Titolo nota 09/10/2011

$\forall m \geq 0 \quad 3^{m+1} \mid (7^{3^m} - 1)$.

(Hint: induzione su m)

$m = 0$ vero, $3 \mid (7-1)$. $\longleftarrow$ passo base

Ipotesi induttiva: $3^{m+1} \mid (7^{3^m} - 1) \Rightarrow 3^{m+2} \mid \underbrace{(7^{3^{m+1}} - 1)}$

$$7^{3^m} - 1 = 3^{m+1} \cdot k$$

$$(7^{3^m} - 1)^3 = \overbrace{3^{3m+3} \cdot k^3}$$

$$= \underbrace{7^{3^{m+1}} - 1} + 3 \cdot 7^{3^m} - 3 \cdot 7^{2 \cdot 3^m}$$

$$7^{3^{m+1}} - 1 = k^3 \cdot 3^{3m+3} + 3 \cdot 7^{3^m} \underbrace{\left(7^{3^m} - 1\right)}_{}$$

Ip. ind

$$= k^3 \cdot 3^{3m+3} + 3^{m+2} \cdot h$$

$$3m + 3 \geq m + 2$$

$$3^{m+2} \mid 7^{3^{m+1}} - 1$$

$\square$

$$\nu_p(n) = \max \left\{ h \in \mathbb{N} : p^h \mid n \right\}$$

(Hint:)

(Hint: induzione ~)

$$\log_2 k \leq \nu_2(5^k - 1) \leq 3(1 + \log_2 k)$$

$(k \geq 9)$

$$h_k \doteq \nu_2(5^k - 1)$$

$$\begin{cases} h_{2k} = h_k + 1 \\ h_{2k+1} = 2 \end{cases}$$

$$5^{2k} - 1 = (5^k - 1)\underbrace{(5^k + 1)}_{\equiv 2\,(4)}$$

$$5^{2k+1} - 1 = \underbrace{(5 - 1)}_{2^2}\underbrace{(5^{2k} + 5^{2k-1} + \dots + 1)}_{\equiv 1\,(2)}$$

A^{76} $\quad 76 \cdot (d_r A)^3$

$\boxed{\lg_2 76}$

$$(A^{38})^2$$

$$A^{38} = (A^{19})^2$$

$$A^{19} = A \cdot A^{18}$$

A^9

A^8

A^4

A^2

Quali sono le ultime 2 cifre di 2^{2011} ?

Hint: congruenze, periodicità.

$$\left(\mathbb{Z}/100\mathbb{Z}\right)^* \cong \left(\mathbb{Z}/25\mathbb{Z}\right)^* \times \left(\mathbb{Z}/4\mathbb{Z}\right)^*$$ (Teorema cinese, pagina 8,9)

$$\overbrace{\left|\left(\mathbb{Z}/100\mathbb{Z}\right)^*\right|} = \varphi(100) = 40$$

$$\left|\left(\mathbb{Z}/25\mathbb{Z}\right)^*\right| = \varphi(25) = 20 \qquad \left|\left(\mathbb{Z}/4\mathbb{Z}\right)^* = \{-1, 1\}\right| = 2$$

Cauchy : $o(g) \mid o(G)$ $G = (\mathbb{Z}/25\mathbb{Z})^*$ $g = 2$

$2^{20} \equiv 1 \ (25)$

Teo Eulero

$a^{\varphi(m)} \equiv 1 \pmod m$

$(a, m) = 1$

$2^{2011} = 2^{11} = 2048$

$$\begin{cases} a \equiv 48 \ (25) \\ a \equiv 0 \ (4) \end{cases}$$

$\underline{a = 48}$ Ultime cifre di 2^{2011}