Prelmo 2019 - TdN - Pomeriggio

Note Title 21/05/2019

N5 $n>1$ $\quad 2^n+1=p$ primo $\iff p \mid 3^{2^{n-1}}+1$

$\Leftarrow \quad p \mid 3^{2^{n-1}}+1 \mid (3^{2^{n-1}}+1)(3^{2^{n-1}}-1) = 3^{2^n}-1$

$3^{2^n} \equiv 1 \pmod p$

p può dividere uno solo dei due elementi $p \mid 2$ impossibile

$\operatorname{ord}_p 3 \mid 2^n$

$\operatorname{ord}_p 3 \nmid 2^{n-1} \quad \Rightarrow \quad = 2^n.$

$2^n = p-1$

$\operatorname{ord}_m a \mid \varphi(m) = m-1 \iff m$ è primo.

$\Rightarrow \quad p$ primo $\quad p \mid 3^{2^n}-1 \quad 2^n = \varphi(p)$

divide sicuramente uno fra $3^{2^{n-1}}-1$ e $3^{2^{n-1}}+1$

Quando si verifica questo? $\operatorname{ord}_p 3 \mid 2^{n-1}$

Se g è un generatore mod p

$\operatorname{ord}_p(g^i) = 2^n \quad \operatorname{ord}(g^i) \mid 2^{n-1} \iff i$ è pari.

$\iff g^i$ quadrato

$g^i = 3$

RECIPROCITÀ QUADRATICA

In questo caso dice 3 è un quadrato mod p

$\iff p \equiv 1 \pmod 3$

$p = 2^n+1 \quad n$ è ovviamente è pari

$2^n \equiv 1 \pmod 3$

$2^n + 1 \equiv 2 \pmod 3$

$\Rightarrow$ 3 NON È QUADRATO mod p

FINE.

IRQ

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \equiv \square \bmod p \quad a \neq 0 \\ -1 & a \not\equiv \square \bmod p \quad a \neq 0 \\ 0 & a = 0 \end{cases}$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$ se p, q sono primi dispari

$$\left(\frac{-1}{3}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\cdot 1} = 1$$ perché $p \equiv 1 \pmod 4$

$$\left(\frac{3}{p}\right) = 1 \iff \left(\frac{p}{3}\right) = 1$$

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases}$$

N6

lemma: $\#\{ k \in \{1, \dots p-1\} \mid \left(\frac{k}{p}\right) = \left(\frac{k+1}{p}\right) = 1 \} = \left[\frac{p}{4}\right]$.

dim: $k = x^2 \quad k+1 = y^2 \ (p)$

vogliamo trovare il $\#$ di soluzioni di

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

$$\sum_{x=0}^{p-1}\left(\frac{x^2+1}{p}\right) \equiv \sum_{x=0}^{p-1}(x^2+1)^{\frac{p-1}{2}} \quad (p)$$

$$\equiv \sum_{x=0}^{p-1} x^{p-1} + \sim x^{p-2} + \dots + 1 \quad (p)$$

$$\equiv p-1 + \sum_{x=0}^{p-1} f(x) \quad (p) \qquad \text{con deg } f \leq p-2$$

$$\equiv -1 \quad (p)$$

$$\sum_{x=0}^{p-1}\left(\frac{x^2+1}{p}\right) = -1 \qquad \left(\frac{x^2+1}{p}\right) = 1 \text{ per } \frac{p-1}{2} \text{ valori di}$$

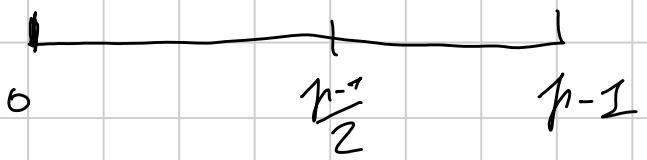
$$\text{o } \frac{p-3}{2}.$$

(occhio a $p \bmod 4$)

$$(x)^2 \equiv (-x)^2 \equiv x^2 \quad (p)$$

i valori assunti da x^2 t.c. x^2+1 è $\square \bmod p$

sono $\frac{p-1}{2} / 2 = \left\lfloor \frac{p}{4} \right\rfloor$



per assurdo in $\left[0, \frac{p-1}{2}\right]$ ci sono $\leq \frac{p}{12}$

$\Rightarrow$ in $\left(\frac{p-1}{2}, p-1\right]$ ci sono $\geq \#\mathbb{Q} - \frac{p}{12}$

$$= \frac{p-1}{2} - \frac{p}{12}$$

in $\left(\frac{p-1}{2}, p-1\right]$ ci sono $\leq \frac{p}{12}$ non residui

conto le coppie $(k, k+1) = (\square, \square)$ in $\left(\frac{p-1}{2}, p-1\right]$

- NR R R R ... R NR - - -

sono almeno $\frac{p}{2} - 2\frac{p}{12} = \frac{p}{2} - \frac{p}{6} = \frac{p}{3}$

