underset{p_3}{\underset{\shortparallel}{2^{\overset{q_3}{4a+3}}-1}}$ non sono tutti e 3 numeri primi

p_3 primo $\Rightarrow$ q_3 primo

$$1 \equiv \left(\frac{2}{q_3}\right) \equiv 2^{\frac{q_3-1}{2}} \equiv 2^{q_2} \mod q_3$$

basta conoscere $q_3 \equiv 4 \cdot 1 + 3 \ (8)$

$$\Rightarrow \underset{4a+3}{\underset{\shortparallel}{q_3}} \mid 2^{q_2}-1 = p_2 = 2^{2a+1}-1$$

ci deve essere uguaglianza perché sono primi, ma è assurdo

$\square$

TST TAIWAN

$(m,n)=1$. Allora $\phi(5^m-1)\neq 5^n-1$

- $m=1$ non funziona

- m pari: n dispari, quindi $v_2(5^n-1)=2$ il n° di fattori 2 nella fattorizz.

  ma $8\mid 5^m-1$, $3\mid 5^m-1$ $\Rightarrow 24\mid 5^m-1$

  $\Rightarrow \phi(24)=4\cdot 2=8\mid \phi(5^m-1)$, assurdo

- m dispari, $A=5^m-1$.

Se $p^2\mid A$, allora $p\mid \phi(A)=5^n-1$

$p\mid A=5^m-1$

$\Rightarrow p\mid (5^n-1,5^m-1)=5^{(m,n)}-1=4$

(Quindi p dispari $\Rightarrow p^2\nmid A$)

$A=4\cdot p_1\cdots p_k=5^m-1$

$\phi(A)=2\cdot(p_1-1)\cdots(p_k-1)=5^n-1$

Mod p_i ho $5^m\equiv 1\ (p_i)\Rightarrow 5^{m+1}\equiv 5\ (p_i)$

$\Rightarrow \left(\frac{5}{p_i}\right)=+1$

$\Rightarrow \left(\frac{p_i}{5}\right)=+1\Rightarrow p_i\equiv\pm 1\,(5)$

Siccome $p_i-1\mid 5^n-1$, $p_i\not\equiv 1\ (5)$, quindi

$p_i\equiv -1 \pmod 5$

Guardando mod 5: $\int 4\cdot(-1)^k\equiv -1\ (5)$

$$\left. 2\cdot(-2)^k \equiv -1 \ (5) \right.$$

$$\begin{cases} (-1)^k \equiv 1 \ (5) \Rightarrow k \text{ pari}, \ k = 2t \\ 2\cdot(-1)^t \equiv -1 \ (5), \text{ assurdo.} \end{cases}$$ $\square$

Teorema Se a è un intero NON QUADRATO, esistono infiniti primi p per cui $\left(\frac{a}{p}\right) = -1$

Esercizio $a_1, \dots, a_{2019}$ interi ≥ 0

Supponiamo che per ogni $n > 0$ si abbia

$$a_1^n + \dots + a_{2019}^n = \square$$

Quanti sono come minimo gli $a_i = 0$?

Soluz. Sicuramente "so fare" il caso in cui

$$a_1 = \dots = a_k = 1, \quad a_{k+1} = \dots = a_{2019} = 0,$$

con K = più grande quadrato < 2019, cioè 1936

Prendiamo $n = p-1$, $p > \max\{a_i\}$. Allora (se t = n° degli $a_i \neq 0$) ottengo

$$\square \equiv a_1^{p-1} + \dots + a_{2019}^{p-1} \equiv t \pmod p$$

$\xRightarrow{\text{teorema}}$ t è un quadrato $\Rightarrow t \leq 1936.$ $\square$

TST di qualche posto

$$2^m - 1 \mid 3^n - 1 \Rightarrow n \text{ pari}$$

$$m, n \geq 2$$

Soluzione Sia p un primo che divide $2^m - 1$

[Oss gratis: m è dispari]

$p \mid 2^m - 1 \mid 3^n - 1$, e se (per assurdo) n fosse dispari avrei $3^{n+1} \equiv 3 \ (p) \Rightarrow \left(\frac{3}{p}\right) = +1$

