Bollettino
Unione Matematica
Italiana

Giovanni Ricci

Sull'aritmetica dei polinomi in a^x (a, x interi) a coefficienti interi

Bollettino dell'Unione Matematica Italiana, Serie 1, Vol. **12** (1933), n.4, p. 222–228.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_1933_1_12_4_222_0>

Sull'aritmetica dei polinomi in a^x (a, x interi) a coefficienti interi.

Nota di GIOVANNI RICCI (a Pisa).

Sunto. - *Detto* P_x *il massimo divisore primo del prodotto* $F(a)\cdot F(a^2)\dots F(a^x)$ (F *polinomio di grado* $n \geq 1$, *irriducibile a coefficienti interi,* a *e* x *interi,* $|a| \geq 2$) *si dimostra che è*

$$\lim_{x \to \infty} \frac{x \log x}{P_x} \leq 2(n+1).$$

1. Sia

$$F(y) = c_0 y^n + c_1 y^{n-1} + \dots + c_{n-1} y + c_n, \quad (c_0 \neq 0,\ c_n \neq 0,\ n \geq 1)$$

una funzione razionale intera in y, a coefficienti interi, irriducibile, di grado $n \geq 1$ e poniamo

$$G(x) = F(a^x) = c_0 a^{nx} + c_1 a^{(n-1)x} + \dots + c_n$$

essendo a un intero in valore assoluto ≥ 2. G. PÓLYA [1] ha dimostrato incidentalmente che le funzioni a valori interi $G(x)$, e anche funzioni a valori interi di tipo più generale di queste, ammettono

[1] G. PÓLYA, *Arithmetische Eigenschaften...*, « Journal f. Mathematik », Bd. 151. 1921, pp. 19-21.

infiniti divisori primi, in altre parole, detto P_x il massimo divisore primo del prodotto

(1) $$G(1) \cdot G(2) \dots G(x).$$

risulta

(2) $$\lim_{x \to \infty} P_x = \infty.$$

Questo si vede subito, con PÓLYA, per assurdo. Possiamo supporre, senza alterare la generalità, che a e c_n siano primi fra loro, poichè ove non lo fossero potremmo assumere l'intero positivo k abbastanza grande e porre

$$dG_1(x) = G(x+k) = F(a^{x+k}) = d(c_0' a^{nx} + c_1' a^{(n-1)x} + \dots + c_n')$$

con d opportuno divisore di c_n e $c_n' = \frac{c}{d}$ primo con a; allora saremmo ridotti a dimostrare l'asserto per la funzione $G_1(x)$.

Supponiamo che non valga la (2); detti $p_1, p_2, \dots, p_r$ gl'interi primi (in nu merofinito) che non superano $\lim P_x$, siano $p_1^{b_1}, p_2^{b_2}, \dots, p_r^{b_r}$ rispettivamente le massime potenze di $p_1, p_2, \dots, p_r$ che dividono $G(1) = F(a)$ e poniamo

$$m = \varphi(p_1^{b_1+1}) \cdot \varphi(p_2^{b_2+1}) \dots \varphi(p_r^{b_r+1}).$$

Evidentemente

$$G(1+mz) = F(a^{1+mz}) \equiv 0 \pmod{p_i^{b_i}}, \quad \not\equiv 0 \pmod{p_i^{b_i+1}}, \quad (i = 1, 2, \dots, r),$$

quindi per qualunque intero positivo z risulta $|G(1+mz)| \leq p_1^{b_1} \dots p_r^{b_r}$, ciò che è assurdo.

Più difficile risulta indagare l'andamento, per x crescente indefinitamente, del massimo divisore primo P_x del prodotto (1), e lo scopo della presente Nota è appunto quello di dimostrare *con mezzi elementari* le proposizioni che seguono, le quali costituiscono un primo passo verso tale indagine.