MA in tutto l'intervallo $[0, p-1]$ ci sono $\frac{p}{4}$ coppie $(\square, \square)$

assurdo perché $\frac{p}{3} > \frac{p}{4}$

(SISTEMARE GLI OFF-BY-ONE)

N7] per assurdo $\exists n$ tali i fattori primi di b_n dividono qualche b_i per $i = 1, \dots, n-1$

$p \mid b_n$ $\exists k < n$ con $p \mid b_k$ e prendo k_0 il minimo

$v_p(b_{k_0}) = \ell$ claim: $v_p(b_n) = \ell$

$$P(b_{k_0}) = a_d b_{k_0}^d + \dots + a_2 b_{k_0}^2 + a_0 \equiv (p^{\ell+1})$$

$$\equiv a_0 \ (p^{\ell+1}) \quad \text{perché } 2\ell \geq \ell+1$$

$b_{k_0+s} \equiv b_s \ (p^{\ell+1})$ $\rightarrow$ b_i periodici di periodo k_0

$p \mid g_n \Rightarrow k_0 \mid n$ e $g_n \equiv g_{k_0} \pmod{p^{g+1}}$

$\Rightarrow \nu_p(g_n) = g$

$g_n = p_1^{e_1} \cdots p_r^{e_r} \leq \prod_{d \mid n} g_d \leq g_1 \cdots g_{\lfloor \frac{n}{2} \rfloor} \leq \left(g_{\lfloor \frac{n}{2} \rfloor}\right)^{\lfloor \frac{n}{2} \rfloor}$

$g_n = P^{(\lceil \frac{n}{2} \rceil)}\left(g_{\lfloor \frac{n}{2} \rfloor}\right)$ $\qquad P(x) \geq x^d$

$\geq g_{\lfloor \frac{n}{2} \rfloor}^{d^{\lceil \frac{n}{2} \rceil}}$

avremmo $\left(g_{\lfloor \frac{n}{2} \rfloor}\right)^{\lfloor \frac{n}{2} \rfloor} \geq g_{\lfloor \frac{n}{2} \rfloor}^{d^{\lceil \frac{n}{2} \rceil}} \iff$

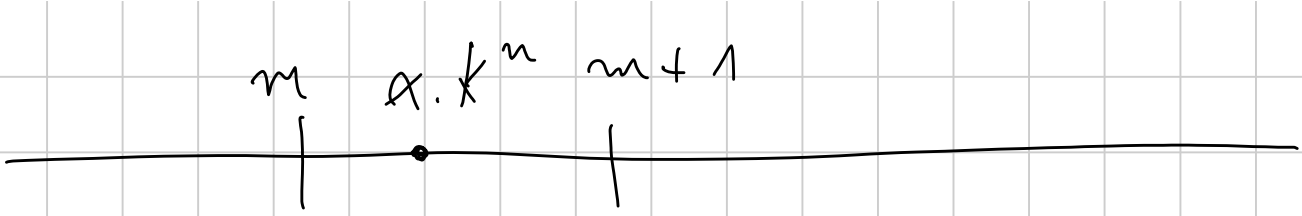
$\lfloor \frac{n}{2} \rfloor \geq d^{\lceil \frac{n}{2} \rceil}$ falsa per $d \geq 2$

NB M, K INTERI POSITIVI CON $K-1$ NON SQUAREFREE.

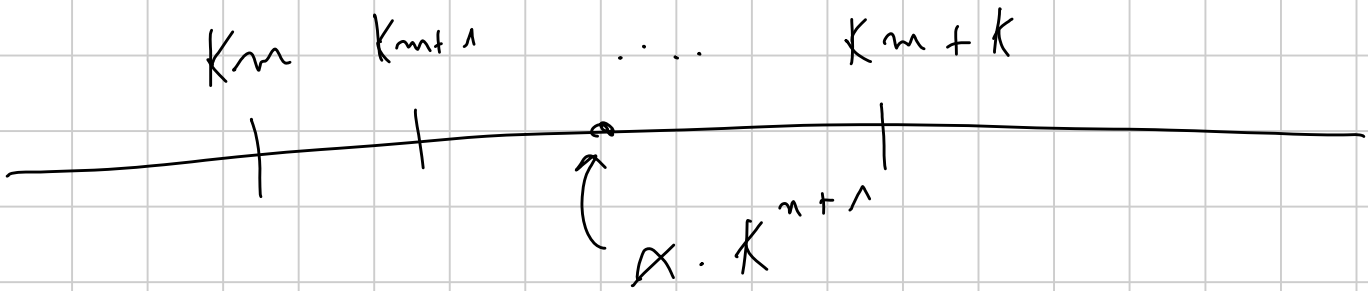
Th. ESISTE A REALE T.C.

$$\left(\lfloor A \cdot K^n \rfloor, M\right) = 1 \quad \forall n \geq 1$$

$\lfloor A \cdot K^n \rfloor$ COS'È?