* Se $p \equiv 1 \ (4)$, la RQ dice che anche $\left(\frac{p}{3}\right) = \left(\frac{3}{p}\right) = +1$

$\Rightarrow p \equiv 1 \ (3) \Rightarrow p \equiv 1 \ (12)$

* Se $p \equiv -1 \ (4)$, la RQ dà $\left(\frac{p}{3}\right) = -1 \left(\frac{3}{p}\right) = -1$

$\Rightarrow p \equiv -1 \ (3) \Rightarrow p \equiv -1 \ (12)$

Deduciamo che $2^m - 1 \equiv \pm 1 \ (12)$, che è assurdo con entrambi i possibili segni. $\square$

Tanti fattori primi $\equiv 3 \ (8)$

$\forall n > 0, \quad 2^{3^n} + 1$ ha $\geq n$ divisori primi $\equiv 3 \ (8)$

Idee • $2^9 + 1 = (2^3)^3 + 1 = (2^3 + 1)(2^{3 \cdot 2} - 2^3 + 1)$

$2^{27} + 1 = \underbrace{(2^9 + 1)}(2^{9 \cdot 2} - 2^9 + 1)$

$= (2^3 + 1)(2^{3 \cdot 2} - 2^3 + 1)(2^{9 \cdot 2} - 2^9 + 1)$

• (simile) Sia p un fattore di $2^n + 1$. Allora $p \not\equiv -1 \ (8)$, e se n è dispari non è nemmeno $\equiv 5 \ (8)$

Oss livello basic: $p \mid 2^n+1$ con n pari $\Rightarrow p \equiv 1\ (4)$,

quindi posso supporre n dispari

$$2^n+1 \equiv 0\ (p) \quad \Rightarrow \quad 2^{n+1} \equiv -2 \quad (p)$$

$$\Rightarrow \left(\frac{-2}{p}\right) = 1,$$

ma $$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1\ (8) \\ 1 & p \equiv 3\ (8) \\ -1 & p \equiv 5\ (8) \\ -1 & p \equiv 7\ (8) \end{cases}$$

LEMMA DI THUE

Fissiamo n intero positivo, K mod n.

La congruenza $y \equiv Kx \pmod n$ ha una soluz. intera (x_0, y_0) con $|x_0|, |y_0| \leq \sqrt{n}$

Dim. Prendiamo tutte le coppie (x, y) con

$$0 \leq x \leq \sqrt{n}, \qquad 0 \leq y \leq \sqrt{n}$$

Quante sono? $(\lfloor\sqrt{n}\rfloor + 1)\cdot(\lfloor\sqrt{n}\rfloor + 1) > n$ (anche se n è $\square$)

Per ogni coppia calcolo $y - Kx$ mod n.

Per pigeonhole ci sono 2 coppie distinte (x_1, y_1) e (x_2, y_2) t.c.

$$y_1 - Kx_1 \equiv y_2 - Kx_2 \quad (p)$$

$$\Leftrightarrow \quad y_1 - y_2 \equiv K(x_1 - x_2) \quad (p)$$

$\Rightarrow (x_1 - x_2, y_1 - y_2)$ è soluz, e $|x_1 - x_2| \leq \sqrt{n}$, $|y_1 - y_2| \leq \sqrt{n}$ $\blacksquare$

Lemma Se $p \equiv 1\ (4)$ esistono a, b interi t.c.

$$p = a^2 + b^2$$

Dim. Se $p = a^2+b^2 \Rightarrow a^2+b^2 \equiv 0\ (p)$

$$\Rightarrow (a \cdot b^{-1})^2 \equiv -1\ (p)$$

(Questo motiva la condiz. $p \equiv 1\ (4)$). Sia $m \in \mathbb{Z}$ t.c. $m^2 \equiv -1\ (p)$. Cerco di risolvere $a \cdot b^{-1} \equiv m\ (p)$

$\Leftrightarrow \quad a \equiv mb \pmod{p}$

Thue $\Rightarrow$ c'è soluz $\neq (0,0)$ con $|a|, |b| < \sqrt{p}$.

