PREIMO 2010 – NP

Titolo nota 17/05/2010

Problema 5 Esistono infiniti p tali che $\exists\, n \in \mathbb{N}$

$$n! + 1 \equiv 0 \pmod{p} \qquad p \neq 1 \pmod{n}$$

Esperimento: $8! + 1 = 61 \cdot 661$

Idea: $n = p - k$ scegliendo bene p e k

$$n! = (p-k)! = \frac{(p-1)!}{(p-1)(p-2)\cdots(p-(k-1))} \text{ "}\equiv\text{"} \frac{-1}{(k-1)!\,(-1)^{k-1}}$$

Soluzione 1 q primo $(2q)! - 1 \equiv 3 \pmod{4}$

Prendo un $p \equiv 3 \pmod{4}$ t.c. $p \mid (2q)! - 1$

$n = p - 2q - 1$ Vediamo:

$$n! + 1 = \frac{(p-1)!}{(p-1)(p-2)\cdots(p-2q)} + 1 \text{ "}\equiv\text{"} \frac{-1}{(2q)!} + 1 \equiv 0 \pmod{p}$$

NON SCRIVERE COSÌ, ma

$$(p-1)! + (p-1)(p-2)\cdots(p-2q)$$

e dim. che $p \mid$ num.

Resta da controllare che

$n \nmid p-1$. Suppongo per assurdo che $n \mid p-1$, cioè

$p - 2q - 1 \mid p - 1$

$p - 2q - 1 \mid p - 2q - 1$

Sottraendo: $\underbrace{p - 2q - 1}_{\text{pari}} \mid 2q$

Quindi: $p - 2q - 1 = 2 \Rightarrow p = 2q + 3 \equiv 1 \pmod{4}$

$p - 2q - 1 = 2q \Rightarrow p = 4q + 1 \equiv 1 \pmod{4}$. Assurdo.

Soluzione 2 Prendo $p \mid (2q-1)! + 1$ (q forse primo)

(p primo)

$n = p - 2q$

$$n! + 1 = \frac{(p-1)!}{(p-1)(p-2)\cdots(p-(2q-1))} + 1 \overset{\cdot\cdot"}{\equiv} \frac{+1}{\underbrace{+(2q-1)!}_{\equiv -1 \ (p)}} + 1 \equiv 0 \ (p)$$

Resta da controllare che

$n \nmid p-1$. Per assurdo suppongo che $n \mid p-1$, cioè

$p \equiv 1 \ (n)$. Ma io so che $p \equiv 2q \ (n)$

quindi deve essere $2q \equiv 1 \ (n)$, cioè

$n \mid (2q-1)$ ed in particolare

$n \leq 2q-1$, cioè $p - 2q \leq 2q-1$, cioè

$p \leq 4q-1$

Ci sono 2 casi

- se $p > 4q-1$ ho trovato il p che cercavo con $n = p-2q$
- se $p \leq 4q-1$. In questo caso posso usare questo p e

$n = (2q-1)$

È ancora vero che $p \mid n! + 1$.

Resta da verificare che $n \nmid p-1$, cioè $p \not\equiv 1 \ (n)$

p di sicuro non è $\leq 2q-1$.

p " " " è $2q = n+1$

quindi la classe di p modulo n è compresa tra 2 $(2q+1)$ e $4q-1 = n + (n+1)$.

Resta il caso in cui $p = 4q-1$. Devo quindi scegliere q non primo (che non si è mai usato) ma tale che $4q-1$ non sia primo (ci sono vari modi semplici di farlo)

—o—o—

Problema 8 $\quad (y+1) \mid (x^2+1) \qquad (x+1) \mid (y^2+1)$

x e y sono P-P o D-D.

(a) Esistono soluzioni con x e y dispari : $x = 33$, $y = 217$.

Come ridurre i casi ...

Se y è dispari, allora y^2+1 ha 1 solo fattore 2 e gli altri fattori primi sono tutti $\equiv 1 \ (4)$

Quindi $x+1$ deve avere 1 solo 2 e tutti fattori $\equiv 1 \ (4)$

$x \equiv 1 \ (4)$ $\qquad x+1 = 10, 26, 34$

(b) VIETA JUMPING $\qquad x, y$ pari

$(x+1) \mid (y^2+1) \quad \Rightarrow \quad (x+1) \mid (x^2+y^2)$ ... analogo ...

$(x+1) \mid (x^2-1) \qquad (y+1) \mid (x^2+y^2)$

Claim: $(x+1)(y+1) \mid (x^2+y^2)$

Basta dimostrare che $(x+1, y+1) = 1$.

Supponga per assurdo che $p \mid (x+1) \qquad p \mid (y+1)$

$x \equiv -1 \ (p) \qquad y \equiv -1 \ (p)$

Quindi $y^2+1 \equiv 2 \ (p)$ ma $p \mid (x+1) \mid (y^2+1)$

$y^2+1 \equiv 0 \ (p)$ ma allora $p = 2$ che non va bene perché $x+1$ dispari.

Quindi: se ci fossero soluzioni, avremmo che

$(x+1)(y+1) \mid (x^2+y^2)$, cioè

$$\frac{x^2+y^2}{(x+1)(y+1)} = k \qquad \frac{\text{secondo grado}}{\sim} = \text{vieta jumping.}$$

Supponiamo che (a,b) sia una soluzione, con $\boxed{b \le a}$

Allora $\quad a^2+b^2 = k(ab+a+b+1) = kab+ka+kb+k$

$$a^2 - k(b+1)a + b^2 - kb - k = 0$$

cioè a è soluzione dell'equazione

$$x^2 - k(b+1)x + b^2 - kb - k = 0$$

Sia a_1 l'altra soluzione. Cosa so di a_1?

