PreIMO 2008 NP

Titolo nota 19/05/2008

N5 $19^k \equiv 97 \quad (2^n)$ Per ogni n, esiste k tale che

Induzione: k piccoli a mano $(n = 1, 2, 3)$

$n \Rightarrow n+1$ Supponiamo che $19^k \equiv 97 \quad (2^n)$

Vediamo mod 2^{n+1}

$$19^k \equiv \begin{cases} 97 & (2^{n+1}) \quad \rightarrow \text{OK} \\ 97 + 2^n & (2^{n+1}) \quad \rightarrow \text{OCCORRE CAMBIARE } k \end{cases}$$

il nuovo k, diciamo k' sarà t.c. $19^{k'} \equiv 97 \quad (2^n)$

Quindi $k' = k + \text{multiplo di } \operatorname{ord}_{2^n}(19)$

(k': nuovo, k: vecchio)

$\operatorname{ord}_{2^n}(a) \mid 2^{n-1} = \varphi(2^n)$

(a: DISPARI)

$\operatorname{ord}_{2^n}(a) \mid 2^{n-2}$ per $n \geq 3$

mod 2^n esiste un generatore se $n = 1$ e $n = 2$

Per gli n successivi il massimo ordine moltiplicativo è 2^{n-2}

CANDIDATO PER $k' = k + 2^{n-2}$

OVVIO: $19^{k+2^{n-2}} \equiv 19^k \cdot 19^{2^{n-2}} \equiv 97 \cdot 1 \quad (2^n)$

($19^{2^{n-2}} \equiv 1$)

Hope: $19^k \cdot 19^{2^{n-2}} \equiv 97 \quad (2^{n+1})$

$$19^k = 97 + 2^n D$$

↑ dispari

$$19^{2^{n-2}} = 1 + 2^n A$$

$$19^k \cdot 19^{2^{n-2}} = (97 + 2^n D)(1 + 2^n A) = 97 + 2^n (A + D) + \text{roba} \cdot 2^{2n}$$

Basta dimostrare che A è dispari.

Per induzione

$$19^{2^{n-2}} = 1 + 2^n A_n \quad \text{↖ Dispari} \qquad \forall n \geq 3$$

$n = 3$ a mano

$n \Rightarrow n+1$

$$19^{2^{n-1}} = \left(19^{2^{n-2}}\right)^2 = (1 + 2^n A_n)^2$$

A_{n+1} dispari

$$= 1 + 2^{n+1} A_n + 2^{2n} A_n^2 = 1 + 2^{n+1} (A_n + \text{robq pari})$$

Fatto generale $\quad x \equiv 1 \pmod{p^a} \quad n > a$

$x \not\equiv 1 \pmod{p^{a+1}}$

$$\mathrm{ord}_{p^n}(x) = p^{n-a} \qquad (\text{se } p^a \neq 2)$$

$$x^p = (1 + kp^a)^p = 1 + k' p^{a+1}$$

$\uparrow$

$(k, p) = 1$

$$x^m = (1 + kp^a)^m = 1 + mkp^a + \text{roba con } p^{2a}$$

7 $\binom{2p-1}{p-1} - 1$ è divisibile per p^3

$$\binom{2p-1}{p-1} - 1 = \frac{(2p-1)(2p-2)\cdot\ldots\cdot(p+1)}{(p-1)!} - 1$$

$$= \frac{(2p-1)\cdot\ldots\cdot(p+1) - (p-1)(p-2)\cdot\ldots\cdot 2 - 1}{(p-1)!} \quad \text{div. per } p^3$$

$(p-1)!$ ↑ NO p

Tesi $\Leftrightarrow$ $p^3 \mid$ Numeratore

$$\text{Num} = (p+1)(p+2)\cdot\ldots\cdot(p+(p-1)) - (p-1)(p-2)\cdot\ldots\cdot(p-(p-1))$$

$$Q(x) = (x+1)(x+2)\cdot\ldots\cdot(x+(p-1)) - (x-1)(x-2)\cdot\ldots\cdot(x-(p-1))$$

Tesi $\Leftrightarrow$ $Q(p)$ div. per p^3

p è > 3 per ipotesi $\qquad Q(0) = 0$

$Q(x) = x\,R(x)$ GRATIS che $\quad p \mid Q(p)$

$$Q(-x) = (-x+1)(-x+2)\cdots(-x+(p-1)) - (-x-1)(-x-2)\cdots(-x-(p-1))$$

$$= (x-1)(x-2)\cdots(x-(p-1)) - (x+1)(x+2)\cdots$$

$$= -Q(x)$$

$\Rightarrow$ $Q(x)$ è DISPARI $\Rightarrow$ Q contiene solo potenze dispari di x

$$Q(x) = ax + bx^3 + cx^5 + \cdots$$

Se dimostro che $a = 0$, automaticamente $p^3 \mid Q(p)$

Quindi tesi $\Leftrightarrow$ a multiplo di p^2.

Coeff. di x in $(x+1)(x+2)\cdots(x+(p-1))$?

