PreIMO 2012 — Teoria dei Numeri (M)

Titolo nota 22/05/2012

$\nu_p(n) \doteq \max\{h : p^h \mid n\}$

N 1. $a, m > 0$ $\quad \nu_2(n!) \equiv a \pmod m$

$m = 2^s \cdot d$ $\qquad d \equiv 1\,(2)$

$$\nu_2(n!) \equiv \begin{matrix} a \pmod{2^s} \\ a \pmod d \end{matrix}$$

$$\underbrace{\nu_2(n!) = \sum_{j=1}^{+\infty} \left\lfloor \frac{n}{2^j} \right\rfloor}_{} \longrightarrow \boxed{\begin{matrix} n - \nu_2(n!) = \text{numero di "1"} \\ (n \text{ pari}) \quad \text{nella repp binaria di } n \end{matrix}}$$

1011010
101101
10110
1011
...

$\pmod d \qquad \exists k \quad 2^k \equiv 1 \quad (d)$

n	$n - \nu_2(n!)$	$\nu_2(n!) \pmod d$
2^k	1	0

$+1 \qquad \cdot 2^k$

$-1 \qquad +2$

$\tilde{n} : \quad \nu_2(\tilde{n}!) \equiv a \ (d)$

$\tilde{n} \to 2^{kh} + \tilde{n} \longrightarrow \begin{matrix} +0 & \nu_2(\tilde{n}!) \ (d) \\ +1 & \nu_2(\tilde{n}!) \ (2^s) \end{matrix}$

$\tilde{\tilde{n}} : \quad \nu_2(\tilde{\tilde{n}}!) \equiv a \pmod m.$

Ingredienti: Th. Cinese del Resto,

$$\nu_p(n!) = \sum_{j=1}^{+\infty} \left\lfloor \frac{n}{p^j} \right\rfloor = \frac{n - (\text{somma cifre in base } p)}{p-1}$$

N 2. $m = k(k+1)$ che consiste di due blocchi decimali identici di n cifre

$n=3 \qquad \underbrace{741}\,741 = \underbrace{741}\cdot 1001$

$$m = k(k+1) = (10^n+1)\cdot A \qquad \underline{10^{n-1} < A < 10^n}$$

visto che n non è una potenza di 2

$$10^n+1 = \boxed{p\cdot q} \qquad (p,q)=1$$

$$\left(10^{2^s\cdot d}+1\right) = \left(10^{2^s}+1\right)\cdot \underbrace{(\text{robe})}$$

$$\gcd\left(10^{2^s}+1,\ 10^{2^s\cdot(d-1)} - 10^{2^s\cdot(d-2)} + \dots + (-1)^d\right)$$

$$\gcd\left(10^{2^s}+1,\ \underbrace{(-1)^{d-1} - (-1)^{d-2} + (-1)^{d-3} - \dots}\right)$$

$$\gcd\left(10^{2^s}+1,\ \text{robe}\right) \le d$$

$$\begin{cases} k_1 \equiv 0 \ (p) \\ k_1 \equiv -1 \ (q) \end{cases} \qquad k(k+1) \equiv 0 \ (10^n+1) \qquad k(k+1) = (10^n+1)\cdot A$$

$$\begin{cases} k_2 \equiv -1 \ (p) \\ k_2 \equiv 0 \ (q) \end{cases} \qquad 0 < k_1, k_2 \le 10^n$$

$$\boxed{k_1 + k_2 \equiv -1 \ (10^n+1)}$$

$$k \doteq \max(k_1,k_2) \ge 5\cdot 10^{n-1}$$

$$k(k+1) \ge 25\cdot 10^{2n-2}$$

$$\frac{k(k+1)}{10^n+1} \ge 25\cdot 10^{n-2} = \frac{1}{4}10^n$$

$m = k(k+1)$ soddisfa le richieste del problema.

almeno $2^{\omega(10^n+1)}$ soluzioni, in generale.

N3.

N. 3

$x_1 = 1 \qquad y_1 = 2$

$$x_{n+1} = 22y_n - 15x_n$$
$$y_{n+1} = 17y_n - 12x_n$$

$y_n = \frac{1}{22}(15x_n + x_{n+1}) \qquad y_{n+1} = \frac{1}{22}(15x_{n+1} + x_{n+2})$

$$x_{n+2} = 2x_{n+1} - 9x_n$$

Analogamente $\quad y_{n+2} = 2y_{n+1} - 9y_n$

$x_1 = 1 \quad x_2 = 29 \quad \rightarrow$ tutti dispari

$y_1 = 2 \quad y_2 = 22 \quad \rightarrow$ tutti $\equiv 2 \pmod 4$

infiniti termini pos. e neg.:

$$x_{n+3} = 2(2x_{n+1} - 9x_n) - 9x_{n+1} = -5x_{n+1} - 18x_n$$

$x_n, y_n \equiv 0 \pmod 7$ per $n = 1999^{1945}$?

