WC 2011 - Teoria dei Numeri

Titolo nota 28/01/2011

Shift $\longleftrightarrow$ multiplo n

S = somma cifre

$$S\underbrace{(111\ldots11)}_{\frac{10^{16}-1}{9}} = n \cdot (1+2+\ldots+16)$$

$9n$ è uno shift $\Rightarrow$ $9 \mid S$

$$n = S/9 \cdot (10^{16}-1)\frac{1}{8\cdot 17}$$

$$n = j \cdot \left(\frac{10^{16}-1}{17}\right)$$

$j \geq 2 \Rightarrow n \geq 10^{15}$

No

$10n$ avrebbe 17 cifre

Mod $10^{16}-1$

SHIFT = MOLTIPLICARE PER 10

$$10^k n \equiv j \cdot n \pmod{10^{16}-1}$$

$\Updownarrow$

$$10^k \equiv j \pmod{\tfrac{10^{16}-1}{n}}$$

$\frac{1}{17} = 0,\overline{\quad\quad}$

1ª cifra decimale $\left[\frac{10}{17}\right]$

2ª cifra " $\left[\frac{100}{17}\right]$ $\quad 100 = 5 \cdot 17 + 15$

$10^i \equiv r \quad \left[\frac{10r}{17}\right]$

$\frac{1}{17} = 0,\overline{a_1 \dots a_{16}}$ $\quad A = a_1 \dots a_{16}$

$A_3 = a_3 a_4 \dots a_{16} a_1 a_2$

$\frac{10^{16}}{17} = A + \frac{1}{17}$

$\frac{1}{17} = 0, a_1 a_2 \underline{\quad A_3 \quad}$

$a_1 a_2 = \left[\frac{100}{17}\right]$ $\quad 100 \equiv 15 \pmod{17}$

$\frac{15 \cdot 10^{16}}{17} = A_3 + \frac{15}{17}$

$A_i = \left[\frac{r_i \cdot 10^6}{17}\right]$

$A = A_1$ $\quad \frac{10^{16}}{17} = A_1 + \frac{1}{17}$

$\frac{r\,10^{16}}{17} = r A_1 + \frac{r}{17}$

$\left[\frac{r\,10^6}{17}\right] = r A_1$

PROBLEMA 2)

IL PIÙ PICCOLO PRIMO!

q IL PIÙ PICCOLO CHE DIVIDE

ALMENO UN n_i PER QUALCHE $i \in \{1, \dots, k\}$

$q \mid n_i$ $\quad$ $n_i \mid p^{n_{i-1}} - 1$

$q \mid p^{n_{i-1}} - 1$

$\operatorname{ord}_q(p) \mid n_{i-1}$

$\mid q-1$

$\operatorname{ord}_q(p) \mid (n_{i-1}, q-1)$

FATTORI PRIMI DI $q-1$ SONO $< q$

FATTORI PRIMI DI $n_{i-1} \geq q$

$\operatorname{ord}_q(p) = 1$ $\quad$ $q \mid p-1$!

2 NON È NICE! $\quad$ $p-1 \geq 1$ $\quad$ $q \mid p-1$ è impossibile

$n_1 = p-1$ $\quad$ $n_2 \mid p^{p-1} - 1$

1) $\exists\, q$ TALE CHE $\operatorname{ord}_q(p) = p-1$

SE $p \geq 5$

$p^{p-1}-1$ CHE DIVISORI HA?

$p^{d}-1 \mid p^{p-1}-1 \qquad \forall d \mid p-1$

CI SONO DEI FATTORI q TALI CHE:

$q \mid p^{p-1}-1$ MA $q \nmid p^{d}-1 \quad \forall d \mid p-1 \quad d < p-1$

$p \geq 5$ È NICE?

$n_1 = p-1$ PQ: $\mathrm{mcd}_q(p) = p-1$

$q^a \,\|\, p^{p-1}-1 \qquad n_2 = q^a$

$q \equiv 1 \pmod{p-1} \Rightarrow n_2 > p-1$

$n_1 \mid p^{n_2}-1 \qquad p \equiv 1 \pmod{n_1}$

$p^{n_2} \equiv 1 \pmod{n_1}$

TUTTI I FATTORI PRIMI DI n_2 SONO $> p-1$

PRESO $r \mid p-1 \qquad v_r(p-1) = v_r(p^{n_2}-1)$.

