N 1 - M

Titolo nota 10/09/2009

Problema 6 IMO 1988

a, b interi positivi tali che

$$ab+1 \mid a^2+b^2$$

Tesi: $\dfrac{a^2+b^2}{ab+1}$ è un quadrato perfetto.

Metodo: $a^2+b^2 = k(ab+1)$ $\quad k \in \mathbb{Z}$ FISSATO

Se (a,b) è una soluzione, allora è una radice (intera positiva) dell'equazione

$$x^2+b^2 = k(xb+1)$$

$$x^2 - kbx + b^2 - k = 0, \qquad x^2 - sx + p = 0$$

Radici: a, a' $\quad a+a' = kb \quad a' = kb-a$

$$aa' = b^2-k$$

L'altra soluzione, a', è non negativa $(a' \geq 0)$.

$a'^2+b^2 > 0$ (> 0) se $a' < 0$ $\quad a'b+1 \leq 0$ $\quad k(a'b+1) \leq 0$ ASSURDO

Osservazione Se $a \geq b$ allora $a' < b$

(il prodotto delle radici è $< b^2$)

Data una soluzione (a,b) $\quad a \geq b$ posso produrne un'altra (a', b) $\quad a' < b$.

Vale dunque l'uguaglianza

$$a'^2+b^2 = k(a'b+1)$$

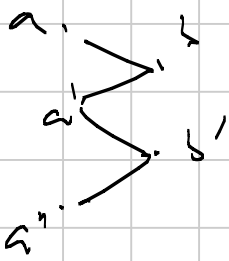
b è radice dell'equazione

$$y^2 - ka'y + a'^2 - k = 0$$

$b > a'$ $\quad$ b' seconda sol. $\quad$ $b' < a'$

$$(a,b) \to (a',b) \to (a',b') \to (a'',b')$$

$a \geq b$ $\quad$ $a' < b$ $\quad$ $a' > b'$ – $a'' < b'$



MI FERMO quando trovo una sol. $=0$

P. es. $b=0$

$$a^2 + 0^2 = k(a \cdot 0 + 1)$$

$$a^2 = k$$

$(a,0)$ sol. con $k = a^2$

$$a^2 + b^2 = a^2(ab+1)$$

$$b^2 - a^3 b + a^2 - a^2 = 0$$

$b = 0$ oppure $b = a^3$

(a, a^3) è soluzione con $k = a^2$

$$\frac{a^2+b^2}{ab+1} \in \mathbb{N} \qquad a^2 = \frac{a^2 + a^6}{a^4+1} \in \mathbb{N}$$

Andando avanti, posso trovare altre soluzioni andando "a ritroso":

$$a^2 + a^6 = k(a \cdot a^3 + 1)$$

x^2 $\quad$ b^2 $\quad$ a^2 $\quad$ b

a è soluzione di $x^2 - a^5 x + a^6 - a^2 = 0$

L'altra soluzione è $a^5 - a$.

Problema 5 – IMO 2007

a, b interi positivi.

Se $4ab-1 \mid (4a^2-1)^2$ allora $a=b$.

Supponiamo $\dfrac{(4a^2-1)^2}{4ab-1} = k \in \mathbb{Z}$

Congruenza modulo $4a$:

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

$$1 \equiv k \cdot (-1) \pmod{4a}$$

$$k \equiv -1 \pmod{4a}$$

$$k = 4ab' - 1$$

Claim: in effetti è vero anche che

$$4ab-1 \mid (4b^2-1)^2$$

Dim. claim. Ragioniamo modulo $4ab-1$:

$$(4b^2-1)^2 \equiv (4b^2 - 4^2a^2b^2)^2 \equiv 16b^4(1-4a^2)^2 \pmod{4ab-1}$$

$4ab-1$ divide

$$\equiv 0$$

RIASSUNTO: (tesi: $a=b$)

Per assurdo: supponiamo che esista una soluzione con $a<b$ $\quad 4ab-1 \mid (4a^2-1)^2$

Allora esiste un'altra soluzione (a, b') con $a \neq b'$ $\quad 4ab'-1 \mid (4a^2-1)^2$

(Se fosse $a \leq b'$ allora:

