PREIMO 2006 N – Pom.

Titolo nota 22/05/2006

$$(a-b)^{a \cdot b} = a^b \cdot b^a \qquad a = b+K$$

$$(K)^{(b+K)b} = (b+K)^b \cdot b^{(b+K)} \qquad a = mb$$

$$[(m-1)b]^{mb^2} = (mb)^b \cdot (b)^{mb}$$

$$(m-1)^{mb} \cdot b^{mb} = m \cdot b^{m+1}$$

$$m-1 \mid b \qquad m \mid b \longrightarrow m = 2$$

$$a = 2b$$

$$(2b-b)^{2b^2} = (2b)^b \cdot b^{2b}$$

$$b^{2b^{\cancel{2}}} = (2b)^{\cancel{b}} \cdot b^{2\cancel{b}}$$

$$b^{2b} = 2b^3 \qquad b = 2 \qquad b^{2b-3} = 2$$

$$a - b = \sqrt[ab]{a^b \cdot b^a} = \sqrt[a]{a} \cdot \sqrt[b]{b}$$

$$\sqrt[n]{n} \leq 2 - \frac{1}{n}$$

$$a - b = \sqrt[a]{a} \cdot \sqrt[b]{b} < 4$$

$$a = b + 3$$

$$a = b + 2$$

$$a = b + 1$$

$$3^{b(b+3)} = (b+3)^b \cdot b^{b+3} \quad \checkmark$$

$$2^{b(b+2)} = (b+2)^b \cdot b^{b+2} \implies (4,2)$$

$$1 = (b+1)^b \cdot b^{b+1} \quad \checkmark$$

$$\sqrt[n]{n \cdot \underbrace{1 \cdot 1 \cdot 1 \cdot \ldots \cdot 1}_{n-1}} \leq \frac{n + (n-1) \cdot 1}{n} =$$

$$= \frac{2n-1}{n} = 2 - \frac{1}{n}$$

$$(a-b)^{ab} = a^b b^a$$

$a = d \cdot x$

$b = d \cdot y$

$d = (a;b) \longrightarrow (x;y) = 1$

$$d^{d^2xy}(x-y)^{d^2xy} = d^{dx+dy}x^{dy}y^{dx}$$

$$d^{dxy-x-y}(x-y)^{dxy} = x^y y^x$$

$$\cancel{(x-y)^{dxy} = x^y y^x d^{x+y-dxy}}$$

$x = y+1$

$$d^{dy^2+dy-2y-1} = y^{y+1}(y+1)^y$$

$z = dy(y+1) - y - (y+1)$

$p^\alpha \| y \qquad p^\beta \| d$

$\alpha(y+1) = \beta z$

$Z = dy^2 + dy - 2y - 1 = 1$

$dy\cancel{(y+1)} = 2\cancel{(y+1)}$

$dy = 2$

$d = 2$

$y = 1 \quad x = 2 \qquad a = 4 \quad b = 2$

$d = 1$

$y = 2 \quad x = 3 \qquad$ NO

$a, b \in N^+ \quad a^n + n \mid b^n + n \quad \forall n \in N \quad \Rightarrow a = b$

$p_1 \mid a^n + n \qquad a^n + n \equiv b^n + n \ (p_1)$

$a^n \equiv b^n \equiv 0$

$p_1 \quad a^n + n \equiv 0 \pmod{p_1} \qquad a^n \equiv b^n \equiv 0$

$p > a, b \qquad a \equiv b \ (p) \Rightarrow a = b$

$a^n + n \equiv 0 \ (p) \Rightarrow \underline{b^n + n \equiv 0 \ (p)}$

$n = k(p-1) + h$

$\underline{a^{k(p-1)+h}} + k(p-1) + h \equiv 0 \ (p)$

$$(a^k)^{p-1} \cdot a^h \equiv a^h$$

$$\downarrow$$

$$1$$

$$n = (a+1)\underbrace{(p-1)}_{\equiv -1} + 1$$

$$a^h - k + h \equiv 0 \quad (p)$$

$$a - k + 1 \equiv 0 \quad (p) \Rightarrow k \equiv a+1$$

$$k = a+1$$

$$a^n + n \equiv 0 \quad (p)$$

$$b^n + n \equiv 0 \equiv b + (a+1)(p-1) + 1 \equiv b - a - 1 + 1 \equiv b - a \quad (p)$$

