WC 2009 - TEORIA DEI NUMERI

Titolo nota 20/01/2010

4) $\prod_{1 \le i < j \le n} \frac{X_j - X_i}{j-i}$

CONTIAMO CON CHE ESPONENTE p DIVIDE NUMERATORE

a_k = il num di fattori del num. multipli di p^k. $v_p\left(\prod (X_j - X_i)\right) = \sum_{i=1}^{\infty} a_i$.

1) per induzione.

2) Fissato k, avrò p^k classi di resto. Detto b_i il numero di elementi $x_j \equiv i \pmod{p^k}$,

$$a_k = \sum_{i=2}^{p^k} \binom{b_i}{2} = \sum_{i=2}^{p^k} \frac{b_i^2 - b_i}{2} = \frac{\sum b_i^2}{2} - \frac{\sum b_i}{2} = \frac{n}{2}$$

$\sum b_i = n$

è minimo nel caso in cui i fattori sono ben distribuiti.

$|b_i - b_j| \le 1$ $\quad b_n \ge b_j + 2$ $\quad v_p\left(\prod \frac{x_j - x_i}{j-i}\right) \ge 0$

---

2) LEMMA: SE, DATO $P(X_1, \dots, X_n)$ DI GRADO d_i NELLA VARIABILE X_i, HO, PER OGNI n-UPLA CON $0 \le X_i \le d_i$, CHE' $P(X_1, \dots, X_n)$ E' INTERO, ALLORA $P(X_1, \dots, X_n)$ E' INTERO $\forall X_i \in \mathbb{Z}$.

- CAMBIARE BASE È SCRIVERE p NON COME $\sum a \prod x_i^{k_i}$, MA COME $\sum a \prod \binom{x_i}{k_i}$ $\quad x_i = 0$, CONTANO SOLO I TERMINI DI TIPO $\binom{x_i}{0}$ ..

- $q(x_1, \dots, x_n) = p(x_1+1, \dots, x_n) - p(x_1, \dots, x_n)$

Il GRADO IN x_1 È DIMINUITO. q È INTERO PER $0 \le x_1 \le d_1 - 1$ QUINDI PER HP INDUTTIVA È SEMPRE INTERO.

WLOG $x > 0$

$p(x, x_2, \dots, x_n)$ È SEMPRE INTERO, CON x INTERO.

$$p(x, x_2, \dots, x_n) = \sum_{n=0}^{x-1} \left(p(n+1, x_2, \dots, x_n) - p(n, x_2, \dots, x_n) \right) + p(0, x_2, \dots, x_n)$$

(INT. ; INT.)

$$p(x_1, \dots, x_n) := \prod \frac{(x_j - x_i)}{j - i}$$

$0 \le x_i \le d_i \iff 1 \le x_i \le d_i + 1$

$d_i = n - 1, \quad 1 \le x_i \le n$ ← SE È INTERO QUI, È INTERO SEMPRE.

SE $\exists i \ne j : x_i = x_j$, $p(x_1, \dots, x_n) = 0$

ALTRIMENTI $x_i : \{1, \dots, n\} \to \{1, \dots, n\}$

$$\prod \frac{(x_j - x_i)}{j - i} = \pm 1 \to \operatorname{sgn}(\sigma) \quad (-1)^{I(\sigma)}$$

VANDERMONDE

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots \\ \binom{x_1}{1} & \binom{x_2}{1} & \dots \\ \binom{x_1}{2} & \binom{x_2}{2} & \dots \\ \vdots & \vdots \end{pmatrix}$$

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}$$

$\det(\Pi) = P(X_1, \dots, X_n)$

SE $X_i = X_j$? $\quad P(X_1, \dots, X_n, \dots, X_j, \dots, X_n) = 0$

QUINDI $\prod (X_j - X_i) \mid P$ MA $P = K \prod (X_j - X_i)$

$\deg \prod (X_j - X_i) = \deg(P)$. PER TROVARE K, BASTA CONSIDERARE UN TERMINE.

$X_1^0 \cdot X_2^1 \cdot X_3^2 \cdots X_n^{n-1}$

$$K = \prod_{i=1}^{n} \frac{1}{(i-1)!} = \prod_{1 \le i < j \le n} \frac{1}{(j-i)}$$

$$\det(\Pi) = \prod \frac{(X_j - X_i)}{j-i}$$

È INTERO $\quad$ È INTERO

$Q_{ij} = P_{j-1}(X_i)$ CONTA SOLO IL COEFF. DIR. DI P_{j-1}

PRENDO $\binom{X}{k}$

5) QUANDO $\frac{2^{p-1}-1}{p}$ È QUADRATO?