$n-1 \qquad n^k-1 \qquad r \mid n$

se $r \mid k \qquad v_r(n^k-1) > v_r(n-1) \qquad \forall r \mid n-1$

se $r \nmid k \qquad v_r(n^k-1) = v_r(n-1)$

$\left(\frac{p^{n_2}-1}{p-1}, p-1\right) = 1$

$n_1 = p-1 \qquad n_2 = q^k$ SODDISFANO LE RICHIESTE!

2) $n_1 = p-1$ r IL PIÙ GRANDE FATTORE PRIMO DI $p-1$

$$\left(\frac{p^r-1}{p-1}, p-1\right) = \begin{matrix} 1 \text{ O } r \\ \text{DISP} \end{matrix} \qquad r \mid p-1 \text{ E' } r$$

$$\left(\frac{p^r-1}{r(p-1)}, p-1\right) = 1$$

SE $r=2$ $\quad p = 2^n + 1$

$$\left(\frac{p+1}{2}, p-1\right) = 1$$ FRANNE SE $p \equiv 3 \ (4)$ CIOÈ $p=3$

$$n_2 = \frac{p^r-1}{r(p-1)}$$

$$n_2 \mid p^r - 1 \mid p^{p-1} - 1$$

$$n_1 \mid p^{n_2} - 1$$

$$(n_2, p-1) = 1$$

COME SOPRA $\left(\frac{p^{n_2}-1}{p-1}, p-1\right) = 1$

$$\left(\frac{p^{p-1}-1}{n_2}, n_2\right) = 1$$

$$\left(\frac{p^{p-1}-1}{p^2-1} \cdot \frac{p^2-1}{n_2}, n_2 \right) = 1$$

$$\left(\frac{p^{p-1}-1}{p^2-1} \cdot 2\cdot(p-1), n_2 \right) = 1 \quad \text{HOPE}$$

$(2, n_2) = 1 \qquad 2 \nmid n_2 \qquad n_2 = \frac{p^2-1}{2(p-1)}$

p^2-1 HA SOLO UN FATTORE 2 IN PIÙ DI $p-1$

$(p-1, n_2) = 1$

$\forall\, q \mid p-1 \qquad q$ PRIMO $q \neq 2$

$v_q(p^2-1) = v_q(p-1) \Rightarrow q \nmid n_2$

$$\left(\frac{p^{p-1}-1}{p^2-1}, n_2 \right) = \qquad q \mid \frac{p^{p-1}-1}{p^2-1}$$

e $q \mid n_2$

$q \mid n_2 \Rightarrow q \mid p^2-1$

$p^2 \equiv 1 \pmod q$

e $v_q\left((p^2)^{\frac{p-1}{2}}-1\right) > v_q(p^2-1) \Rightarrow q \mid \frac{p-1}{2}$

$\Pi \nmid \quad (p-1, n_2| = 1 \quad \Rightarrow q \mid \frac{p-1}{2} \Rightarrow q \nmid n_2$!

$$\left(\frac{p^{p-1}-1}{n_2}, n_2\right) = 1$$

$$p-1 \geq \frac{p+1}{2}$$

$$\frac{p^n-1}{n(p-1)} \geq \frac{p+1}{2} \quad ?$$

$$n=2 \qquad \frac{p^2-1}{2(p-1)} = \frac{p+1}{2}$$

$$n>2$$

$$\frac{p^n-1}{p-1} \geq (p+1)\cdot\frac{n}{2}$$

$$1+\ldots+p^{n-1} \geq (p+1)\frac{n}{2}$$

$$\geq$$

$$p+\ldots+p^{n-1} \geq p\cdot(n-1) \geq \frac{p+1}{2}\cdot n \qquad \square$$

$p \geq 5$

$p=3$

$n_1=2 \qquad n_2 \mid p^2-1=8 \qquad \left(\frac{8}{n_2}, n_2\right)=1$

$n_2=8$

$n_3 \mid 3^8 - 1 = (3^4-1)(3^4+1)$ $\qquad 3^4+1 = 82$

$n_3 = 41$ $\qquad \left(41, \frac{(3^4-1)(3^4+1)}{41}\right) = 1$

$n_1 \mid 3^{41}-1 \qquad 2 \mid 3^{41}-1$

$\left(\frac{3^{41}-1}{2}, 2\right) = 1 \qquad 3^{41} \equiv (-1)^{41} \equiv -1 \quad (4)$

