PREIMO 2015 – TDN POMERIGGIO

Titolo nota 25/05/2015

Esercizio N5 $ab \neq \square \Rightarrow \exists n$ t.c. $(a^n-1)(b^n-1) \neq \square$.

Teo. $ab \neq \square \Rightarrow$ esiste un numero primo p dispari tale che $n = ab$ non è un quadrato modulo p.

Supposto il teo. vero, consideriamo il simbolo di Legendre modulo p:

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

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

1 fattore uno $+1$, l'altro -1.

Per simmetria supponiamo $\left(\frac{a}{p}\right) = +1 \quad \left(\frac{b}{p}\right) = -1$

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

Proviamo con l'esponente $n = \frac{p-1}{2}$

$$(a^{\frac{p-1}{2}} - 1)(b^{\frac{p-1}{2}} - 1)$$

↓ divisibile per p

$\equiv -2 \pmod p$ non divisibile per p.

Se la potenza di p che divide $a^{p-1/2}-1$ è dispari, sono a posto.

Se no, cambio n, e prendo $\frac{p-1}{2} \cdot p$

$$a^{\frac{p-1}{2}p} - 1$$

LTE: la potenza di p che divide $a^{\frac{p-1}{2}p} - 1$ è la potenza di p che divide $a^{p-1/2}-1$ $+ 1$.

(Per l'altro fattore non c'è problema: $b^{\frac{p-1}{2}p} - 1 \equiv b^{\frac{p-1}{2}} - 1 \equiv -2 \pmod p$)

PROBLEMA 6

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$$

$\forall p$ e a, b t.c. $p \mid ab-1$ allora $p \mid f(a)f(b) - 1$

Trovare f

SOLUZIONE: $f(x) = \pm x^n$

$$p \mid ab-1 \mid (ab)^n - 1$$

$$b \equiv \frac{1}{a} \pmod p$$

$$f(b) \equiv f\left(\frac{1}{a}\right) = \frac{g(a)}{a^n}$$

Traccia della dimostrazione del teorema

① Basta considerare m "liberi da quadrati"

$m = q_1 \cdots q_k$ q_i primi distinti

Caso A m dispari

Con il teo. cinese del resto, posso risolvere il sistema

$$\begin{cases} x \equiv a_1 \pmod{q_1} \\ x \equiv a_2 \pmod{q_2} \\ \dots \\ x \equiv a_n \pmod{q_k} \\ x \equiv 1 \pmod 4 \end{cases} \qquad x \equiv b \pmod{4 q_1 \cdots q_k}$$

$\left(\frac{a_1}{q_1}\right) = -1 \qquad \left(\frac{a_2}{q_2}\right) = 1, \dots, \left(\frac{a_k}{q_k}\right) = 1$

RECIPROCITA' QUADRATICA

$$\left(\frac{a_i}{q_i}\right) = \left(\frac{q_i}{a_i}\right)$$

DIRICHLET Esiste un primo $p \equiv b \pmod{4 q_1 \dots q_k}$

$$\left(\frac{p}{q_1 \cdots q_k}\right) = \left(\frac{p}{q_1}\right)\left(\frac{p}{q_2}\right) \cdots \left(\frac{p}{q_k}\right) = (-1)(+1)\cdots(+1) = -1.$$

$$\left(\frac{n}{p}\right) = \left(\frac{q_1 \cdots q_k}{p}\right) = -1$$

PROBLEMA 6

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$$

$\forall\, p$ e a, b t.c. $p \mid ab - 1$ allora $p \mid f(a) f(b) - 1$

Trovare f

SOLUZIONE: $f(x) = \pm x^n$

$$p \mid ab - 1 \mid (ab)^n - 1$$

$$b \equiv \frac{1}{a} \pmod{p}$$

$$f(b) \equiv f\left(\frac{1}{a}\right) = \frac{g(a)}{a^n}$$

dove $g(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$

se $p \mid ab - 1 \longrightarrow p \mid f(a) \cdot \frac{g(a)}{a^n} - 1$

$\to$ p| $f(a)\,g(a) - a^n$

fissato a vale per infiniti p

$\to$ $f(a)\,g(a) = a^n$

$f(x)\,g(x) - x^n = F(x)$

ha infinite radici

$\to$ $F(x) \equiv 0$

$f(x)\,g(x) = x^n$

$\to$ $f(x) = \pm x^k$

per qualche k

$f(q)$ q PRIMO

$f(q) = \pm q^k$ PER QUALCHE k

PER ASSURDO:

