N2 MEDIUM

Note Title 04/02/2023

- VIETA JUMPING
- INTERI GAUSSIANI
- EQ. DI PELL
- SIMBOLI DI LEGENDRE

IMO 88/6 $\quad a,b \in \mathbb{Z}^+ \quad \frac{a^2+b^2}{2ab+1} = k \in \mathbb{Z}^+ \Rightarrow k = m^2$

Data una sol. (a,b) di $a^2+b^2-k(2ab+1)=0$, vogliamo trovarne una "più piccola" (a',b), con lo stesso k.

Assumiamo per ass. di avere $k \neq \square$, con una sol. (a,b) con $a+b$ minimale, WLOG $a \geq b$ *, a è sol. di $t^2 - kb\cdot t + (b^2-k) = 0$.

Per formule di Viète, l'altra sol. è

$$a' = kb - a = \frac{b^2-k}{a}.$$

* se (a,b) è sol. anche (b,a) lo è

$\downarrow$

$a' \in \mathbb{Z}$

Se fosse $a' < 0$ $\quad \frac{a'^2+b^2}{1+a'b} = k > 0$ assurdo

($1+a'b \leq -1 < 0$)

$\rightarrow a' \geq 0$.

Se $a' > 0 \Rightarrow a' = \frac{b^2-k}{a} < \frac{b^2}{a} \overset{b \leq a}{\leq} \frac{a^2}{a} = a$ $\quad a' < a$

$a'+b < a+b$ assurdo

$\Rightarrow a' = 0 = \frac{b^2-k}{a} \Rightarrow k = b^2$.

IMO 2007/5

$a,b \in \mathbb{Z}^+ \quad 4ab-1 \mid (4a^2-1)^2 \Longrightarrow a=b$

L'ipotesi a dx non è simmetrica, quindi la vogliamo rendere tale

$4ab-1 \mid (4a^2b-b)^2 \qquad 4a^2b-b \equiv a-b \pmod{4ab-1}$

$\Rightarrow 4ab-1 \mid (a-b)^2 \to \exists k$ t.c.

$(a-b)^2 = k(4ab-1)$

$a^2-(2+4k)b\cdot a+(b^2+k)=0$

se $a=b$ abbiamo finito.

Se $a \neq b$, WLOG $a>b$; a è sol di $t^2-(2+4k)b\cdot t+(b^2+k)=0$

L'altra sol. è $a' = (2+4k)b-a = \frac{b^2+k}{a} \in \mathbb{Z}^+$

Se (a,b) era la sol. con $a+b$ minimale, non possiamo avere $a' < a$. Tuttavia, abbiamo

$$k = \frac{(a-b)^2}{4ab-1} < \frac{(a-b)^2}{3ab} = \frac{1}{3}\left(\frac{a}{b}+\frac{b}{a}\right)-\frac{2}{3} \leq \frac{1}{3}\left(a+\frac{1}{a}\right)-\frac{2}{3} \leq$$

($ab \geq 1$; $1 < \frac{a}{b} \leq a$; $f(t) = t+\frac{1}{t}$ è crescente su $[1,+\infty)$)

$$\leq \frac{1}{3}(a+1)-\frac{2}{3} = \frac{1}{3}(a-1)$$

Ma allora $a' = \frac{b^2+k}{a} < \frac{(a-1)^2+\frac{1}{3}(a-1)}{a} < \frac{a^2}{a} = a$

($\frac{1}{3}(a-1) < 2(a-1) < 2a-1$)

$\to (a',b)$ ha somma più piccola, quindi assurdo. □

Notiamo che in entrambi i problemi era importante avere la simmetria, in modo da poter scambiare le due variabili.

ESERCIZI

I) $\frac{a^2+b^2+1}{ab} = k \in \mathbb{Z}^+ \Rightarrow k=3 \qquad a,b \in \mathbb{Z}^+$

II) Trovare tutte le sol. di $a|b^2-b+1 \wedge b|a^2-a+1$

III) $\frac{a^2+b^2}{ab-1}=k \in \mathbb{Z}^+ \Rightarrow k=5$

INTERI DI GAUSS

$$\mathbb{Z}[i]=\{a+bi : a,b\in\mathbb{Z}\}$$

$N(a+bi)=a^2+b^2=(a+bi)(a-bi)$ ← è il coniugato di $a+bi$

$\alpha,\beta\in\mathbb{Z}[i]$ $\quad N(\alpha)N(\beta)=N(\alpha\beta)$

INVERTIBILI

$\alpha\beta=1 \Rightarrow N(\alpha)N(\beta)=1 \Rightarrow N(\alpha)=N(\beta)=1 \Rightarrow \alpha\in\{1,-1,i,-i\}$.