$$b - a \equiv 0 \ (p)$$

$$\Downarrow$$

$$a \equiv b$$

$p \mid a^n + n$ dunque poi $p \mid b^n + n$

1ª idea

$a^n \equiv 1 \pmod{p}$

$n \equiv -1 \pmod{p}$

SI TROVA

$0 \equiv b^n + n \equiv 1 - 1 \equiv 0$

2ª idea

$$\begin{cases} a^n \equiv a \pmod{p} \\ n \equiv -a \pmod{p} \end{cases} \leftarrow \boxed{\begin{matrix} n \equiv 1 \pmod{p-1} \\ n \equiv -a \pmod{p} \end{matrix}}$$

Teo. CINESE

$0 \equiv b^n + n \equiv b - a \pmod{p}$ FINE

$p \mid q^r + 1 \qquad q \mid r^p + 1 \qquad r \mid p^q + 1$

I $\quad p \le r \le q$

$p^q \equiv -1 \quad (r)$

$p^{2q} \equiv 1 \quad (r)$

$\mathrm{ord}_r\, p \mid 2q$ — 1, 2, q, $2q$

$\mathrm{ord}_r\, p \mid (r-1)$

① $2q \Rightarrow 2q \mid (r-1)$ NO

② $q \Rightarrow q \mid (r-1)$ NO

③ $1 \Rightarrow p \equiv 1 \quad (r) \Rightarrow r \mid p-1$

④ $2 \quad (p-1)(p+1) \equiv 0 \quad (r) \Rightarrow r \mid (p+1) \qquad r = p+1$

$q \mid 10$

$p = 2$

$r = 3$

$p \le q \le r$

$p^q \equiv -1 \quad (r)$

$p^{2q} \equiv 1 \quad (r)$

$\mathrm{ord}_r\, p \mid 2q$

$\mathrm{ord}_r\, p \mid (r-1)$

1. $1 \Rightarrow p \equiv 1 \quad (r) \qquad r \mid (p-1)$
2. $2 \Rightarrow p \equiv -1 \quad (r) \qquad r \mid p+1 \qquad r = p+1$
3. q
4. $2q \Rightarrow 2q \mid (r-1) \qquad \frac{r-1}{2q} \qquad r = kq+1$

$q \mid r^p + 1 \qquad q \mid (kq+1)^p + 1 \qquad q \mid 2$

$$f(x)\,h(x) + g(x)\cdot s(x) = k$$

$p \mid f(x)$ $\qquad p_1, \dots p_n$

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \dots + a_1 x + a_0$$

$$f(a_0^2 p) = \dots \quad + a_1 a_0^2 p + a_0$$ $\qquad P = P_1 \cdots P_M$

$$= a_0 \left(\dots + a_1 a_0 P + 1 \right)$$

$$f(a_0^m P) = a_0 \left(\underbrace{\dots}_{a_0 P} \quad +1 \right)$$ $\qquad a_0 \quad -a_0$

$$g(x) = f(x) + a_0$$

$$\frac{f(a_0 x)}{a_0} = h(x) \qquad (h(0) = 1)$$

$1 \le x \le N$ $\qquad$ $f(x) = a_n x^n + \dots$

$|f(x)| \le C N^n$ $\qquad$ $\to$ almeno $\frac{N}{n}$ valori distinti

$p_1, \dots, p_k$ $\qquad$ $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$$(\alpha_1 + \dots + \alpha_k) \log 2 \le \alpha_1 \log p_1 + \dots + \alpha_k \log p_k \le n \log N + c_1$$

$$\alpha_1 + \dots + \alpha_k \le \frac{n \log N + c_1}{\log 2} \sim n$$

$$\le (n+1)^k$$