$x_1 = 1, \quad x_2 = 29 \equiv 1 \qquad x_3 \equiv 0$

$x_4 \equiv 5 \qquad x_5 \equiv 3 \quad x_6 \equiv 3$

$x_n \equiv x_{n+1} \longrightarrow x_{n+2} \equiv 0 \quad x_{n+3} \equiv 5x_n$

$x_{n+4} \equiv 3x_n \qquad x_{n+5} \equiv 3x_n$

$x_n \equiv 0 \pmod 7 \iff n \equiv 3 \pmod 4$

$1999^{1945} \equiv 3 \pmod 4$

Per y_n è falso $(\forall n)$. Supponiamo, per assurdo, che sia vero.

$y_n \equiv 0 \pmod 7$

$y_{n-1} \equiv y_{n-2}$

$y_{n-3} \equiv 4y_{n-1}$

$y_{n-4} \equiv 0$

$A_{n+2} = c A_{n+1} + d A_n$

il suo periodo modulo p divide $|\mathbb{F}_{p^2}^*| = p^2-1$

$y_n \not\equiv 0 \ (7)$

vi basta verificare i primi 48 termini.

$$w_{n+1} = \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} -15 & 22 \\ -12 & 17 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = M w_n$$

$w_{n+2} = M^2 w_n$

Cayley-Hamilton: il poly char di $\{w_n\}_{n\in\mathbb{N}}$ è quello di M, ossia $\det(M - \lambda I)$

$\underline{w_{n+2} - c w_{n+1} - d w_n} \overset{\shortparallel}{0}$ ha polinomio char $x^2 - cx - d$

$x^2 - \mathrm{Tr}\, M \cdot x + \det M$

$x^2 - 2x + 9$ polychar di M

$w_{n+1} = M w_n$ $\qquad \boxed{M^2 - cM - dI = 0}$

$w_{n+2} = M^2 w_n$ $\qquad (M^2 - cM - dI) w_n =$

N.4 Remind.

p primo $(\neq 2)$ $\qquad n = p^r m \qquad h = p^s k \qquad r > 0$

$(m, p) = (k, p) = 1$

$$p^{r+s} \parallel (1+n)^h - 1 = (1+p^r m)^{p^s k} - 1$$

e il numero a destra è divisibile per almeno un altro primo q $(\neq p)$.

$$3^x 7^y + 1 = a^d \qquad x, y \geq 0 \quad a, d > 1$$

$\boxed{d \text{ dispari}}$

$$a^d - 1 = (a-1)(a^{d-1} + \dots + a + 1)$$

<u>1° caso</u> $\quad 3 \cdot 7 \mid a-1$

$3 \nmid d \qquad a^3 - 1 \mid a^d - 1$

$a^3 - 1$ ha dei fattori primi $\neq 3, 7$

non va bene

$7 \mid d \qquad a^7 - 1 \mid a^d - 1 \quad \to$ come sopra

<u>2° caso</u> $\quad a - 1 = 7^\beta \qquad \beta \geq 1$

La potenza di 3 non compare in $a^d - 1$

$$a^d - 1 \equiv (-1)^d - 1 \equiv -2 \pmod 3$$

Basta il ragionamento per il primo 7.

<u>3° caso</u> $\quad a - 1 = 3^\alpha \qquad \alpha \geq 1$

$a^d - 1$ NON PUÒ ESSERE una potenza di 3

L'unico ordine possibile di a mod 7 è 3.

$3 \mid d \qquad a^3 - 1 \mid a^d - 1$

Controlliamo ~~d~~ prima $a^3 - 1$

Vorremmo $\quad a^3 - 1 = 3^{\alpha+1} 7^\gamma$

Calcolo: $\quad a^3 = (1 + 3^\alpha)^3 = 1 + 3^{\alpha+1} + 3^{2\alpha+1} + 3^{3\alpha}$

Semplificando, si ha $\quad 1 + 3^\alpha + 3^{2\alpha-1} = 7^\gamma$

$7^\gamma = (1+2\cdot 3)^\gamma = 1 + 2\gamma\cdot 3 + \dots$

$\alpha = 1 \qquad 1+3+3 = 7 \qquad$ OK

$\alpha > 1 \qquad \alpha < 2\alpha - 1$ la potenza più piccola a sinistra è 3^α

$\Rightarrow \quad 3^{\alpha-1} \mid \gamma \qquad \Rightarrow \quad 3^{\alpha-1} \leq \gamma$

$7^\gamma \geq 7^{3^{\alpha-1}} \gg 1 + 3^\alpha + 3^{2\alpha-1}$ NO.

$\alpha = 1$ O.K $\qquad 4^3 - 1 = 3^2\cdot 7$

Infine ; $a-1 = 1 \qquad a = 2$

$2^d - 1 \equiv 0 \ (3)$? NO (d dispari)

$2^d - 1 \equiv 0 \ (7)$? $d = 3 \qquad 2^3 - 1 = 7$

$2^d - 1 = 7^\beta$ con $\beta > 1$?

NO, PER IL REMIND.