α è primo se $\forall \beta,\gamma \quad \alpha|\beta\gamma \Rightarrow \alpha|\beta \vee \alpha|\gamma$

α è irriducibile se $\beta\gamma=\alpha \Rightarrow \beta$ o γ invertibile

FATT IN IRRIDUCIBILI: $\forall \alpha\in\mathbb{Z}[i]$ $\exists$ v invertibile e $p_1,\dots,p_n$ primi tali che $\alpha=v\cdot p_1\cdots p_n$ e i p_i sono unici a meno di ordine e associati.

Si può parlare di MCD e vale il Teorema di Bezout.

I primi di $\mathbb{Z}[i]$ sono tutti e soli i $p\in\mathbb{Z}$ tali che $p\equiv 3\ (4)$ e gli $x+iy$ con $x^2+y^2=p$ con $p\equiv 1\ (4)$:

- $p\equiv 3\ (4)$, se $\alpha\beta=p \Rightarrow N(\alpha)N(\beta)=p^2$, se α e β non sono INV $N(\alpha),N(\beta)\neq 1$ $\Rightarrow N(\alpha)=N(\beta)=p$, ma allora $\exists x,y\in\mathbb{Z}: x^2+y^2=p\equiv 3\ (4)$, mod 4 non torna, oppure $x^2+y^2\equiv 0\ (p) \Rightarrow \left(\frac{x}{y}\right)^2+1\equiv 0\ (p) \Rightarrow \left(\frac{x}{y}\right)^2\equiv -1\ (p)$, assurdo.

(CRIT DI EULERO: $a \in \mathbb{Z}$ é RES QUAD mod $p \iff a^{\frac{p-1}{2}} \equiv 1 \ (p)$)

• $p \equiv 1 \ (4)$, siccome -1 é RQ mod p $\exists d \in \mathbb{Z} : d^2 \equiv -1 \ (p) \Rightarrow p \mid d^2+1 = (d+i)(d-i)$
ma: $p \nmid d+i$ e $p \nmid d-i$ (in $\mathbb{Z}[i]$) perché $p(a+bi) = \underbrace{pa + pbi}$ sono multipli di p. Quindi p non é primo $\Rightarrow \exists \alpha, \beta \in \mathbb{Z}[i]$ con $\alpha\beta = p$ e α, β non INV.
$N(\alpha) N(\beta) = p^2 \Rightarrow N(\alpha) = N(\beta) = p$, $\alpha\bar{\alpha} = \beta\bar{\beta} = p$ (note che α e β sono IRR)
($\iff \exists x, y \in \mathbb{Z}^+$ con $x^2+y^2 = p$ e sono NNMCI!)

LEMMA DI THUE: sia p primo e $k \in \mathbb{Z}$ con $p \nmid k$, allora $\exists a, b$ con $-\sqrt{p} < a, b < \sqrt{p}$ tali che $ak \equiv b \ (p)$. (dimostrate $x^2+y^2 = p$ con questo)

• per casa: dimostrate che non ci sono altri primi.

Vediamo per quali $n \in \mathbb{Z}^+$ $\exists x, y \in \mathbb{Z}_{>0}$ tali che $x^2+y^2 = n$:
N moltiplicativa $\Rightarrow (x^2+y^2)(z^2+w^2) = (xz-yw)^2 + (xw+yz)^2$.
Sappiamo fare i $p \equiv 1 \ (4)$, p^2 con $p \equiv 3 \ (4)$, $2 \ (= 1^2+1^2)$ e per l'identità tutti i loro prodotti. Si può fare altro? NO: prendiamo n con un certo $p \equiv 3 \ (4)$ tale che $v_p(n)$ é dispari. Se $n = x^2+y^2 \Rightarrow x^2+y^2 \equiv 0 \ (p)$, se x, y non sono $0 \pmod p$ trovo $(x/y)^2 \equiv -1 \ (p)$, falso da sopra; quindi $p \mid x, y \Rightarrow$ pongo $x = px_1$ e $y = py_1$, $n/p^2 = x_1^2+y_1^2$, da qua itero finché $v_p(n) = 1$.