$\alpha \cdot k^{n+1}$ DOVE SARÀ?



SE $\lfloor \alpha \cdot k^n \rfloor = m$ POSSIAMO MODIFICARE "DI POCO" α IN MODO TALE CHE

$$\lfloor \alpha \cdot k^{n+1} \rfloor = km + j \quad \text{CON}$$

$j \in \{0, \dots, k-1\}$ DI NOSTRA SCELTA

$$\alpha = \sum_{i=0}^{+\infty} \frac{j_i}{k^i} \quad \text{CON} \quad j_i \in \{0, \dots, k-1\}$$

$$\lfloor \alpha \cdot k^n \rfloor = j_0 \cdot k^n + j_1 \cdot k^{n-1} + \dots + j_n \cdot k^0$$

SENZA TRANNE QUANDO GLI j_i SONO DEFINITIVAMENTE $k-1$

(I.E.: $0,999\ldots = 1$)

$\lfloor 0,\bar{9} \cdot 10 \rfloor = 10 \neq 9$

M

$0 \quad 1 \quad 2 \quad \ldots \quad M-1$

$2k \quad 2k+1 \quad \ldots \quad 3k-1$

NON DEFINITIVAMENTE

$2k^2+k \quad 2k^2+k+1 \quad \ldots \quad 2k^2+2k-1$

-1

PORTROPPO NO.

$-k \quad -k+1 \quad \ldots \quad -1$

$-k \quad -k+1 \quad \ldots \quad -1$

IDEE: SCEGLIAMO X COPRIMO CON M

E VORREMMO $x \to x$ CIOÈ:

$$x \equiv kx + j \quad (M)$$

$$j \neq k-1$$

$$0 \leq j \leq k-1$$

$$\Big\} \rightarrow \quad 0 \leq j \leq k-2$$

POSSIAMO SCEGLIERE M SQUAREFREE:

$$M = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$$

$$\tilde{M} = p_1 \cdot \ldots \cdot p_n$$

I NUMERI COPRIMI CON M SONO I NUMERI COPRIMI CON $\tilde{M}$

- $kx + j \equiv x \quad (M)$
- $0 \leq j \leq k-2$ ✓
- M SQUAREFREE ✓
- $(x, M) = 1$

$$(k-1)\,x \equiv -j \quad (M)$$

$$MCD(k-1, M) = d \mid j$$

$J = d$ LO PRENDIAMO

$$(K-1)x \equiv -d \ (M)$$

$$0 \leq d = MCD(K-1, M) \leq K-1$$

SE $d = K-1 \rightarrow K-1 \mid M$

MA NON È POSSIBILE PERCHÉ M È SQUAREFREE E $K-1$ NO!

$$\Longrightarrow 0 \leq d \leq K-2$$

$$(K-1)x \equiv -d \ (M)$$

$d \mid K-1$ E $d \mid M$

E $d = MCD(K-1, M)$

$$\frac{(K-1)}{d} x \equiv -1 \left(\frac{M}{d}\right)$$

MA $\frac{(K-1)}{d}$ E $\frac{M}{d}$ SONO COPRIMI

C'È UNA SOLUZIONE $\bar{X}$. E IN PARTICOLARE

$X = \left(\bar{X} + l \cdot \frac{M}{d}\right)$ È SEMPRE SOLUZIONE:

$$(K-1)\left(\bar{X} + l \cdot \frac{M}{d}\right) \equiv$$

$$(K-1)\bar{X} + M \cdot \frac{l \cdot (K-1)}{d} \equiv -d \quad (M)$$

INTERO

$$\equiv 0 \quad (M)$$

$\left(\bar{X} + l \cdot \frac{M}{d}, M\right) = 1$ CI BASTA TROVARE l

$\left(\bar{X}, \frac{M}{d}\right) = 1$

FISSIAMO UN PRIMO p. DICO CHE $\exists\, l_p$ t.c.

$p \mid \bar{x} + l_p \cdot \frac{M}{d}$. SE PER ASSURDO

$p \mid \bar{x} + l_p \cdot \frac{M}{d} \quad \forall p \Longrightarrow$

- $p \mid \frac{M}{d}$ $\qquad$ $p \mid \bar{x}$

MA $\left(\bar{x}, \frac{M}{d}\right) = 1$

RIUSCIAMO A SCANSARE OGNI PRIMO E SE SCANSIAMO TUTTI I PRIMI DI M ABBIAMO VINTO: $M = p_1 \cdot \ldots \cdot p_k$

CI BASTA

$$\begin{cases} l \equiv l_{p_1} \pmod{p_1} \\ \ldots \\ l \equiv l_{p_k} \pmod{p_k} \end{cases} \Longrightarrow \bar{x} + l \cdot \frac{M}{d} \text{ NON È MULTIPLO DI } p_i \ \forall i$$