$= \pm$ somma di tutti i prodotti a $(p-2)$ fattori

$= (p-1)! \sum_{i=1}^{p-1} \frac{1}{i}$

Coeff. di x in $(x-1)(x-2)\cdots(x-(p-1))$ è

stessa cosa con segno cambiato. Mi riduco a

$$2(p-1)! \sum_{i=1}^{p-1} \frac{1}{i}$$

$$\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i} + \frac{1}{p-i} = \sum_{i=1}^{\frac{p-1}{2}} \frac{p}{i(p-i)} = p \underbrace{\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i(p-i)}}_{\text{Altro fattore } p}$$

Modulo p $\qquad \dfrac{1}{i(p-i)} \equiv -\dfrac{1}{i^2}$

$$\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i^2} \overset{(p)}{\equiv} \frac{1}{2} \sum_{i=1}^{p-1} \frac{1}{i^2} \equiv \frac{1}{2} \sum_{i=1}^{p-1} i^2 \equiv 0 \quad (p) \text{ se } p>3$$

Quando i varia da 1 a $\frac{p-1}{2}$, i^2 descrive tutti i residui $\square$ mod p, quindi $\frac{1}{i^2}$ fa la stessa cosa, quindi

GUADAGNO p se $p>3$

$$\sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i^2} \equiv \sum_{i=1}^{\frac{p-1}{2}} i^2 = \frac{\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right)\left(2\cdot\frac{p-1}{2}+1\right)}{6}$$

4 $q(x)$ MONICO $q(0), q(1), \dots, q(p-1)$ potenze $(p-1)$ esime distinte

Domanda: minimo grado di $q(x)$.

Un polinomio $q(x)$ con la proprietà richiesta è

$$q(x) = x^{p-1}$$

Voglio dim. che il min. grado è $p-1$

Sia $q(x)$ di grado $\leq p-2$

Riduco $q(x)$ mod p

$q(0), q(1), \dots, q(p-1)$ possono essere solo 0 oppure 1

3 CASI → tutti 0 (1)
→ tutti 1 (2)
→ un po' e un po' (3)

CASO 1

$$q(0) = q(1) = \dots = q(p-1) = 0$$

$$q(x) = x(x-1)\cdots(x-(p-1))\,r(x)$$
$$= (x^p - x)\,r(x)$$

come polinomi con coeff. (mod p)

Quindi come pol. a coeff. interi

$$q(x) = (x^p - x)\,r(x) + p\,s(x)$$

$r(x) \neq 0$ perché $q(x)$ è monico

CASO 2 stessa cosa con $q(x)-1$

CASO 3 Supponiamo che sia di grado $\leq p-2$

Lemma WC se $\deg q(x) \leq p-2$, allora

$$\sum_{i=0}^{p-1} q(i) \equiv 0 \pmod{p}$$

↑

NON POSSONO essere un po' 0 e un po' 1

Il caso 3 si pone solo se grado $q(x) \geq p-1$.

NB $q(x) = 24x+1$ è $\square$ per $x = 0, 1, 2$ $(p=3)$

(quindi monico serve!)

N6

$$1 + 4^x + 4^y = z^2$$

Soluzioni intere positive

wlog $y \geq x$

$$1 + 4^x + (2^y)^2 = z^2$$

$z > 2^y \Rightarrow z \geq 2^y + 1$

$$1 + 4^x + (2^y)^2 = z^2 \geq (2^y + 1)^2 = (2^y)^2 + 2^{y+1} + 1$$

$4^x \geq 2^{y+1}$, $2^{2x} \geq 2^{y+1} \Rightarrow$ $\boxed{2x \geq y+1}$

$z = 2m+1$

$$1 + 4^x + 4^y = 4m^2 + 4m + 1$$

$$4^x (1 + 4^{y-x}) = 4m(m+1)$$

Quindi $x \geq 1$

$$4^{x-1}\left(1+4^{y-x}\right) = m(m+1)$$

$$4^{a}\left(1+4^{b}\right) = m(m+1)$$

- **Caso $b>0$** Uno solo tra m e $m+1$ è pari, quindi

$4^a \mid m$ oppure $4^a \mid m+1$

$m = k\cdot 4^a$

$4^a\left(1+4^b\right) = k4^a\left(k4^a+1\right)$

$1+4^b = 4^a k^2 + k \geq 4^a + 1$

$b \geq a$

$(m+1) = k\cdot 4^a$

$4^a\left(1+4^b\right) = k\cdot 4^a\left(k\cdot 4^a - 1\right)$

$1+4^b = k^2 4^a - k \overset{?}{\geq} 4^a - 1$

$4^a\left(k^2-1\right) \geq k-1$ sì

$4^a(k+1) \geq 1$ sì

$4^b \geq 4^a - 2$

$b \geq a$

In ogni caso $b \geq a$, cioè $y - x \geq x - 1$, cioè $\boxed{2x \leq y+1}$

Mettendo insieme alla disug. iniziale abbiamo $y = 2x - 1$.

Queste sono tutte soluzioni

$$1 + 4^x + 4^y = 1 + 4^x + 4^{2x-1} = 1 + 2^{2x} + 2^{4x-2} =$$

$$= 1 + 2 \cdot 2^{2x-1} + \left(2^{2x-1}\right)^2$$

$$= \left(1 + 2^{2x-1}\right)^2 = z^2$$

- **Caso $b = a$** $\quad 4^a (1 + 4^b) = m(m+1) \qquad 2^{2a+1} = m(m+1)$

  potenze di 2

  soluzione $x = y = 1$ (già considerata) $\leftarrow$ $m = 1 \quad m+1 = 2$

  $a = 0$

Se $x = 0$

$$2 + 4^y = z^2$$

modulo 4 è $\equiv 2, 3$

modulo 4 è $\equiv 0, 1$