PROBLEMA: trova le coppie $x, y \in \mathbb{Z}$ tali che $x^5 - 1 = y^2$.
DIM: $x^5 = y^2+1 = (y+i)(y-i)$, proviamo a dire che $y+i$ e $y-i$ sono coprimi
$MCD(y+i, y-i) = MCD(y+i, 2i) = MCD(y+i, 2)$, note che se x é pari $y^2 \equiv -1 \ (4)$ che non va bene $\Rightarrow x$ é dispari e y é pari.
OSS: se $\alpha \mid \beta \Rightarrow N(\alpha) \mid N(\beta)$. nel nostro caso se α é un divisore comune $N(\alpha) \mid y^2+1$ e $N(\alpha) \mid 4$, ma y^2+1 é dispari $\Rightarrow N(\alpha) = 1 \Rightarrow y+i$ e $y-i$ sono coprimi.
come in $\mathbb{Z}$ questo si dice che $\exists \alpha \in \mathbb{Z}[i]$: $\alpha^5 = y+i$ e $\bar{\alpha}^5 = y-i$, pongo
$\alpha = a+bi \Rightarrow y+i = (a+bi)^5 = a^5 - 10a^3b^2 + 5ab^4 + i(5a^4b - 10a^2b^3 + b^5)$,

dalla parte Imm vedo $b|1 \Rightarrow b = \pm 1$:

- $b=1 \Rightarrow 1 = 5a^4 - 10a^2 + 1 \Rightarrow 5a^2(a^2-2) = 0 \Rightarrow a = 0$
- $b=-1 \Rightarrow 1 = -5a^4 + 10a^2 - 1 \Rightarrow 0 \equiv 2 \ (5)$, impossibile.

Quindi $\alpha = i \Rightarrow x^5 = 1 \Rightarrow x = 1 \Rightarrow y = 0$.

ES PER CASA

1) $xy = z^2 + 1$ con $x, y, z \in \mathbb{Z}^+$, allora $\exists a, b, c, d \in \mathbb{Z} : x = a^2 + b^2$, $y = c^2 + d^2$ e $z = ac + bd$.
2) Trovare i primi p tali $\exists x, y : x^2 + 2y^2 = p$ (CON THUE).
3) BMO 2021/3: siano $a, b, c \in \mathbb{Z}^+$ tali che $(a,b) + [a,b] = 2021^c$ e $|a-b|$ è primo, allora $(a+b)^2 + 4$ è composto.

Equazioni di Pell $\quad d \in \mathbb{Z}$, $d > 0$, d non quadrato

$$x^2 - dy^2 = 1 \qquad x, y \in \mathbb{Z}$$

$$\mathbb{Q}(\sqrt{d}) = \{ a + b\sqrt{d} \mid a, b \in \mathbb{Q} \}$$

$$\mathbb{Z}[\sqrt{d}] = \{ a + b\sqrt{d} \mid a, b \in \mathbb{Z} \}$$

$$\frac{a + b\sqrt{d}}{c + e\sqrt{d}} = \frac{(a + b\sqrt{d})(c - e\sqrt{d})}{\underbrace{c^2 - e^2 d}_{\in \mathbb{Q}}} =$$

$N(a + b\sqrt{}$

(di norma 1)

$\{$ unità fondamentale: minimo elemento in

$\mathbb{Z}[\sqrt{d}]$ con $N(\xi) = 1$ e $\xi > 1$

Ogni elemento di norma 1 è della forma

$\pm \xi^k \quad k \in \mathbb{Z} \quad \xi = u + v\sqrt{d} \quad \xi^{-1} = u - v\sqrt{d}$

$\eta \in \mathbb{Z}[\sqrt{d}] \quad N(\eta) \quad 1 \le \pm \eta \xi^k < \xi$

quasi-Pell $\quad x^2 - d y^2 = m$

Esempi

$x^2 - 5y^2 = 1$

$9^2 - 5 \cdot 4^2 = 1$

$2^2 - 5 \cdot 1^2 = -1$

$N(2 + \sqrt{5}) = -1$

$N\left((2+\sqrt{5})^2\right) = 1$

$4 + 4\sqrt{5} + 5 = 9 + 4\sqrt{5} = \xi \lesssim 18$

unità fondamentale

$(9 + 4\sqrt{5})^n = x_n + y_n \sqrt{5}$

$1 = \xi^0 = 1 + 0\sqrt{5} \qquad x_0 = 1 \qquad y_0 = 0$

$\vdots$

$\xi^{n+1} = \xi\, \xi^n = (9 + 4\sqrt{5})(x_n + \sqrt{5} y_n) =$

$= 9x_n + 9y_n\sqrt{5} + 4x_n\sqrt{5} + 20 y_n$

$$\begin{cases} x_{n+1} = 9x_n + 20y_n \\ y_{n+1} = 4x_n + 9y_n \end{cases} \qquad \xi^{-n} = x_n - y_n\sqrt{5}$$

$$x^2 - 5y^2 = -29$$

Sia $\alpha = x + \sqrt{5}y > 0$ con $x^2 - 5y^2 = -2$

trovo $k \in \mathbb{N}$ t. c. $\sqrt{\frac{29}{\xi}} \le \alpha \cdot \xi^k < \sqrt{29\,\xi}$ $\qquad \beta = \alpha \cdot \xi^k$