$f(q) \neq \pm$ POTENZA DI q

$\exists\ p \in \mathbb{P} \mid p \neq q,\ p \mid f(q)$

$f(q) = \pm p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$p_k \downarrow q$

$b \equiv q^{-1} \pmod{p}$ $\qquad q \not\equiv 0 \pmod{p}$

$p \mid q \cdot q^{-1} - 1$

$p \mid f(q)\, f(q^{-1}) - 1$

$\equiv 0 \pmod{p}$ $\square$

$f(q) = \pm q^k$ ← VERA PER OGNI q

$f(x) = a_n x^n + \dots + a_0$

$\lim_{q \to +\infty} \dfrac{f(q)}{a_n q^n} = 1$ $\qquad \lim_{q \to +\infty} \dfrac{\pm q^k}{a_n q^n} = 1$

CI SONO ∞ q

$K = n$ E $a_n = \pm 1$

$$f(q) \equiv q^K \quad o \quad f(q) \equiv -q^K$$

IL POLINOMIO $\overline{f}(x) = f(x) - x^K$

$\overline{f}(x) = 0$ HA INFINITE RADICI

$f(x) = x^K$ $\qquad$ $f(x) = -x^K$

Esercizio N7 $\qquad m^2 + 2 \cdot 3^n = m(2^{n+1} - 1)$.

L'equazione è quadratica in m $(f(m) = 0)$

Se ha due radici, x, y, si ha

$$\begin{cases} x + y = 2^{n+1} - 1 \\ xy = 2 \cdot 3^n \end{cases}$$

Per simmetria, possiamo $x = 3^a$ $\quad y = 2 \cdot 3^{n-a}$.

$f(x) = 0$ $\qquad 3^{2a} + 2 \cdot 3^n = 3^a (2^{n+1} - 1)$.

SEMPLIFICANDO, $\qquad 3^a + 2 \cdot 3^{n-a} = 2^{n+1} - 1$.

1° caso n pari.

$a \equiv n - a \pmod 2$

TUTTI E DUE PARI o TUTTI E DUE DISPARI

CONGRUENZA mod 8

P $3^a + 2\cdot 3^{n-a} \equiv 1 + 2 - 1 \equiv 3 \pmod 8$

D $3^a + 2\cdot 3^{n-a} \equiv 3 + 2 - 3 \equiv 1 \pmod 8$

NON VA BENE per $n \geq 2$

(IL CASO PARI EVENTUALE RESTANTE È $n=0$)

2° caso n dispari $(n+1$ pari$)$

$$3 \mid 2^{n+1} - 1$$

Se $3^k \| m$ scrivo $v_3(m) = k$

$$v_3(2^{n+1}-1) = v_3\left((2^{n+1}-1)(2^{n+1}+1)\right) = v_3(4^{n+1}-1)$$

LTE $\Rightarrow$ $1 + v_3(n+1)$.

(a destra)

A sinistra (perché $a \neq n-a$)

$$v_3(3^a + 2\cdot 3^{n-a}) = \min\{a, n-a\}.$$

Questo dice $\min\{a, n-a\} = 1 + v_3(n+1)$

$$= 1 + v_3\left(\frac{n+1}{2}\right)$$

Traducendo, questo significa

$$\min\{3^a, 3^{n-a}\} \leq 3\,\frac{n+1}{2}$$

$$\max\{3^a, 3^{n-a}\} = \frac{3^n}{\min \ldots} \geq \frac{3^{n-1}\cdot 2}{n+1}$$

Osserviamo infine

$$3^a + 2\cdot 3^{n-a} \geq 3^{\max\{a,\, n-a\}} + \left(2\cdot 3^{\min\{a, n-a\}}\right)$$

$$\geq \frac{3^{n-1}\cdot 2}{n+1}$$

Quest'ultimo numero è $> 2^{n+1} - 1$

se $n \geq 9$

RESTA UN NUMERO FINITO DI CASI DA VERIFICARE

($n=0$ PARI, $n=1, 3, 5, 7$ DISPARI)