$4ab-1 < 4a^2-1$ $\quad (4ab-1)(4ab'-1) < (4a^2-1)^2$

$4ab'-1 \leq 4a^2-1$

L'altra soluzione era: $4ab'-1 = \dfrac{(4a^2-1)^2}{4ab-1}$)

D'altra parte ho anche $4ab'-1 = (4b'^2-1)^2$

$(a,b) \to (a,b') \to (a',b') \to$

$a<b$ $\quad (a>b')$ $\quad (a',b')$ $\to$

ARRIVO AD UNA SOL. MINIMALE

(per simmetria suppongo $b=1$)

$4ab-1 \mid (4b^2-1)^2$

$4a-1 \mid 3^2$

$4a-1=3 \quad a=1=b$ ASSURDO

PREIMO N8 (2007)

a, b, m, n interi positivi. Trovare le soluzioni di

$$a^m b^n = (a+b)^2 + 1.$$

SOLUZIONE STANDARD: disuguaglianze (m, n piccoli + divisibilità).

SOLUZIONE ELEGANTE:

LEMMA L'equazione $x^2+y^2+1 = kxy$ ha soluzioni in interi positivi se e solo se $k=3$ (e in questo caso ne ha infinite).

DIM. LEMMA Supponiamo $k \neq 3$.

1° caso (Assurdo) Esiste una soluzione (x_0, y_0) con $x_0 = y_0$.

$$2x_0^2 + 1 = kx_0^2$$
$$1 = (k-2)x_0^2$$
$$\Rightarrow \quad x_0^2 = 1, \quad k-2 = 1 \quad k = 3 \quad \text{ASSURDO}.$$

2° caso (Assurdo) Esiste una sol (a, b) con $a > b$.

$$a^2 + b^2 + 1 = kab$$

a è soluzione dell'equazione

$$x^2 - kbx + b^2 + 1 = 0.$$

C'è un'altra soluzione a' $\quad a + a' = kb$, $\quad aa' = b^2 + 1$

Se $b > 1$, allora $a' < b$

(infatti $a' \geq b$ $\quad a > b \Rightarrow aa' \geq b^2 + b > b^2 + 1$)
$\quad a \geq b + 1$

Trovo una sol con $b = 1$ (per simmetria)

$$x^2 - kx + 2 = 0$$

Basta vedere $x = 1, x = 2$ che danno entrambe $k = 3$.
($x = -1, -2$ in questo caso non importano)

Invece per $k = 3$ c'è la soluzione $(1, 1)$

$$x^2 + y^2 + 1 = 3xy$$

Trovando altre soluzioni "a ritroso" ne trovo altre

$(1,1) \to (2,1) \to (2,5) \to (13,5) \to \dots$

(Sono tutte perché in ogni "catena" ci deve essere una sol con x (o y) $= 1$).

→ Problema: $\quad a^m b^n - 2ab = a^2 + b^2 + 1$

$$(a^{m-1} b^{n-1} - 2)ab = a^2 + b^2 + 1$$

k ←

Soluzioni → $\quad a^{m-1} b^{n-1} - 2 = 3$
$\quad a^{m-1} b^{n-1} = 5$

$a=5$ $\qquad 3\cdot 5\cdot b = 25+5^2+1$

$m=2$ $\qquad b = 2,13 \qquad n=1$

e simmetrica $((a,m) \leftrightarrow (b,n))$.

METODO DEL PIÙ PICCOLO PRIMO.

Problema 3 – IMO 1990

Per quali $n>1$ si ha che $\dfrac{2^n+1}{n^2}$ è un intero?

$n^2 \mid 2^n+1 \qquad 2^n+1 \equiv 0 \pmod{n^2}$.

$\downarrow$

VALE $\forall d \mid n$

$\forall p \mid n$ primo

p = minimo divisore primo di n

(Oss.: n deve essere dispari)

$2^n+1 \equiv 0 \pmod p$

$2^n \equiv -1 \pmod p$

$2^{2n} \equiv 1 \pmod p$

$\text{ord}_p 2 \mid (2n, p-1) \quad \overset{p \text{ min.}}{\Longrightarrow} \quad \text{ord}_p 2 \mid 2$

