Bollettino
Unione Matematica Italiana

Marco Cugiani

Sull'aritmetica dei polinomi di esponenziali a valori interi.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **7** (1952), n.1, p. 38–43.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1952_3_7_1_38_0>

Sull'Aritmetica dei polinomî di esponenziali a valori interi.

Nota di MARCO CUGIANI (a Milano).

Sunto. - *Sia* $F(y) = c_0y^n + c_1y^{n-1} + \ldots + c_n (c_0 \neq 0,\ c_n \neq 0.\ n \geq 1)$ *un polinomio a coefficienti interi, irriducibile. Detto* P_x *il massimo divisore primo del prodotto*

$$F(a) \cdot F(a^{2^m}) \ldots F(a^{x^m})$$

(a, x, m *interi*, $m \geq 1$, $|a| \geq 2$, $(a, c_n) = 1$) *si dimostra che*

$$\varliminf P_x / \sqrt{x \log x} > 0.$$

I.

È già stato fatto oggetto di studio il comportamento aritmetico, al variare dell'intero x, di un polinomio a coefficienti interi, irriducibile, del tipo:

$$F(y) = c_0y^n + c_1y^{n-1} + \ldots + c_n \qquad (c_n \neq 0,\ c_0 \neq 0,\ n \geq 1) \tag{1}$$

quando l'argomento y del polinomio sia assunto uguale ad a^x (con $|a|$ intero ≥ 2) [1].

Ora noi ci proponiamo di estendere lo studio al caso in cui si assuma $y = a^{x^m}$ (a, m interi; $|a| \geq 2$, $m \geq 1$, $(a, c_n) = 1$).

([22]) E. BOMPIANI, op. cit. in ([11]). M. VILLA, *Direzioni d'osculazione e di iperosculazione di due trasformazioni puntuali.* Questo « Bollettino » S. III, A. II, pagg. 188-195 (1947).

([1]) Vedi G. RICCI, *Sull'aritmetica dei polinomi in* $a^x \ldots$, « Boll. U. M. I. ». 12 (1933), pagg. 222-228.

Vedi inoltre G. PÓLYA : *Arithmetische Eigenschaften...*, « Jour. f. Math. », Bd. 151 (1921), pagg. 1-31.

Più precisamente vogliamo dimostrare che posto:

$$G(x) = F(a^{x^m}) \tag{2}$$

(per x intero) e chiamato P_x il massimo divisore primo del prodotto

$$\Pi(x) = |\, G(1) \cdot G(2) \dots G(x) \,| \tag{3}$$

esiste un numero positivo γ (indipendente da x) tale che per x abbastanza grande si ha:

$$P_x > \gamma \sqrt{x \log x}.$$

Ciò equivale ad affermare che

$$\varliminf P_x / \sqrt{x \log x} > 0.$$

Se ne deduce in particolare che $P_x \to +\infty$ per $x \to +\infty$.

II.

Alla dimostrazione del nostro teorema premetteremo tre lemmi (la lettera p denoterà sempre numeri primi).

LEMMA I. - Per $(k, p) = 1$ la congruenza:

$$y^m \equiv k \pmod{p^s} \tag{4}$$

ammette al più $2m$ soluzioni (mod p^s).

Questo lemma è una immediata conseguenza di una proposizione dimostrata da SAMBASIVA RAO, la quale afferma anzi, più precisamente, che la (4), se è solubile, ammette esattamente un numero di soluzioni dato da $(\gamma m, \varphi(p^s))$. dove $\gamma = 2$ per $p = 2$ e $2 | m$, ed invece $\gamma = 1$ in tutti gli altri casi, mentre $\varphi(n)$ è l'indicatrice di EULER (²).

LEMMA II. - Il numero $N(\xi)$ delle soluzioni della congruenza:

$$x^m \equiv kp^r \pmod{g \cdot p^s} \tag{5}$$

(dove $(k, p) = (g, p) = 1$, $0 < r < s$) che non superano un numero reale prefissato ξ, soddisfa alla limitazione

$$N(\xi) \leq 2m \left(\frac{\xi}{p^{s/m}} + 1 \right).$$

Per dimostrarlo osserviamo anzitutto che ogni soluzione della (5)

(²) K. SAMBASIVA RAO, *On the representation of a number as the sum of the* k — th *power of a prime and an* l — th *power-free number*, « Proc. Indian Acad. Sci. », A 11 (1940), pagg. 429-436.

