PREIMO 2016 — TdN — Pomeriggio

Titolo nota 23/05/2016

N5 $\quad (f(n), f(2^n)) = 1 \quad \forall n$

$a - b \mid f(a) - f(b)$

supp. $\exists n$ t.c. $p \mid f(2^n)$ p primo

$p \mid f(2^n + kp)$.

$x_k = 2^n + kp$

$2^{x_k} - x_k \mid f(2^{x_k}) - f(x_k)$

$p \mid 2^{x_k} - x_k \qquad 2^{2^n + kp} - 2^n - kp \equiv 0 \ (p)$

$p = 2 \longrightarrow$ ok

$p \neq 2 \qquad 2^{2^n - n + kp} \equiv 1 \ (p)$

$p - 1 \mid 2^n - n + kp \qquad p - 1 \mid 2^n - n + k$

possiamo trovare un tale k, e chiamiamo k_0

$p \mid 2^{x_{k_0}} - x_{k_0} \mid f(2^{x_{k_0}}) - f(x_{k_0})$

$p \mid f(x_{k_0}) \Longrightarrow p \mid f(2^{x_{k_0}})$ assurdo

$(f(x_{k_0}), f(2^{x_{k_0}})) = 1$

$\forall n \quad f(2^n) = \begin{cases} 1 \\ -1 \end{cases}$

$\Rightarrow$ WLOG vale infinite volte $f(2^n) = 1$

$f(x) - 1$ avrebbe infinite radici

$f(x) \equiv 1$

analogamente per -1

gli unici polinomi che soddisfano

sono $f(x) \equiv 1, -1$

N7 SIA q UN NUMERO PRIMO. DIMOSTRARE CHE ESISTE UN INTERO POSITIVO N_q TALE CHE:

- SE $K > N_q$;
- SE $qK+1$ È UN PRIMO p;

ALLORA $p \nmid 1^{q-1} + 2^{q-1} + \dots + K^{q-1}$

CONSIDERARE IL POLINOMIO f TALE CHE:

$$f(n) = \sum_{i \le n} (i)^{q-1}.$$

CONDIZIONE: p DIVIDE $f(K)$

$qk \equiv -1 \pmod{p} \rightarrow k \equiv -\frac{1}{q} \pmod{p}$

p DIVIDE $f\left(-\frac{1}{q}\right)$

È UN NUMERO A PRIORI REALE

$\Downarrow$

IN REALTÀ RAZIONALE

IL NUMERATORE DI $f\left(-\frac{1}{q}\right)$ È MULTIPLO DI OGNI p DELLA FORMA $qk-1$ A ABBASTANZA GRANDE.

$f\left(-\frac{1}{q}\right) = 0$

↖ DIPENDE SOLO DA q

LEMMA Sia $n \in \mathbb{N}$.

Th Esistono $a_0, a_1, \dots, a_n$ INTERI TALI CHE:

$$x^n = a_n \binom{x}{n} + a_{n-1} \binom{x}{n-1} + \dots + a_0 \binom{x}{0}$$

$$\binom{x}{k} = \frac{x(x-1)\dots(x-k+1)}{k!}$$

DIM.

INDUZIONE

P.B. $n = 0$ $\quad x^0 = 1 \cdot \binom{x}{0}$

PASSO INDUTTIVO:

$$x^n - n! \binom{x}{n}$$

$$\binom{x}{n} = \frac{1}{n!} x^n + c_{n-1} \cdot \frac{1}{n!} x^{n-1} + \dots + c_0 \frac{1}{n!} \cdot x^0$$

C_i INTERI: COEFFICIENTI DI

$x(x-1)(x-2)\dots(x-n+1)$

C_i INTERI $\longrightarrow$ $n!\binom{x}{n}$ A COEFFICIENTI INTERI.

$$x^n - n!\binom{x}{n} = -c_{n-1}x^{n-1} - c_{n-2}x^{n-2} - \dots - c_0 \cdot x^0$$

$\downarrow$ IPOTESI INDUTTIVA ESTESA

OGNI x^i È DELLA FORMA $d_i\binom{x}{i} + d_{i-1}\binom{x}{i-1} + \dots$

SOSTITUISCO OGNI x^i CON LA SUA FORMA COME SOMMA DI BINOMIALI. È DUNQUE OTTENGO UN'ALTRA SOMMA DI BINOMIALI.