Allora $\quad 0 < a^2+b^2 < 2p$, ed inoltre

$$a^2+b^2 \equiv (mb)^2+b^2$$
$$\equiv b^2(m^2+1) \equiv 0\ (p)$$

$\Rightarrow a^2+b^2 = p.$ $\square$

Esercizio Sia p primo t.c. $\left(\frac{7}{p}\right) = +1$. Allora uno fra $\pm p$ si scrive come $y^2 - 7x^2$.

Soluz. Prendo m t.c. $m^2 \equiv 7 \bmod p$, e uso Thue su $y \equiv mx \bmod p \rightarrow$ soluz $\neq (0,0)$ con $|x|, |y| < \sqrt{p}$.

$$y^2 - 7x^2 \equiv m^2x^2 - 7x^2 \equiv 0\ (p)$$
$$|y^2 - 7x^2| < 7p$$

$$y^2 - 7x^2 = \pm p, \ \pm 2p, \ \pm 3p, \ \pm 4p, \ \pm 5p, \ \pm 6p$$

OK

in modo analogo a $2p$

mod 4 scopro che $x \equiv y \equiv 0 \, (2)$ $\Rightarrow \left(\frac{y}{2}\right)^2 - 7\left(\frac{x}{2}\right)^2 = \pm p$

* $y^2 - 7x^2 = \pm 5p \Rightarrow y^2 \equiv 7x^2 \, (5)$

$x \not\equiv 0 \, (5)$: $(y/x)^2 \equiv 2 \, (5)$ assurdo

$x \equiv 0$: $y \equiv 0 \Rightarrow x^2 - 7y^2 \equiv 0 \, (25)$, assurdo

* Se $y^2 - 7x^2 = \pm 2p$, x e y sono dispari

$$\left(\frac{3a-7b}{2}\right)^2 - 7\left(\frac{3b-a}{2}\right)^2 =$$

$$= \frac{1}{4}\left[9a^2 + 49b^2 - \cancel{42ab} - 63b^2 - 7a^2 + \cancel{42ab}\right]$$

$$= \frac{1}{4}\left[2a^2 - 14b^2\right] = \frac{1}{2}(a^2 - 7b^2) = \pm p$$

(MAGIA!)

Dietro le quinte: $N(y + \sqrt{7}x) = \pm 2p$

Risolviamo $c^2 - 7d^2 = \pm 2 \rightsquigarrow$ e.g. $3 + \sqrt{7}$

$$N\left(\frac{y + \sqrt{7}x}{3 + \sqrt{7}}\right) = \frac{N(y + \sqrt{7}x)}{N(3 + \sqrt{7})} = \frac{\pm 2p}{2} = \pm p$$

$$\frac{y + \sqrt{7}x}{3 + \sqrt{7}} = \frac{1}{2}\left((y + \sqrt{7}x)(3 - \sqrt{7})\right) = \frac{1}{2}\left(3y - 7x + \sqrt{7}(3x - y)\right)$$

Teo Un intero positivo n è somma di 2 quadrati se e solo se, scrivendo $n = 2^a \cdot p_1^{e_1} \cdots p_k^{e_k} \, q_1^{f_1} \cdots q_\ell^{f_\ell}$

primi $\equiv 1(4)$ primi $\equiv 3(4)$

tutti gli f_i sono pari.

Sketch di dim

$$\underbrace{(a^2+b^2)}_{N(a+bi)}\underbrace{(c^2+d^2)}_{N(c+di)} = \underbrace{(ac-bd)^2+(ad+bc)^2}_{N((a+bi)(c+di))}$$

parte sufficiente

Parte nec: $p \equiv 3(4)$, $p \mid x^2+y^2$

Se per assurdo $p \nmid y$ $\quad \left(\frac{x}{y}\right)^2+1 \equiv 0 \ (p)$

$\Rightarrow \left(\frac{-1}{p}\right) = 1$, assurdo

$\Rightarrow p \mid y \Rightarrow p \mid x \Rightarrow p^2 \mid x^2+y^2$ $\square$

Può venire la tentazione di pensare che

$y^2 - ax^2 = \pm p$ ha soluz $\Leftrightarrow \left(\frac{a}{p}\right) = 1$

Controesempio: $y^2+5x^2=7$ non ha soluzione,

ma $\left(\frac{-5}{7}\right) = +1$