La proposizione qui ricordata è il lemma 3 pag. 431.

deve soddisfare anche la

$$x^m \equiv kp' \pmod{p^s}, \tag{6}$$

e quindi basterà dimostrare il lemma per la (6). Perchè uno dei numeri x

$$1, 2, 3, \ldots, [\xi]$$

possa soddisfare la (6) dovrà essere anzitutto $m \mid r$ ed x multiplo di $p^{r/m}$; dovrà cioè aversi per $x = y \cdot p^{r/m}$

$$y^m \cdot p' \equiv kp^r \pmod{p^s},$$

ossia

$$y^m \equiv k \pmod{p^{s-r}}.$$

Questa congruenza ammette al più $2m$ soluzioni in ogni gruppo di p^{s-r} numeri consecutivi, e ciò in virtù del Lemma I; quindi la (6) ammette al più $2m$ soluzioni in ogni gruppo di

$$p^{s-r+\frac{r}{m}} = p^{s+\frac{1-m}{m}r}$$

numeri consecutivi. Avremo perciò:

$$N(\xi) \leq 2m\left(\left[\frac{\xi}{p^{s+(1-m)r/m}}\right] + 1\right) \leq 2m\left(\frac{\xi}{p^{s/m}} + 1\right).$$

Osservazione. - Se anche fosse $r \geq s$ allora dovendo essere x^m un multiplo di p^s il numero $N(\xi)$ dovrebbe soddisfare alla limitazione

$$N(\xi) \leq \frac{\xi}{p^{s/m}}$$

e quindi a maggior ragione anche alla limitazione precedente.

LEMMA III. - Vale la limitazione:

$$\sum_{p \leq x} p = O\left(\frac{x^2}{\log x}\right).$$

Questa è una immediata conseguenza del fatto che, come è ben noto, detto p_n l'n-esimo numero primo, si ha:

$$p_n = O(n \log n) \qquad \text{e quindi} \qquad p_n < kn \log n,$$

per $n \geq 2$ e k indipendente da n. Avremo perciò ovviamente (posto $(p_{r-1} \leq x < p_r)$:

$$\sum_{p \leq x} p \leq 2 + k\int_2^r t \log t \, dt = O(r^2 \log r) = O\left(\frac{x^2}{\log x}\right).$$

III.

Scelti ora due numeri γ_1, γ_2 reali positivi (con $\gamma_1 < |c_0| < \gamma_2$) si può in conseguenza determinare uno ξ_0 tale che per ogni $\xi \geq \xi_0$ ed ogni $\xi' \leq \xi$ si abbia

$$\gamma_1 \cdot |a|^{n(\xi-1)^m} < |G([\xi])| < \gamma_2 \cdot |a|^{n\xi^m}; \qquad |G([\xi'])| < \gamma_2 \cdot |a|^{n\xi^m}.$$

Poniamo allora (per $\xi \geq \xi_0$):

$$\Phi(\xi) = \log \Pi([\xi]) = \log |G(1) \cdot G(2) \dots G([\xi])|$$

ed avremo (per $\xi \geq \xi_0$ e $\xi' \leq \xi$, avendo inoltre posto $a' = |a|$):

$$(7) \quad \begin{cases} n(\xi-1)^m \log a' + \log \gamma_1 < \log |G([\xi])| < n\xi^m \log a' + \log \gamma_2 \\ \log |G([\xi'])| < n\xi^m \log a' + \log \gamma_2 \end{cases}$$

e conseguentemente

$$(8) \quad \Phi(\xi) \geq \Phi(\xi_0) + \sum_{h=[\xi_0+1]}^{[\xi]} (n(h-1)^m \log a' + \log \gamma_1) =$$

$$= \Phi(\xi_0) + n \log a' \frac{\xi^{m+1}}{m+1} + O(\xi^m) + |[\xi] - [\xi_0 + 1]| \log \gamma_1$$

$$= \gamma_3 \xi^{m+1} + O(\xi^m), \qquad (\gamma_3 \text{ costante positiva}).$$

Sia ora p un numero primo assegnato non divisore di a (si ricordi che $(a, c_n) = 1$) e consideriamo la congruenza:

$$(9) \qquad G(x) = F(a^{x^m}) \equiv 0 \pmod{p^t};$$

se y_0 è una radice della congruenza:

$$(10) \qquad F(y) \equiv 0 \pmod{p^t}$$

e se

$$a^{z_0} \equiv y_0 \pmod{p^t}$$

e se inoltre chiamiamo $g(p^t)$ il gaussiano di p^t in base a (cioè l'esponente a cui appartiene $a \pmod{p^t}$), allora le soluzioni della congruenza:

$$(11) \qquad x^m \equiv z_0 \pmod{g(p^t)}$$

sono le radici della (9) corrispondenti alla radice y_0 della (10).

Ora se D è il discriminante del polinomio $F(y)$ il numero delle soluzioni della (10) non può superare la costante $\gamma_4 = nD^2$. Per quanto si riferisce alla (11) due casi possono darsi:

$$1^\circ) \quad p \nmid z_0, \qquad\qquad 2^\circ) \quad p \mid z_0.$$

Ricordiamo che in generale si ha $g(p^t) = p^{t-\alpha} \cdot \beta$ (dove α e β

sono indipendenti da i, una volta fissati a e p e si ha $\beta \leq p-1$). Soltanto nei casi in cui risultasse $\alpha > 1$ si dovrà porre $g(p^i) = \beta$ tutte le volte che si abbia $\alpha > i$.