COROLLARIO: $\binom{0}{k} + \binom{1}{k} + \dots + \binom{x}{k} = \binom{x+1}{k+1}$

PER $x \in \mathbb{N}$

ALLORA: $1^n + 2^n + 3^n + \dots + X^n =$

$$= a_n \binom{x+1}{n+1} + a_{n-1} \binom{x+1}{n} + \dots + a_0 \binom{x+1}{1}$$

DOVE GLI a_i RISPETTANO

$$x^n = a_n \binom{x}{n} + a_{n-1} \binom{x}{n-1} + \dots + a_0 \binom{x}{0}$$

X^n COME $\sum$ DI BINOMIALI $\rightarrow$ $1^n + 2^n + \dots + X^n$ COME SOMMA DI BINOMIALI

$$X^{q-1} = a_{q-1} \binom{x}{q-1} + a_{q-2} \binom{x}{q-2} + \dots + a_0 \binom{x}{0}$$

$$X^{q-1} - a_{q-1} \binom{x}{q-1} = a_{q-2} \binom{x}{q-2} + \dots + a_0 \binom{x}{0}$$

I TERMINI CON X^{q-1} SI DEVONO SEMPLIFICARE

GRADO $\leq q-2$

$$x^{q-1} - a_{q-1}\binom{x}{q-1}$$

$$\binom{x}{q-1} = \frac{1}{(q-1)!}\cdot x^{q-1} + \dots$$ ← GRADO MINORE

DEVE VALERE $x^{q-1} - a_{q-1}\cdot\frac{1}{(q-1)!}x^{q-1} = 0$

$$a_{q-1} = (q-1)!$$

$$x^{q-1} = (q-1)!\binom{x}{q-1} + a_{q-2}\binom{x}{q-2} + \dots + a_0\binom{x}{0}$$

$$1^{q-1} + 2^{q-1} + \dots + x^{q-1} = (q-1)!\binom{x+1}{q} + a_{q-2}\binom{x+1}{q-1}$$

$$+ \dots + a_0\binom{x+1}{1} = f(x)$$

$f(x)$ È A COEFFICIENTI RAZIONALI

SUPPONIAMO CHE PER INFINITI VALORI DI x $qx+1 = p$ PRIMO E $p \mid f(x)$

$f(x)$ È A COEFFICIENTI RAZIONALI.

SE p NON DIVIDE IL DENOMINATORE DI NESSUN COEFFICIENTE DI $f(x)$, ALLORA POSSIAMO TRATTARE $f(x)$ COME POLINOMIO A COEFFICIENTI MODULO p.

POSSIAMO AD ESEMPIO CONSIDERARE $f\left(\frac{1}{2}\right) \equiv$

$\equiv f\left(\frac{p+1}{2}\right) \quad (p)$

VORREMMO FARE DELLE CONGRUENZE CON DEI NUMERI RAZIONALI.

$q\,k \equiv -1 \quad (p)$. SE $p > q, k$

$k \equiv -\frac{1}{q} \quad (p)$

PERCIÒ, SE p È SUFFICIENTEMENTE GRANDE DA:

- ESSERE $> q, k$;
- NON COMPARIRE IN $f(x)$.

ALLORA p DIVIDE IL NUMERATORE DI

$f\left(-\frac{1}{q}\right)$ PERCHÉ:

$-\frac{1}{q} \in V(p) \rightarrow f\left(-\frac{1}{q}\right) \equiv f(k)\ (p)$

ORA: $f\left(-\frac{1}{q}\right)$ DIPENDE SOLO DA q.

PERÒ È DIVISO DA INFINITI PRIMI.

$f\left(-\frac{1}{q}\right) = \frac{a}{b}$ E p DIVIDE $\wedge$ PER INFINITI PRIMI $p \Rightarrow a = 0$

$f\left(-\frac{1}{q}\right) \stackrel{?}{=} 0$. SE $f\left(-\frac{1}{q}\right) \neq 0$ ABBIAMO FINITO.