$p \neq 2$ È INTERO

$\frac{(2^{\frac{p-1}{2}}-1)(2^{\frac{p-1}{2}}+1)}{p} = a^2$ $\quad p \mid 2^{\frac{p-1}{2}}+1$

ALLORA $2^{\frac{p-1}{2}}-1 = c^2$ $\quad \frac{p-1}{2} \geq 2$ $\quad p \geq 5$

$(2^{\frac{p-1}{2}}-1)\left(\frac{2^{\frac{p-1}{2}}+1}{p}\right) = a^2$

$p \mid 2^{\frac{p-1}{2}}-1$, ALLORA $2^{\frac{p-1}{2}}+1 = c^2$ $\quad 2^{\frac{p-1}{2}} = (c-1)(c+1)$

UNO È DIV ESATTAMENTE PER 2.

$a \cdot b = 2^n$ $\quad a \mid b \vee b \mid a$

$p > 7$ $\quad c-1 \mid c+1$ $\quad p = 7$ NO SOL. $\quad c-1 \mid 2$

NO CORRIS.

$\frac{(11^{\frac{p-1}{2}}-1)(11^{\frac{p-1}{2}}+1)}{p}$

2 CASI: $\frac{11^{\frac{p-1}{2}}+1}{p} = 2c^2 \vee 11^{\frac{p-1}{2}}+1 = 2c^2$

$\left(\frac{2}{11}\right) = -1$ $\quad 2 \equiv -9 \pmod{11}$ $\quad 2 \equiv \left(\frac{1}{c}\right)^2$

$\left(\frac{11}{p}\right)\left(\frac{p}{11}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{p-1}{2}}$

a non q. $\iff$ a un non quad

$\frac{11^{\frac{p-1}{2}}+1}{p} = 2c^2$ $\quad \left(\frac{11}{p}\right) = -1$ $\quad \left(\frac{p}{11}\right) = -1$ $\quad$ PARI

$\frac{p-1}{2}$ PARI $\Rightarrow$:) $\qquad (11^{\frac{p-1}{2}}-1) = (11^{\frac{p-1}{4}}-1)(11^{\frac{p-1}{4}}+1)$

$11^{\frac{p-1}{2}} - 1 = 2c^2$ MOD 3 $\quad \frac{p-1}{2}$ È PARI

$11^{\frac{p-1}{4}} + 1 = x^2 \qquad 11^{\frac{p-1}{4}} = (x-1)(x+1)$ NO

$11^{\frac{p-1}{4}} - 1 = y^2 \qquad 11 \mid y^2+1$ $\quad (-1)$ NO RES MOD 11

$\frac{(7^{\frac{p-1}{2}}-1)(7^{\frac{p-1}{2}}+1)}{p} \qquad \left(\frac{2}{7}\right) = 1 \qquad 2 \equiv 9$

4 CASI: $\quad 7^{\frac{p-1}{2}} - 1 = 2p \cdot c^2 \quad \vee \quad$ ~~$7^{\frac{p-1}{2}} - 1 = 2c^2$~~ NO

$7^{\frac{p-1}{2}} + 1 = 2d^2$

$-1 \equiv 2c^2 \equiv (3c)^2 \pmod 7$

$p=3$ È SOL

$7 \equiv 1 \ (3) \qquad 3 \mid 7^{p-1} - 1$

Se $3 \nmid p-1$, $\quad 3 \parallel 7^{p-1} - 1$

$7^{p-1} - 1 = (7-1)(7^{p-2} + \ldots + 1)$ $\quad$ ($3 \parallel$ 7−1; $p-1$ mod 3)

$\left(\frac{a^p - b^p}{a-b}, a-b\right) \mid p$

$3 \mid p-1 \qquad 7^{\frac{p-1}{2}} + 1 = 2d^2 \qquad (7^{\frac{p-1}{2}} = n^3)$

$\frac{p-1}{2} = 3k$

$n = 7^k$

$(n+1)(n^2-n+1) = 2d^2$ $\quad$ nn poss. avere fattori in comune, se non 3

$n+1 = 2 \quad (\bmod 3)$

$n^2 - n + 1$ è disp $\qquad n^2 - n + 1 = g^2$

$(n-1)^2 < n^2 - n + 1 < n^2 \quad \forall n > 1$

Fissato a, per quali p $p \mid a^{p-1} - 1$

6) a o b NEGATIVI: CASO FACILE, COSTA 1 pt

$a=0 \quad b=0 \qquad a=1 \quad b=2$

PRINCIPIO: SE C'È UNA SOLUZIONE NON SI FA CON I MODULI!!