$p \mid 2^1-1=1$ ASSURDO

oppure

$p \mid 2^2-1=3$

Eventuali soluzioni sono della forma

$n = 3^k m \qquad (k \geq 1, \ m \text{ dispari}, \ 3 \nmid m)$

Se $n = 3^k m$ è soluzione, in particolare ho $(n^2 = 3^{2k} m^2)$

$$2^{3^k m} + 1 \equiv 0 \pmod{3^{2k}}$$

$k=1$ $m=1$ $\quad 2^3 + 1 \equiv 9$ $\quad 3^2 \| 9$

$2^{3^2} + 1$ $\quad 3^3 \| 2^{3^2} + 1$

$3^{a+1} \| 2^{3^a} + 1$ $\quad$ ⊗

$2^{3^k} + 1 = 3^{k+1} b$

$2^{3^k} = 3^{k+1} b - 1$

$2^{3^k m} = (3^{k+1} b - 1)^m = \ldots - \binom{m}{2} 3^{2k+2} b^2 + 3^{k+1} mb - 1$

$2^{3^k m} + 1 = \underbrace{\qquad - \qquad}_{\text{divisibili per potenze di 3 più alte}} + 3^{k+1} mb$

⊗ MI DICE CHE $k=1$

$$2^{3^k m} + 1 \equiv 0 \pmod{3^{2k}}$$

$2k \le k+1$ $\quad k \le 1$.

Resta il caso $n = 3m$ $\quad$ ($n=3$ sol)

$$2^{3m} + 1 \equiv 0 \pmod{9m^2}$$

$$2^{6m} \equiv 1 \pmod{9m^2}$$

Sia q il più piccolo fattore primo di m (se $m > 1$)

$$2^{6m} \equiv 1 \pmod{q}$$

$\operatorname{ord}_q 2 \mid (q-1, 6m) \mid 6$

$\operatorname{ord}_q 2 = 1, 2, 3, 6$

$q \mid 2^1 - 1 = 1$ $\quad q \mid 2^2 - 1 = 3$ $\quad q \mid 2^3 - 1 = 7$ $\quad q \mid 2^6 - 1 = 63 = 3^2 \cdot 7$

$\Rightarrow q = 7$.

$2^3 \equiv 1 \pmod 7$ $\quad$ $2^{3n} \equiv 1 \pmod 7$

$2^{3n+1} \equiv 2 \pmod 7$ $\quad$ NO

$\neq 0$

Problema 4 – IMO 1999

$0 < n < 2p$ con $n^{p-1} \mid (p-1)^n + 1$

(p primo)

Trovare le soluzioni.

$n = 1$ $\quad$ OK $\quad \forall p$.

$p = 2$ $\quad$ $n = 1, 2$.

$p > 2$ (dispari) $\rightarrow$ quindi n dispari.

q = minimo primo che divide n.

Una soluzione è tale che $(p-1)^n + 1 \equiv 0 \pmod q$

$(p-1)^n \equiv -1 \pmod q$

So anche che $(p-1)^{q-1} \equiv 1 \pmod q$

$(q-1, n) = 1$ $\quad$ posso ottenere

$an + b(q-1) = 1$ $\quad$ a dispari

$p - 1 \equiv (p-1)^{an + b(q-1)} \equiv (-1)^a \cdot 1^b \equiv -1 \pmod q$

$p \equiv 0 \pmod q$ $\quad$ $q \mid p$ $\quad$ $q = p$.

Ordine moltiplicativo $\quad \text{ord}_q (p-1) \mid (2n, q-1) \mid 2$

$(p-1)^2 \equiv 1 \pmod q$ $\quad$ $q \mid p(p-2)$

Se $q \mid p-2$ $\quad p \equiv 2 \pmod q$ $\quad p-1 \equiv 1 \pmod q$

$(p-1)^n + 1 \equiv 2 \pmod q$ ASSURDO

IN ENTRAMBI I MODI SI HA $q = p$ -

Poiché $q \mid n$, $n < qp$ resta solo il caso $n = p$.