$f(x) = 1^{q-1} + \dots + x^{q-1} = (q-1)!\binom{x+1}{q} + a_{q-2}\binom{x+1}{q-1} +$

$\dots + a_0\binom{x+1}{1}$

$x = -\frac{1}{q}$

$0 \stackrel{?}{=} (q-1)!\binom{-\frac{1}{q}+1}{q} + a_{q-2}\binom{-\frac{1}{q}+1}{q-1} + \dots + a_0\binom{-\frac{1}{q}+1}{1}$

$$0 \stackrel{?}{\equiv} \frac{(q-1)!}{q\,q!}\left(-\frac{1}{q}+1\right)\left(-\frac{1}{q}\right)\left(-\frac{1}{q}-1\right)\cdots\left(-\frac{1}{q}+2-q\right)+$$

$$\frac{a_{q-2}}{(q-1)!}\left(-\frac{1}{q}+1\right)\cdots\left(-\frac{1}{q}+3-q\right)+\cdots+\frac{a_0}{1!}\left(-\frac{1}{q}+1\right)$$

$$\Downarrow \text{MOLTIPLICHIAMO PER } q^{q+1}$$

$$0 \stackrel{?}{\equiv} \underbrace{\left((q-1)(-1)(-1-q)\cdots(-1+2q-q^2)\right.}_{\not\equiv 0 \,(q)}+$$

$$\frac{a_{q-2}}{(q-1)!}\cdot q^2\left(q-1\right)(-1)\cdots\left(-1+3q-q^2\right)+\Big] \equiv 0\,(q)$$

$$\frac{a_{q-3}}{(q-2)!}\,q^3(\ldots)\cdots(\ldots)+\Big] \equiv 0\,(q)$$

a_{q-3} NON HA q AL DENOMINATORE

NON HA q AL DENOMINATORE

$$+\frac{a_0}{1!}\,q^q\cdot(q-1)$$

GUARDO MODULO q

$\equiv 0\,(q)$

ASSURDO!

$$0 \stackrel{?}{\equiv} \sum \text{NUMERI MULTIPLI DI } q + \text{NON MULTIPLO DI } q$$

OVVERO NON MULTIPLO DI q.

IN6 Sol intere di $x^2+y^2 = p+1, 2p-1, \dots, p(p-7)+1$

p primo >5.

Vedere le soluzioni di $x^2+y^2 \equiv 1 \pmod p$

$-\frac{p-1}{2} \le x, y \le \frac{p-1}{2}$ $\quad -\frac{p-1}{2}, \dots, -1, 0, 1, \dots, \frac{p-1}{2}$

Se cerco x, y qui dentro ho

$$x^2+y^2 \le 2\left(\frac{p-1}{2}\right)^2 =$$

Mossa 1

Si verifica che $2\left(\frac{p-1}{2}\right)^2 \le p(p-3)+1 \quad (p \ge 5)$

$1 = x^2+y^2 \qquad x, y \in \{0, \pm 1\}$

4 sol $(0,+1)$ $(0,-1)$ $(1,0)$, $(-1,0)$

Mi aspetterebbero più di 4 soluzioni della congruenza.

Contiamo quante sono ESATTAMENTE le soluzioni

$$x^2+y^2 \equiv 1 \iff y^2 \equiv 1-x^2 \qquad (*)$$

Fissato x ha $\begin{cases} 2 \text{ sol} & \text{se } 1-x^2 \equiv \square \neq 0 \pmod p \\ 1 \text{ sol} & \text{se } 1-x^2 \equiv 0 \\ 0 \text{ sol} & \text{se } 1-x^2 \not\equiv \square \pmod p \end{cases}$

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \\ 0 \\ -1 \end{cases}$$ nei tre casi precedenti

Fissato x: n° sol. $= 1 + \left(\frac{1-x^2}{p}\right)$

Il n° TOTALE DI SOLUZIONI è

$$N = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left[1 + \left(\frac{1-x^2}{p}\right)\right].$$