$n=3 \Rightarrow m=6 \quad m=9$

$n=5 \Rightarrow m=9 \quad m=54$

GLI ALTRI NON DANNO SOLUZIONE

N8 $f: \mathbb{N}^+ \to \mathbb{N}^+$

$$n \leq f(n) \leq n + 2014$$

$$(m,n)=1 \to (f(m), f(n)) = 1.$$

$$\Downarrow \sim$$

$$p \mid f(n) \to p \mid n \quad (p \text{ PRIMO})$$

$p_1 < p_2 < \dots < p_k < \dots$ ← TUTTI I PRIMI

$f(p_1)$

$\dots$

$f(p_k)$

1. $(p_A, p_B) = 1 \to (f(p_A), f(p_B)) = 1$

I FATTORI PRIMI DI $f(p_1), \dots, f(p_k)$ SONO A DUE A DUE DISTINTI.

2. SCELGO K IN MODO CHE

$$p_K + 2015 < p_{K+1}$$

DIMOSTRIAMO CHE CI SONO INFINITI K CON QUESTA PROPRIETÀ.

PER ASSURDO: SUPPONIAMO $\exists N \mid \forall\, m > N$ VALE $p_{m+1} \leq p_m + 2015$

CONSIDERIAMO I NUMERI:

$$n!+2,\ n!+3,\ \dots,\ n!+2017$$

PER n SUFFICIENTEMENTE GRANDE

$$n > \max\{2017, p_{N+1}\}$$

$n!+K$ NON È PRIMO PERCHÉ $K \mid n!+K$ $K \neq 1, n!+K$.

IL PIÙ GRANDE PRIMO $p_z < n!+2$ E IL PIÙ PICCOLO PRIMO $p_{z+1} > n!+2017$ SONO APPUNTO CONSECUTIVI: ASSURDO POICHÉ $z > N$ E $p_{z+1} > p_z + 2015$. □

QUINDI:

ESISTONO INFINITI k TALI CHE

$$p_{k+1} > p_k + 2015.$$

PRENDO UN k CON QUESTA PROPRIETÀ.

E CONSIDERO

$f(p_1)$

...

$f(p_k)$

È POSSIBILE CHE $p_j \mid f(p_i)$ CON $j > k$, $i \le k$.

$p_j \mid f(p_i) \Rightarrow f(p_i) \ge p_j \ge p_{k+1} > p_k + 2015 \ge p_i + 2015$

CONTRO $\quad p_i \le f(p_i) \le p_i + 2015$

p_1
p_2
p_3
...
p_k

SONO TUTTI I PRIM. DA 2 A p_k

LA LORO IMMAGINE HA PRIM $\le p_k$

$f(p_i) \neq 1$. PERCHÉ $f(p_i) \ge p_i > 1$.

$\forall i \; \exists j \mid p_j \mid f(p_i)$, $j \le k$. $\quad j > k$

PERCHÉ $f(p_i) \neq 1$, $p_0 \nmid f(p_i)$

SUPPONIAMO $f(p_i)$ COMPOSTO PER QUALCHE i

$f(p_1)$

$f(p_i) = p_A^{\alpha} \cdot p_B^{\beta}$

$f(p_k)$

$\Big(f(p_x), f(p_y)\Big) = 1.$

NON HANNO FATTORI MUTUALMENTE COMUNI.

DENOTIAMO CON $\omega(n)$ IL NUMERO DI PRIMI DISTINTI DI n.

$\omega(f(p_i)) \geq 1.$

$\omega\big((f(p_1) \cdot \ldots \cdot f(p_i) \cdot \ldots \cdot f(p_k)\big) =$

$= \underbrace{\omega(f(p_1)) + \ldots +}_{\geq 1} \underbrace{\omega(f(p_i))}_{\geq 1} + \ldots + \underbrace{\omega(f(p_k))}_{\geq 1}$

$\geq k+1.$

IL PRODOTTO $f(p_1) \cdot \ldots \cdot f(p_k)$ HA $k+1$ PRIMI DISTINTI:

ASSURDO! POICHÉ $p_j \nmid f(p_i) \quad \forall j > k$

PERCIÒ POICHÉ $\exists$ INFINITI k CON LA PROPRIETÀ

$p_{k+2015} < p_{k+1}$

E $\forall l \leq k$ $f(p_l)$ È UNA POTENZA DI PRIMO

$f(p)$ È UNA POTENZA DI PRIMO $\forall p \in \mathbb{P}$.