Cioè

$$p^{p-1} \mid (p-1)^p + 1$$

$$(p-1)^p = p^p - \binom{p}{1} p^{p-1} \cdots - \binom{p}{2} p^2 + \binom{p}{1} p - 1$$

$\binom{p}{1} = p$

divisibile per p^3

$p-1 \le 2$ $\quad p = 3$ FUNZIONA (VERIFICA)

POLINOMI

$$f(x) = 7x^4 + 3x^3 + 2x + 1$$

Polinomio modulo 2 : $\bar{f}(x) = x^4 + x^3 + 1$

3 : $\bar{f}(x) = x^4 + 2x + 1$

$$f(x) \in \mathbb{Z}[x] \longrightarrow \bar{f}(x) \in \mathbb{Z}/p\mathbb{Z}[x]$$

p primo

Se $f(x)$ è riducibile (scomponibile nel prodotto di due polinomi di grado più piccolo), allora lo è anche $\bar{f}(x)$ *.

Facile : $f(x) = a(x) b(x)$

$\Downarrow$

$\bar{f}(x) = \bar{a}(x) \bar{b}(x)$

$f(x) = p x^n + \dots$ $\quad \bar{f}(x)$ ha grado $< n$.

Se per esempio $f(X)$ è "MONICO" (= primo coeff $= 1$) non ho problemi.

Esempio: $f(X) = X^3 + 2002X^2 - 8193X + 7111$ è irriducibile in $\mathbb{Z}[X]$.

Infatti, consideriamo $\bar{f}(X) \in \mathbb{Z}/2\mathbb{Z}[X]$

$$\bar{f}(X) = X^3 + X + 1$$

NON HA RADICI → È IRRIDUCIBILE (perché ha grado 3)
→ È IRRIDUCIBILE ANCHE IN $\mathbb{Z}[X]$

WARNING: Qualche volta non basta

$f(X) = X^4 + 1$ è IRRIDUCIBILE in $\mathbb{Z}[X]$
ma RIDUCIBILE in $\mathbb{Z}/p\mathbb{Z}[X]$ $\forall\, p$ primo

---

Un polinomio a coefficienti interi può avere per valori solo numeri primi?

NON COSTANTE

$f(X) \in \mathbb{Z}$ Può essere $f(n) = \text{primo}$ $\forall n \in \mathbb{Z}$?

NO: Supponiamo $f(0) = p$ primo.

Allora $f(kp)$ è multiplo di p

$x \equiv y \pmod m \Rightarrow f(x) \equiv f(y) \pmod m$

PER ESSERE PRIMO DOVREBBE ESSERE $f(kp) = (\pm)p$

→ VERO AL MASSIMO UN N° DI VOLTE $\leq 2 \cdot \deg f$

$f(X) \in \mathbb{Z}[X]$ non costante

Può succedere che l'insieme dei numeri primi p che dividono qualche valore $f(n)$ sia FINITO?

NO

DIM. ARITMETICA

$d = \deg(f)$

1° caso: supponiamo $f(0)=1$ $\qquad f(x) = a_d x^d + \dots + a_1 x + 1$

Considerando $f(n!)$:

Se $p \le n$ $\quad f(n!) =$ multiplo di p $+ 1$

$\Rightarrow$ esiste q primo $> n$ t.c. $q \mid f(n!)$

Caso generale: $f(0) = a$

Se $a = 0$ $\qquad f(x) = x\, g(x)$ $\qquad f(p) = p\, g(p)$

è divisibile per p.

Se $a \neq 0$ considero

$$h(x) = \frac{f(ax)}{a} \qquad h(0) = \frac{f(0)}{a} = 1$$

$h(n)$ ha infiniti divisori primi $\rightarrow$ $f(an)$ ha infiniti div. primi.

DIM. ANALITICA

Supponiamo per assurdo che i valori $f(n)$ siano tutti divisibili per $p_1, p_2, \dots, p_k$

Cioè, $\forall n$ si ha $\quad f(n) = \pm p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \qquad a_i \ge 0$.