Distinguo 2 casi : $p \equiv 1, 3 \pmod 4$

1° caso $p \equiv 3 \pmod 4$

Notazione N_0 è solo il termine per $x=0$

N^* tutti gli altri

$N_0 = 1 + \left(\frac{1-0}{p}\right) = 1 + \left(\frac{1}{p}\right) = 1+1 = 2$

Bigezione $x \to x^{-1} = \frac{1}{x}$

$$S = \sum_{x \neq 0} \left(\frac{1-x^2}{p}\right) = \sum_{x \neq 0} \left(\frac{1-\frac{1}{x^2}}{p}\right) = \sum_{x \neq 0} \left(\frac{\left(\frac{x^2-1}{x^2}\right)}{p}\right)$$

$$= \sum_{x \neq 0} \left(\frac{x^2-1}{p}\right) = \sum_{x \neq 0} \left(-\frac{1}{p}\right)\left(\frac{1-x^2}{p}\right) = -S$$

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

$S = 0$

$$N^* = \sum_{x \neq 0} \left(1 + \frac{(1-x^2)}{p}\right) = p - 1 + 0 = p - 1$$

$$\boxed{N = N_0 + N^* = 2 + (p-1) = p+1}$$

2° caso $p \equiv 1 \pmod 4$

In questo caso $\left(\frac{-1}{p}\right) = 1$.

Posso riscrivere N come $N = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(1 + \left(\frac{x^2-1}{p}\right)\right)$

Cambio di variabile $x \mapsto \frac{x}{a}$ $a \neq 0$

bigezione (anche delle classi diverse da zero)

$$\forall a \neq 0 \quad N = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(1 + \left(\frac{\left(\frac{x}{a}\right)^2 - 1}{p}\right)\right) = \sum \left(1 + \left(\frac{\frac{x^2-a^2}{a^2}}{p}\right)\right)$$

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

$x^2 - a^2 = (x-a)(x+a) = y(y+2a)$

Dimostrando per una altra via l'addendo ?, cosa c'entra sul resto.

$\forall a \neq 0 \quad \sum_x \left(\frac{x}{p}\right)\left(\frac{x+2a}{p}\right) = T$ (**)

il tutto vale $N = p + T$

Somma (**) $\forall a \neq 0$

$$(p-1)T = \sum_x \sum_{y \neq x} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$$

$$= \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) - \sum_x \left(\frac{x}{p}\right)\left(\frac{x}{p}\right)$$

$$= \left(\sum_x \left(\frac{x}{p}\right)\right)^2 - \sum_x \left(\frac{x}{p}\right)^2$$

$$= 0^2 - (p-1)$$

$$(p-1)T = -(p-1)$$

$$T = -1$$

$$\boxed{N = p + T = p - 1}$$

$p - 1 > 4$ ok.

$x+2a$,
$x+4a$,
$\vdots$
$x + 2(p-1)a$
sono tutte le classi $\neq x$

N8 $\quad d_1, d_2 \mid \frac{n^2+1}{2} \qquad d_1 + d_2 = n + k$

Cons. eq. del tipo

$$A\, d_1 d_2 = (d_1 + d_2 - k)^2 + 1$$

$$A\, x y = (x + y - k)^2 + 1$$

$$(x, y) \to (x, y') \to (x', y') \to (x', y'') \to \dots$$

Cerco A in modo che ci sia unica soluzione

$$(x, y) = (1, 1)$$

$$A \cdot 1 \cdot 1 = (1 + 1 - k)^2 + 1 = (k-2)^2 + 1$$

$$\underbrace{((k-2)^2+1)}_{n^2+1}\, x y = (x + y - k)^2 + 1$$

Considero l'equazione data come eq. di 2° grado nella x.

Divento

$$x^2 - [(k-1)(k-3)y + 2k]\, x + (y-k)^2 + 1 = 0$$

(x, y) sol $\Rightarrow (x', y)$ sol $\qquad$ WLOG $x \le y$

$$x' = (k-1)(k-3)y + 2k - x$$

$$x' \ge 4 \cdot 2 \cdot y + 2k - x > y$$

DISPARI.

$$(x, y') \to (x_1, y) \to (x_1, y_1) \to (x_2, y_1) \to \dots$$

Le soluzioni crescono

I numeri $x_i + y_i$ a un certo punto sono $> k$.

Pongo $n = x_i + y_i - k \qquad x_i y_i \mid n^2 + 1$

DISPARI $\qquad x_i y_i \mid \frac{n^2+1}{2}$

Le sol contient n
$d_1 = x$; $d_2 = y$,
$d_1 + d_2 = n + k$

$d_1 d_2 \mid \frac{n^2+1}{2}$

$\Rightarrow$.