$\forall q \in \mathbb{P}^{\text{PRIMI}} \quad \exists n \in \mathbb{N}, p \in \mathbb{P} \quad f(p) = q^n.$

VERO PERCHÉ OGNUNO DI $f(p_1), \ldots, f(p_k)$

PRENDE ESATTAMENTE OGNUNO DEI PRIMI $p_1, \dots, p_k$

SUPPONIAMO $f(p) = q^k$ ≥ 2

SUPPONIAMO $f(p^n) \neq$ POTENZA DI q.

$\exists\, r \in \mathbb{P} \mid r \mid f(p^n),\ r \neq q$ POICHÉ $r \neq 0$

$\exists\, s \in \mathbb{P} \mid f(s) = r^J \rightarrow s \neq p$

$(s, p^n) = 1 \rightarrow (f(s), f(p^n)) = (r^J, f(p^n)) \geq r$

($f(s)$: ≥ 1; MOLTIPLO DI r)

ASSURDO.

PERCIÒ $f(p^k) = q^c$. $\forall p \in \mathbb{P},\ k \in \mathbb{Z}^+$.

SUPPONIAMO CHE $\forall k$ VALGA:

$$p^k \leq f(p^k) \leq p^k + 2014$$

$$p^k \leq q^c \leq p^k + 2014$$

$$1 \leq \frac{q^c}{p^k} \leq 1 + \frac{2014}{p^k}$$

$a \leq X \leq b$

$c \leq Y \leq d$

$\frac{a}{d} \leq \frac{X}{Y} \leq \frac{b}{c}$

VALE ANCHE PER $k+1$:

$$1 \leq \frac{q^{c'}}{p^{k+1}} \leq 1 + \frac{2014}{p^{k+1}}$$

$$\left(1 + \frac{2014}{p^k}\right)^{-1} \leq \frac{q^{c'-c}}{p} \leq 1 + \frac{2014}{p^{k+1}}$$

PER k GRANDE: $\exists\, n \mid \frac{q^n}{p}$ È SEMPRE PIÙ VICINO A 1.

$$1-\lambda < \frac{q^n}{p} < 1+\lambda \quad \forall \lambda > 0.$$

ALLORA $q^n = p$ $\nearrow$ $q = p$ OK.

$\searrow$ $q^n = p$, $p \notin \mathbb{P}$

PERCIÒ $f(p) = p^k \quad \forall p \in \mathbb{P}$

$f(n)$. $\exists\, q \mid q \mid f(n)$, $q \nmid n$.

CONSIDERO $(n, q) = 1 \Rightarrow (f(q), f(n)) = 1$

$\Downarrow$

$q \mid f(q)$, $q \mid f(n)$

Problem N7

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

i) $m = 2^\alpha \cdot 3^\beta$ $\quad \alpha \leq 1$, $\beta \leq n$

ii) wlog $\boxed{m = 3^t}$ $\quad m = \frac{2 \cdot 3^n}{3^t}$

$\boxed{t, n-t \geq 3}$

$\boxed{3^2 = 2b^2 + 1}$

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

$$\boxed{3^t + 2 \cdot 3^{n-t} = 2^{n+1} - 1}$$

mod 27 $\quad LHS \equiv 0 \quad (27)$

$\rightarrow 2^{n+1} \equiv 1 \quad (27)$

$2^{18} \equiv 1 \quad (27)$

$18 \mid n+1$

$2^{n+1} \equiv 1 \quad (7)$ $\qquad 2^6 \equiv 1 \quad (7)$

$2^{18} \equiv 1 \quad (7)$

$2^{n+1} - 1 \equiv 0 \quad (19)$ $\qquad 2^{18} \equiv 1 \quad (19)$

$$3^t + 2 \cdot 3^{n-t} \equiv 0 \quad (7) \quad (19)$$

$n - t \geq t$

$$3^t(1 + 2 \cdot 3^{n-2t}) \equiv 0 \quad (7)$$

$$1 + 2 \cdot 3^{n-2t} \equiv 0 \quad (7)$$

$$3^{n-2t} \equiv 3 \quad (7)$$

$$\boxed{n - 2t \equiv 1 \quad (6)}$$

$$3^{n-2t} = 9 \quad (19) \quad \rightarrow \boxed{n - 2t \equiv 2 \quad (8)}$$