Se $d = \deg f$ e $|n| \le N$

$$|f(n)| \le C N^d$$

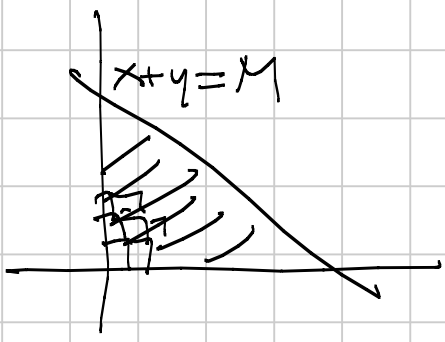
Devo avere

$$p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \le C N^d$$

$$a_1 \log p_1 + \dots + a_k \log p_k \le d \log N + \log C$$

$$(a_1 + \dots + a_k) \log 2 \le e \log N$$

$$a_1 + \dots + a_k \le \underbrace{\frac{e}{\log 2}}_{q} \log N = M$$



n° di questi $\sim \dfrac{M^k}{k!} = \dfrac{q^k (\log N)^k}{k!}$

In totale ci sono al più

$\sum_k \frac{f^k (\log N)^k}{k!}$ valori di n per cui $|f(n)| =$ uno di questi

mentre dovrebbero essere almeno tutti gli n con $|n| \le N$ cioè $2N$.

Oss. Per ogni polinomio $f(x) \in \mathbb{Z}[x]$ esistono infiniti numeri primi p tali che $\bar{f}(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ ha una radice in $\mathbb{Z}/p\mathbb{Z}$.

Principio di identità dei polinomi (in $\mathbb{Z}[x]$)
Se $f(n) = g(n)$ $\forall n$ allora $f(x) = g(x)$.
(Basta per ∞ n).

Se $\bar{f}(x) \in \mathbb{Z}/p\mathbb{Z}[x]$?

Se $\bar{f}(n) = \bar{g}(n)$ $\forall n \in \mathbb{Z}/p\mathbb{Z}$ allora $\bar{f}(x) - \bar{g}(x)$ è divisibile per $(x-n)$ $\forall n \in \mathbb{Z}/p\mathbb{Z}$
div. per $x(x-1)(x-2)\cdots(x-(p-1)) = x^p - x$
($a(x)$ → $x(x-1)\cdots(x-(p-1))$; $b(x)$ → $x^p - x$)
(anche $x^p - x$ è divisibile per (Fermat))
e $a(x), b(x)$ hanno entrambi grado p e sono monici.)

Conseguenza OGNI FUNZIONE $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ può essere espressa tramite un polinomio di grado $\le p-1$.
Quante sono le funzioni? p^p

Quante sono le funzioni che si esprimono mediante polinomi?

$f(x) \sim g(x) \iff x^p - x \mid f(x) - g(x)$

$\iff f(x) = q(x)(x^p - x) + r(x) \qquad r(x) = r'(x)$
$g(x) = q'(x)(x^p - x) + r'(x)$
$r(x) = a_0 + a_1 x + \dots + a_{p-1} x^{p-1}$

SONO p^p

TEO. p primo $\Rightarrow (\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \dots, \overline{p-1}\}$ ha un generatore

DIM. $\forall\, a \in (\mathbb{Z}/p\mathbb{Z})^\times \qquad a^{p-1} \equiv 1 \pmod p$

a è radice di $X^{p-1} - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$.

Se $\operatorname{ord}_p a = d \mid p-1$, a è radice di $X^d - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$.

Quanti possono essere gli a tali che $\operatorname{ord}_p a = d$??

A PRIORI CI SONO DUE CASI.
- NESSUNO (ZERO)
- $\phi(d)$

Supponiamo $\neq 0$ → ALLORA ALMENO 1 : α

$\alpha, \alpha^2, \dots, \alpha^d = 1$ sono tutte radici di $X^d - 1$

$\alpha^d = 1 \quad (\alpha^2)^d = (\alpha^d)^2 = 1$

cioè $\{\alpha, \alpha^2, \dots, \alpha^d\}$ è L'INSIEME DELLE RADICI

Gli el. di ordine d sono qui

e sono del tipo α^k con $(k, d) = 1$.

PER CONCLUDERE

$$\sum_{d \mid p-1} \phi(d) = p-1$$

$$\bigcup_{d \mid p-1} X_d = (\mathbb{Z}/p\mathbb{Z})^* \qquad |X_d| = \begin{cases} 0 \\ \phi(d) \end{cases}$$

X_d : el. d. ordine d

$$\Downarrow$$

$$|X_{p-1}| = \phi(p-1)$$

Esistono $\phi(p-1)$ generatori.

Esercizio facile: se $p \geq 2$ $n \geq 1$ esiste un generatore modulo p^n.

Hint. prendere a generatore modulo p e considerare $a + tp \mod p^2$

$a + tp + sp^2 \mod p^3$

$\vdots$