$\beta' = x - \sqrt{5}y$ $\qquad |\beta'| = \left|\frac{-29}{\beta}\right| \le \sqrt{\frac{29}{29\xi}} = \underbrace{\sqrt{29\,\xi}}_{<6}$

$\beta\beta' = -29$

$\beta = u + \sqrt{5}v$ $\qquad |u| = \left|\frac{\beta + \beta'}{2}\right| \le \sqrt{29\xi}$ con $29 \approx 23$

$$|v| = \left|\frac{\beta - \beta'}{2\sqrt{5}}\right| \le \sqrt{\frac{29\xi}{5}}$$

provando $v = 2, 3$ $\qquad v \lesssim 12$

$16 - 9 \cdot 5 = -29$ $\qquad 4 + 3\sqrt{5}$

$$u_n + \sqrt{5}v_n = (4 + 3\sqrt{5})(9 + 4\sqrt{5})^n$$

$u_0 = 4 \quad v_0 = 3$ $\qquad \begin{cases} u_{n+1} = 9u_n + 20v_n \\ v_{n+1} = 4u_n + 9v_n \end{cases}$

RESIDUI QUADRATICI E SIMBOLI DI LEGENDRE

$a \in \mathbb{Z}$ p primo

$$\left(\frac{a}{p}\right) := \begin{cases} +1 & \text{se } a \text{ è residuo quadratico mod } p \ (\text{e } p \nmid a) \\ -1 & \text{se non lo è} \\ 0 & \text{se } p \mid a \end{cases}$$

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \quad \text{se } a \equiv b \pmod p$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$(a;p)=1 \rightarrow \left(\frac{a^{-1}}{p}\right) = \left(\frac{a}{p}\right)^{-1} = \left(\frac{a}{p}\right)$

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

CRITERIO DI EULERO

Se $(a;p)=1 \rightarrow \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

$p>2$

DIM Sia g un generatore $(\bmod p)$

$a = g^k$ $\quad a$ è QR $\iff \exists\, b = g^l \quad b^2 \equiv a \ (p)$

$\longleftrightarrow \quad g^{2l} \equiv g^k \ (p) \longleftrightarrow 2l \equiv k \ (p-1) \longleftrightarrow k$ è pari

$p-1$ pari

$$a^{\frac{p-1}{2}} \equiv g^{k\frac{p-1}{2}} \ (p) \qquad k\frac{p-1}{2} \equiv \begin{cases} 0 \\ \frac{p-1}{2} \end{cases} \bmod p \quad \begin{matrix} \text{se } k \text{ è pari} \\ \text{se } k \text{ è dispari} \end{matrix}$$

a è QR $\rightarrow \quad a^{\frac{p-1}{2}} \equiv g^0 \equiv 1 \ (p)$

a è NQR $\rightarrow \quad a^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \ (p)$

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

$\longrightarrow \left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p \Rightarrow \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

LEMMA DI GAUSS

$(a,p)=1$ $\quad S = \{0 < k < p/2\}$

$p>2$ $\quad N = |\{k \in S \mid ak \pmod p \in S\}|$

$\longrightarrow \left(\frac{a}{p}\right) = (-1)^N$

Thm. RECIPROCITÀ QUADRATICA

Siano $p, q > 2$ due primi distinti. Allora

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

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} +1 & \text{altrimenti } (p \equiv 1 \ (4) \text{ o } q \equiv 1 \ (4)) \\ -1 & \text{se } p \equiv 3 \ (4) \text{ e } q \equiv 3 \ (4) \end{cases}$$

$\left(\frac{2}{p}\right) = (-1)^N \quad N = |\{k \in S \mid 2k \pmod p \in S\}| = \left\lfloor \frac{p/2}{2} \right\rfloor = \left\lfloor \frac{p}{4} \right\rfloor$

$p>2$ $\quad = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{se } p \equiv 1, 7 \ (8) \\ -1 & \text{se } p \equiv 3, 5 \ (8) \end{cases}$

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{se } p \equiv 1 \ (4) \\ -1 & \text{se } p \equiv 3 \ (4) \end{cases}$