Fatto 1: a_1 è intero perchè somma radici $= k(b+1) \in \mathbb{Z}$

Fatto 2: $a_1 a = b^2 - kb - k < b^2$

D'altra parte per l'ipotesi iniziale $b \leq a$ ho che

$$b a_1 \leq a a_1 < b^2 \quad \text{da cui} \quad a_1 < b$$

Partendo da una coppia di sol. (a,b) con $b \leq a$ ho prodotto una coppia di sol (a_1, b) con $a_1 < b$ cioè una coppia più piccola.

Fatto 3: $a_1 \geq 0$ (basta ripensare all'eq. iniziale in forma di frazione).

Grazie ai Fatti 1, 2, 3 si arriva prima o poi ad una sol. del tipo $(x,0)$ e si vede facilmente che queste non esistono, o per lo meno c'è solo $(0,0)$ che dà $k=0$.

— o — o —

VIETA JUMPING IMO 1988-6 $\frac{x^2+y^2}{xy+1}$ = intero $\Leftrightarrow$ □

IMO 2007-5

Problema 6

(a) $n \geq 2$ $\quad p \mid 2^{2^n}+1$

Tesi: $p \equiv 1 \pmod{2^{n+2}}$.

$p \mid 2^{2^n}+1 \qquad 2^{2^n} \equiv -1 \pmod p$

$$(2^{2^n})^2 = 2^{2^{n+1}} \equiv 1 \pmod p$$

$$\operatorname{ord}_p(2) = 2^{n+1}.$$

(a primi è 2^k con $k \leq n+1$; ma non può essere più piccolo perché altrimenti $2^{2^k} \equiv 1 \Rightarrow 2^{2^n} \equiv 1$ ASSURDO

$2^n \equiv 1 \pmod p$

$\operatorname{ord}_p 2 \mid n$

RECIPROCITÀ QUADRATICA

p primo dispari $\Rightarrow$ 2 è un quadrato modulo p se e solo se $p \equiv \pm 1 \pmod 8$

Ho già dimostrato $p \equiv 1 \pmod{2^{n+1}}$

$n \geq 2 \Rightarrow p \equiv 1 \pmod 8$

$2 \equiv x^2 \pmod p$ $\qquad 2^{2^{n+1}} \equiv 1 \equiv (x^2)^{2^{n+1}} = x^{2^{n+2}}$.

$\operatorname{ord}_p x = 2^{n+2} \mid p-1$

e (a) è dimostrato.

(b) $\quad F_n = 2^{2^n}+1 \qquad F_{n+1} = 2^{2^{n+1}}+1$.

Devo trovare coppie di primi (p,q) con:

$p \mid 2^{q-1}-1 \qquad q \mid 2^{p-1}-1$

Prendo $p \mid F_n \qquad q \mid F_{n+1}$.

$q \mid 2^{2^{n+1}} + 1 \Rightarrow q \mid 2^{2^{n+2}} - 1$

So che $2^{n+2} \mid p-1$

se $a \mid b$ $\quad 2^a - 1 \mid 2^b - 1$

$b = ka \quad 2^{ka} - 1 = (2^a - 1)(2^{a(k-1)} + \dots + 2^a + 1)$

Quindi $q \mid 2^{2^{n+2}} - 1 = 2^{p-1} - 1$.

Per l'altra: $p \mid 2^{2^n} + 1 \mid 2^{2^{n+1}} - 1 \mid 2^{q-1} - 1$

(Mi basta che $2^{n+1} \mid q-1$; in realtà so che $2^{n+3} \mid q-1$).

Per ogni n, ho trovato una coppia (p, q).

Ce ne sono infiniti distinti, perché

$(F_n, F_m) = 1 \quad$ se $n \neq m$

Infatti $(m > n) \quad m = n + k$

$$2^{2^m} + 1 = 2^{2^{n+k}} + 1$$

$\boxed{X = 2^{2^n}}$

$$\frac{F_m - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{X^{2^k} - 1}{X + 1} = X^{2^{k-1}} + \dots + X + 1$$

$F_n \mid F_m - 2$ se $p \mid (F_n, F_m)$

avrei $p \mid 2$ ma gli F_n sono dispari.

Problema 7 Condizione:

$$\left| a_n^3 b_n + b_n^3 c_n + c_n^3 a_n \right| = \text{quadrato}.$$

se $a+b+c=0$ $\qquad c=-a-b$

$$a^3b+b^3c+c^3a =$$

$$\underbrace{a^3b}-ab^3-b^4-a^4-\underbrace{3a^3b}-3a^2b^2-\underbrace{ab^3}_{0}$$

$$= -(a^4+2a^3b+3a^2b^2+2ab^3+b^4)$$

$$= -(a^2+ab+b^2)^2.$$

Se riesco a partizionare gli interi in terne con somma zero, ho fatto.

$1, 0, -1$

$2, 3, -5$

$-2, -3, 5$

$4, 6, -10$

$-4, -6, 10$

...

$\sim \circ \sim$

2ª soluz.

$$|a^3b+b^3c+c^3a| = \square$$

VORREI CHE $\quad b^3c+c^3a=0$

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

$$a=-\frac{b^3}{c^2}$$

→ scelgo b multiplo di c

→ viene fissato a

$$|a^3b+b^3c+c^3a| = \left|\frac{b^{10}}{c^6}\right| = \left|\left(\frac{b^5}{c^3}\right)^2\right|$$

Fissato c, posso scegliere a e b in modo che:

- $|a^3b + b^3c + c^3a| = \square$
- a, b grandi a piacere

$c = 0 \longrightarrow a = -1, \; b = 1$

Per partizionare in terne:

- prendo il più piccolo intero non ancora coperto $\rightarrow c$
- trovo a, b enormi in modo da non averli mai coperti,

$\sim$ o $\sim$