$3^{41}-1 \equiv 2 \quad (4)$

$\frac{3^{41}-1}{2}$ è DISPARI

PROBLEMA 3)

(CINA MO n° 6)

$(n+1)a_1^n + n a_2^n + (n-1)a_3^n \mid (n+1)b_1^n + n b_2^n + (n-1)b_3^n$

$\forall n \in \mathbb{N} \Rightarrow (b_1, b_2, b_3) = (ka_1, ka_2, ka_3)$

$p \mid (n+1)a_1^n + n a_2^n + (n-1)a_3^n \Rightarrow$

$p \mid (n+1)b_1^n + n b_2^n + (n-1)b_3^n$

VOGLIO IMPORRE LA PRIMA DIVISIBILITÀ!

$n = kp$

$\Rightarrow a_1^{kp} - a_3^{kp} \equiv a_1^k - a_3^k$

$a_1^k \equiv a_3^k \ (p) \Rightarrow b_1^k \equiv b_3^k \ (p)$

$b_1 = a_1^2 \quad b_3 = a_3^2$ è RISP. MA NON VALE LA TESI!

$(n+1)a_1^n$ MOD p

$(n+1)$ MOD p DIPENDE SOLO DA n MOD p

LA CONGRUENZA DI a_1^n MOD p DIPENDE DA n (MOD $p-1$)

AL POSTO DI n, SCRIVIAMO LA CONDIZIONE CON $n+K(P-1)$

$$(n+K(P-1)+1)\,a_1^{n+K(P-1)} + (n+K(P-1))\,a_2^{n+K(P-1)} + (n+K(P-1)-1)\,a_3^{n+K(P-1)} \mid \dots$$

LA SUA CONGRUENZA MOD P ?

$P > \max\left(a_1^n + a_2^n + a_3^n,\ b_1^n + b_2^n + b_3^n\right)$

MA $a_1^{K(P-1)} \equiv 1 \pmod P$

$$(n+1-K)\,a_1^n + (n-K)\,a_2^n + (n-K-1)\,a_3^n \pmod P$$

$P \mid \dots$ VUOL DIRE $K \in \mathbb{N}$ T.C.

$$(n+1)\,a_1^n + n\cdot a_2^n + (n-1)\,a_3^n \equiv K\left(a_1^n + a_2^n + a_3^n\right) \quad (P)$$

$P > a_1^n + a_2^n + a_3^n \Longrightarrow$

$$K \equiv \frac{(n+1)\,a_1^n + n\,a_2^n + (n-1)\,a_3^n}{a_1^n + a_2^n + a_3^n} \quad (P)$$

$\Downarrow$

$P \mid (n+K(P-1)+1)\,b_1^{n+K(P-1)} + \dots$

$\Downarrow$

$$(n+1)\,b_1^n + n\cdot b_2^n + (n-1)\,b_3^n \equiv K\left(b_1^n + b_2^n + b_3^n\right) \quad (P)$$

$$K \cdot (a_1^n + a_2^n + a_3^n)\left[(n+1)\,b_1^n + n\,b_2^n + (n-1)\,b_3^n\right] =$$

$$K\,(b_1^n + b_2^n + b_3^n)\left[(n+1)\,a_1^n + n\,a_2^n + (n-1)\,a_3^n\right] \quad (\text{mod } p)$$

$$p > (n+1)\,b_1^n + n\,b_2^n + (n-1)\,b_3^n \Rightarrow K \neq 0 \quad (p)$$

LA CONGRUENZA VALE $\forall p > M$

$\Rightarrow$ VALE CON INTERI!

$$(a_1^n + a_2^n + a_3^n)\left[(n+1)\,b_1^n + n\,b_2^n + (n-1)\,b_3^n\right] =$$

$$(b_1^n + b_2^n + b_3^n)\left[(n+1)\,a_1^n + n\,a_2^n + (n-1)\,a_3^n\right] = 0$$