↓ CRIT. DI EULERO

PROBLEMA $m \in \mathbb{Z}^+$ $\forall p$ primo m è QR mod p $\Rightarrow m$ è $\square$

DIM. Scomponiamo $m = q_1^{\alpha_1} \cdots q_n^{\alpha_n}$. WLOG $\alpha_i = 1$

(altrimenti divido per un quadrato opportuno)

$$\left(\frac{m}{p}\right) = \left(\frac{q_1 \cdots q_n}{p}\right) = \left(\frac{q_1}{p}\right) \cdots \left(\frac{q_n}{p}\right)$$

Per assurdo $n > 0$. Per primo caso voglio un primo $p \equiv 1 (4)$

In tal caso $\left(\frac{m}{p}\right) = \left(\frac{q_1}{p}\right) \cdots \left(\frac{q_n}{p}\right) = \left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right) \cdots \left(\frac{p}{q_n}\right)$ * $(p > \max q_i)$

$p \equiv 1 (q_i) \to \left(\frac{p}{q_i}\right) = 1$ * $(\forall q_i > 2)$

voglio $p \equiv 1 \pmod{q_i}$ $\forall i = 2, \dots, n$

voglio $p \equiv r \pmod{q_1}$ con r NCR mod q_1

$\to$ Per TCR, voglio $p \equiv r' \pmod{4 q_1 \cdots q_n}$ $\left(\text{con } \begin{matrix} r' \equiv r (q_1) \\ r' \equiv 1 (4 q_2 \cdots q_n) \end{matrix}\right)$

Ovviamente $(r', 4 q_1 \cdots q_n) = 1$

Thm Dirichlet: $\forall a, b$ coprimi $\exists \infty$ p primi $p \equiv a \pmod{b}$

$\to \exists p$ t.c. $\left(\frac{m}{p}\right) = \left(\frac{p}{q_1}\right) \cdots \left(\frac{p}{q_n}\right) = (-1) \cdot 1^{n-1} = -1$ assurdo

* Se $q_1 = 2$ voglio $p \equiv 1 \pmod{q_i}$ $\forall i > 1$

$p \equiv 5 \pmod 8$

La prima cond. implica $\left(\frac{p}{q_i}\right) = 1$ $\forall i > 1$

La seconda dice che $p \equiv 1 (4)$ e $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1$

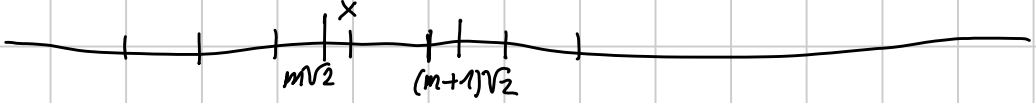
$\to$ Anche in questo caso $\left(\frac{m}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{q_2}\right) \cdots \left(\frac{p}{q_n}\right) = (-1) \cdot (1)^{n-1} = -1$ assurdo

$\to$ quindi $n = 0$, cioè $m = 1$ (e il nostro numero originale era un $\square$)

N

PROBLEMA: $\exists \infty (n,m)$ di interi positivi tali che $n^2 = \lfloor m\sqrt{2} \rfloor$.

Per assurdo sono finite, allora fisso un $M \in \mathbb{Z}^+$ tale che se (m,n) è soluzione $M \geq m,n$. Se prendo un $x > M$ $\exists m \in \mathbb{Z}^+ : x^2 = \lfloor m\sqrt{2} \rfloor + 1$



$m\sqrt{2} \leq x^2$ e $(m+1)\sqrt{2} \geq x^2 + 1 \Rightarrow m\sqrt{2} < x^2 < m\sqrt{2} + (\sqrt{2}-1) < m\sqrt{2} + \frac{1}{2}$

$\Rightarrow 2m\sqrt{2} < 2x^2 < 2m\sqrt{2} + 1$, considero la PELL $y^2 - 2x^2 = -1$, ha ∞ SOL

$\Rightarrow$ anche una con $x > M$, $y^2 = 2x^2 - 1 \Rightarrow 2m\sqrt{2} - 1 < y^2 < 2m\sqrt{2} \Rightarrow \lfloor 2m\sqrt{2} \rfloor = y^2$.

PER CASA

1) ISL NS/2016

2) $\exists \infty n \in \mathbb{Z}^+$ tali che n^2+1 ha due divisori positivi con differenza n.

3) $\exists \infty n \in \mathbb{Z}^+$ tali che $n^2 + 1 \mid n!$.