MA se c'è tipo 2^b, MODULO 16 (2^k) NON È SCONTATO CI SIA UNA SOLUZIONE

$p \mid f(x_1) \quad p \nmid f'(x_1) \Rightarrow \forall k \, \exists x_k : p^k \mid f(x_k)$

$x_{n+1} \equiv x_n \pmod{p^n}$

$1^3 + 2 \quad 1 + 1 = 4$

$(1+4)^3 + 2(1+4) + 1 \equiv 1+12+2+8+1 \equiv 0 \ (8)$

$f(x+ap^k) \equiv f(x) + ap^k \cdot f'(x) \pmod{p^{k+1}}$ $k \geq 1$

$(x+p^k)^n = \boxed{x^n + n \cdot x^{n-1} p^k} + p^{2k}(\ldots)$ ← non conta

$x^n + (x^n)' \, p^k$

$\ldots b \cdot p^k \pmod{p^{k+1}}$

$p^k \nmid f(x) \quad f(x+a \cdot p^k) \equiv f(x) + a \cdot p^k f'(x)$

$b + a \cdot f'(x) \equiv 0 \pmod{p}$

- $\exists !\ a \pmod{2^n}$: $2^n \mid a^3 + 2a + 1$ FALLIAMO

Dato $p(x)$ vogliamo ris.

$p(x) = 4x^2 + 1$ $p(x) \equiv 1 \pmod 4$

$p(x) = \prod q_i^{k_i}(x)$ $q_i(x) \equiv 1 \pmod 4$

APPLICO QUESTA IDEA:

mod 3 $a^3 + 2a + 1 \equiv 3a + 1 \equiv 1$ => b è pari

$(a + k_1)(a^2 + k_2 a + k_3) + (2) = 2b$ ← è quad.

sia $a + k_1$, sia ↓ hanno tutti divisori primi tal, che $\left(\frac{2}{p}\right) = 1$

$\left(\frac{a}{p}\right) = 1$ a è res. quad. / -1 non è res q.

$2 \Rightarrow$ $a + k_1 \pmod 2$

mod 2_i, 2 disp è inutile!

$\left(\frac{2}{p}\right)$ DIPENDE DA CONGR. p mod 8

$\neq 2$ $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2 - 1}{8}}$

LEMMA DI GAUSS!

a, p primo

$a, 2a, \ldots, \frac{p-1}{2} a$ RESTO mod p m volte il resto $> \frac{p}{2}$

$1, \ldots, p-1$

$\left(\frac{a}{p}\right) = (-1)^m$ $\qquad$ $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

$(-1)^m \equiv a^{\frac{p-1}{2}} \pmod p$

$K a = (-1)^{k(K)} \cdot l_K$

$l_i \in \{1, \dots, \frac{p-1}{2}\}$ $\qquad$ $l_i \neq l_j$

$a \cdot 2a \cdot \dots \cdot \frac{p-1}{2} a \equiv \prod l_i \cdot (-1)^{k(i)}$

$Ka \equiv \pm j a \pmod p$

$K \pm j \equiv 0 \pmod p$

$0 < K + j < p$

I l_i SONO $\frac{p-1}{2}$, QUINDI SONO UGUALI A PERM. DI $\{1, \dots, \frac{p-1}{2}\}$

$\prod l_i = \prod_{i=1}^{\frac{p-1}{2}} i$

$a^{\frac{p-1}{2}} \equiv \prod (-1)^{l(i)} \equiv (-1)^m$

VI FATTO IL CONTO CON 2 DÀ

$2, \dots, 2 \cdot \frac{(p-1)}{2}$

$\left(\omega + \frac{1}{\omega}\right)^2 = 2 \qquad \left(\omega + \frac{1}{\omega}\right)^p = \omega + \frac{1}{\omega}$

2 è res. q. mod $p \iff p \equiv \pm 1 \pmod 8$

-2 è res. q. mod $p \iff p \equiv 1, 3 \pmod 8$ $\qquad$ $b = 3$

$a^3 + 2a + 1 = 2$

$a^3 + 2a + 1 = -2$ $\qquad$ $a = -1$

$a^3 + 2a + 1 = 2b$

$a^3 + 2a + 1 \equiv 0 \pmod 8$

$\Downarrow$

$a \equiv 5 \pmod 8$

$(a+1)(a^2 - a + 3) - 2 = 2b$

$a \equiv 5$ $\qquad$ $a^2 - a + 3 \equiv -1 \pmod 8$

$p \mid a^2 - a + 3 \Rightarrow p \equiv 1, 3 \pmod 8$

$\prod p_i^{k_i}$ $\quad p_i \equiv 2, 3$ è 1 o 3 mod 8

$3^2 \equiv 1 \pmod 8$ NO SOL $b \geq 2$

$(0, 0) \qquad (1, 2)$

$a(a^2 + 2a + 1)$

$(a^2+2)a = (2^{a/2} - 1)(2^{a/2} + 1)$ NON SERVE!!