$\forall n \in \mathbb{N}$

$$-a_1^n b_2^n + a_2^n b_1^n + 2a_3^n b_1^n - 2b_1^n a_2^n + b_2^n a_3^n - b_3^n a_2^n$$

$$= 0 \qquad \forall n$$

$$\sum_{i=1}^{\ell} K_i \cdot m_i^n = 0 \qquad \forall n \in \mathbb{N} \qquad m_i \neq m_j \ \forall i \neq j$$

$$\Rightarrow \forall n \quad K_i = 0 \qquad m_n \in \mathbb{R}^+$$

$$m_1 < m_2 < \dots < m_\ell$$

$$\sum_{i=1}^{l} K_i \left(\frac{m_i}{m_l}\right)^n = 0$$

$$K_l + \boxed{\sum_{i=1}^{l-1} K_i \left(\frac{m_i}{m_l}\right)^n} = 0 \qquad \frac{m_i}{m_l} < 1$$

DIVENTA PICCOLA A PIACERE PER n ABB. GRANDE

QUINDI, $K_l = 0$ QUINDI SON TUTTI 0

$$\underline{(b_2 a_1)^n} + 2\underline{(b_3 a_1)^n} + (b_3 a_2)^n - \underline{(a_2 b_1)^n} \underline{-2(a_3 b_1)^n} - \underline{(b_3 b_2)^n} = 0$$

$b_3 a_1$ A CHI PUÒ ESSERE ACCOPPIATO?

PRIMA POSS.) LO ABBINO A $-2\cdot(a_3 b_1)^n$

$$b_3 a_1 = a_3 b_1 \qquad \frac{a_1}{a_3} = \frac{b_1}{b_3}$$

$$b_2 a_1 = a_2 b_1 \qquad \frac{a_1}{a_2} = \frac{b_1}{b_2}$$

$$\boxed{\frac{a_1}{b_1} = \frac{a_3}{b_3} \qquad \frac{a_1}{b_1} = \frac{a_2}{b_2}}$$

$$(b_1, b_2, b_3) = K(a_1, a_2, a_3)$$

$K \in \mathbb{Q}$

$K \in \mathbb{N}^*$

$b_2 a_1 = a_3 b_2$ IMPOSSIBILE! GLI a_i SIANO DISTINTI

$$(b_2 a_1)^n + 2(b_3 a_1)^n + (b_3 a_2)^n - (a_2 b_1)^n - 2(a_3 b_1)^n - (a_3 b_2)^n = 0$$

$$b_3 a_1 = a_2 b_1 \qquad \boxed{b_3 a_1 = a_3 b_2}$$

$$b_2 a_1 = b_3 a_2 = a_3 b_1$$

$$\frac{a_1}{a_2} = \frac{b_1}{b_3} \qquad \frac{a_1}{a_2} = \frac{b_3}{b_2} \qquad \frac{b_1}{b_3} = \frac{b_3}{b_2}$$

$$\frac{a_1}{a_3} = \frac{b_2}{b_3} \qquad \frac{a_1}{a_3} = \frac{b_1}{b_2} \qquad \frac{b_2}{b_3} = \frac{b_1}{b_2}$$

$$b_1 b_2 = b_3^2 \qquad b_2^2 = b_1 b_3$$

$$b_2 a_1 = b_3 a_2 = b_1 a_3$$

$$b_2 a_3 = b_3 a_1 = b_1 a_2$$

$$\frac{a_1}{a_3} = \frac{a_2}{a_1} = \frac{a_3}{a_2} \qquad \frac{a_1}{a_3} \cdot \frac{a_2}{a_1} \cdot \frac{a_3}{a_2} = 1.$$

$$(a_2 b_1)^n + 2(a_3 b_1)^n + (a_3 b_2)^n = (a_1 b_2)^n + 2(a_1 b_3)^n + (a_2 b_3)^n$$

$$(a_3 b_1)^n + (a_3 b_2)^n \qquad (a_1 b_3)^n + (a_1 b_3)^n$$

$$x_1^n + x_2^n + x_3^n + x_4^n = y_1^n + y_2^n + y_3^n + y_4^n$$

$\Rightarrow \quad \{x_1, x_2, x_3, x_4\} = \{y_1, y_2, y_3, y_4\}$

$s_0, s_1, \ldots, s_n$ funzioni simmetriche elementari

$\phi_0, \phi_1, \ldots, \phi_n$ "power sums"

(Sn n elementi)

$s_0 = 1 \qquad \phi_0 = n$

$$s_0 \phi_n - s_1 \phi_{n-1} + s_2 \phi_{n-2} \qquad \pm s_n \phi_0 = 0$$