Si osservi inoltre che risulterà sempre:

$$\alpha < \log(2a') \frac{p}{\log p}; \tag{12}$$

si ha infatti $p^\alpha \mid a^\beta - 1$ e quindi $\mid a^\beta - 1 \mid \geq p^\alpha$ ossia $\mid (2a)^\beta \mid > p^\alpha$, ed essendo $\beta < p$ segue l'asserto.

Posto perciò $s = i - \alpha$ per $\alpha \leq i$ ed $s = 0$ per $\alpha > i$ la (11) si può scrivere:

$$x^m \equiv z_0 \pmod{p^s \cdot \beta}. \tag{13}$$

Nel caso 1°) il numero delle radici (mod $p^s \cdot \beta$) di questa congruenza è dato dal prodotto dei numeri delle radici, rispettivamente (mod p^s) e (mod β), delle due congruenze:

$$x^m \equiv z_0 \pmod{p^s}, \qquad x^m \equiv z_0 \pmod{\beta}.$$

Il primo non supera $2m$ per il lemma I ed il secondo non può superare β. Perciò il numero delle soluzioni della (13) in interi positivi x, con $x \leq \xi$ non può superare il valore dell'espressione:

$$2m \cdot \beta\left(\left[\frac{\xi}{g(p^i)}\right] + 1\right) < 2m\beta\left(\frac{\xi}{p^s \cdot \beta} + 1\right)$$

che a sua volta non supera (essendo $m \geq 1$):

$$2m\left(\frac{\xi}{p^{s/m}} + p\right).$$

Nel caso 2°) si ha invece, per il lemma II, che il numero degli interi positivi $x \leq \xi$ che soddisfano la (13) è maggiorato da:

$$\frac{2m\xi}{p^{s/m}} + 2m.$$

Quindi il numero complessivo delle soluzioni della (9) che risultano $\leq \xi$ è maggiorato da:

$$\gamma_4 \left\{ 2m\left(\frac{\xi}{p^{s/m}} + p\right) + \frac{2m\xi}{p^{s/m}} + 2m \right\} <$$

$$< \gamma_4 \left\{ 4mp + 4m\frac{\xi}{p^{s/m}} \right\} = \gamma_5 \left\{ p + \frac{\xi}{p^{s/m}} \right\}, \quad (\gamma_5 = 4m\gamma_4).$$

D'altra parte l'intero primo p entra in ogni fattore $G(b)$ del

prodotto $\Pi([\xi])$ ad una potenza il cui esponente non supera:

$$(14) \qquad k = \frac{\log |G(b)|}{\log p} < \frac{n\xi^m \log a' + \log \gamma_2}{\log p} \leq \frac{H\xi^m}{\log p}$$

(H costante opportuna) per la seconda delle (7).

Ne segue che, detto $l(p)$ l'esponente della massima potenza di p che divide il prodotto $\Pi([\xi])$, si ha:

$$l(p) \leq \sum_{i=1}^{k} \gamma_5 \left\{ \frac{\xi}{p^{s/m}} + p \right\}$$

(si ricordi che i termini della sommatoria dipendono da i attraverso s). Abbiamo poi (per (12) e (14)):

$$\sum_{i=1}^{k} \gamma_5 \left(\frac{\xi}{p^{s/m}} + p \right) = \gamma_5 \sum_{i=1}^{k} p + \gamma_5 \sum_{i=1}^{k} \frac{\xi}{p^{s/m}} \leq \gamma_5 p \frac{H\xi^m}{\log p} +$$

$$+ \gamma_5 \xi \left(\alpha + \int_0^k \frac{dl}{p^{l/m}} \right) \leq \gamma_6 \xi^m \frac{p}{\log p} + \gamma_5 \xi \frac{p}{\log p} \log (2a') +$$

$$+ \gamma_5 \xi m \left(1 - \frac{1}{p^{k/m}} \right) \cdot \frac{1}{\log p} \leq \gamma_7 \xi^m \frac{p}{\log p} + \gamma_8 \frac{\xi}{\log p}$$

(dove i γ_i sono costanti di evidente significato).

Si deduce quindi:

$$\Phi(\xi) = \sum_p l(p) \log (p) \leq \sum_p | p \cdot O(\xi^m) + O(\xi) | = \sum_p p \cdot O(\xi^m).$$

Se noi ora supponessimo l'esistenza di una successione crescente di interi

$$| y_i | \qquad y_1, y_2, \ldots, y_n, \ldots \qquad (y_n \to +\infty \text{ per } n \to +\infty)$$

tale che risultasse $P_y / \sqrt{y \log y} \to 0$ per $y \to +\infty$ lungo la successione $| y_i |$ avremmo (si ricordi il lemma III):

$$\Phi(y) = \sum_{p \leq P_y} p \cdot O(y^m) = O\left(\frac{P_y^2}{\log P_y} \right) \cdot O(y^m) = o\left(\frac{y \log y}{\log y} \right) \cdot O(y^m) = o(y^{m+1}),$$

il che è in evidente contrasto colla (8). Da questo assurdo segue il nostro asserto.