Sia $F(y)$ *una funzione di* y *razionale intera a coefficienti interi, irriducibile, di grado* $n \geq 1$, *e sia* $G(x) = F(a^x)$ *con* a *intero in valore assoluto* ≥ 2. *Denotiamo con* ε *un numero positivo qualunque e* α *un numero positivo minore di* $\frac{1}{2(n+1)}$.

a) *Il numero* $N_\varepsilon(x)$ *degl'interi primi distinti maggiori di* $x \log^{1-\varepsilon} x$ *che dividono il prodotto* $G(1)G(2) \dots G(x)$ *soddisfa alla condizione*

$$N_\varepsilon(x) > \frac{x}{2(n+1)} + O\left(\frac{x}{\log^\varepsilon x}\right) \qquad (\varepsilon > 0).$$

b) *Il numero* $M_\alpha(x)$ *degl'interi primi distinti maggiori di* $\alpha x \log x$

che dividono il prodotto G(1)G(2)... G(x) *soddisfa alla condizione*

$$M_x(x) > \left\{ \frac{1}{2(n+1)} - \alpha \right\} x + O\left(\frac{x \log\log x}{\log x} \right), \quad \left(0 < \alpha < \frac{1}{2(n+1)} \right).$$

OSSERVAZIONI. — Si conclude che il numero degl'interi primi distinti che dividono il prodotto $G(1)G(2)\dots G(x)$ supera

$$\frac{x}{2(n+1)} + O\left(\frac{x}{\log^2 x} \right).$$

Inoltre, riguardo al massimo divisore primo P_x, dalla proposizione b) deduciamo la limitazione

$$\overline{\lim_{x \to \infty}} \frac{x \log x}{P_x} \leq 2(n+1),$$

che sostituisce la (2) perfezionandola.

2. Andiamo a dimostrare la proposizione a); la proposizione b) ne risulterà immediata conseguenza.

Possiamo supporre senza alterare la generalità, per quello che abbiamo già osservato, $c_0 \geq 1$, e c_n primo con a in guisa che, per qualunque intero positivo x, $G(x)$ risulti primo con a. Scelti due numeri reali positivi γ, γ', con $\gamma < c_0 |a|^{-n} < c_0 < \gamma'$, si può determinare un numero reale ξ_0 abbastanza grande in guisa che per $\xi \geq \xi_0$ e qualunque $\xi' \leq \xi$ si abbia

$$\gamma |a|^{n\xi} < |G([\xi])| < \gamma' |a|^{n\xi}, \quad |G([\xi'])| < \gamma' |a|^{n\xi}.$$

Poniamo per $\xi \geq \xi_0$

$$\Phi(\xi) = \log |G(1)G(2)\dots G([\xi])|, \tag{3}$$

e anche $a' = |a|$. Risulta per $\xi \geq \xi_0$ e $\xi' \leq \xi$

$$\begin{aligned} n\xi \log a' + \log\gamma < \log |G([\xi])| < n\xi \log a' + \log\gamma', \\ \log |G([\xi'])| < n\xi \log a' + \log\gamma', \end{aligned} \tag{4}$$

da cui

$$\begin{aligned} \Phi(\xi) &\geq \Phi(\xi_0) + \sum_{m=[\xi_0+1]}^{[\xi]} (nm \log a' + \log\gamma) \\ &= \Phi(\xi_0) + \frac{n \log a'}{2} ([\xi] + [\xi_0] + 1)([\xi] - [\xi_0]) + ([\xi] - [\xi_0]) \log\gamma \\ &= \frac{n \log a'}{2} \xi^2 + O(\xi). \end{aligned} \tag{5}$$

Questa ultima è un'espressione minorante rispetto a $\Phi(\xi)$; cerchiamo adesso di ottenere per altra via un'espressione maggio-

rante. Andiamo a valutare il contributo portato nella funzione $\Phi(\xi)$ dalla potenza di un numero primo p.

Sia b un intero primo con a e x_0 una eventuale soluzione della congruenza

$$G(x) = F(a^x) \equiv 0 \pmod{b}. \tag{6}$$

Posto $a^{x_0} = y_0$, l'intero y_0 risulta una radice della congruenza

$$F(y) \equiv 0 \pmod{b}; \tag{7}$$

inversamente, a una radice y_0 di quest'ultima congruenza possiamo far corrispondere come radici della (6) tutte quelle eventuali della congruenza binomia

$$a^x \equiv y_0 \pmod{b}; \tag{8}$$

detto $g(b)$ l'esponente cui appartiene $a \pmod{b}$, cioè il minimo intero positivo per cui $a^{g(b)} \equiv 1 \pmod{b}$, il numero degl'interi positivi non superiori a ξ che soddisfano la (8) è minore o uguale a $\left[\frac{\xi}{g(b)}\right] + 1$; dunque detto $h(b)$ il numero delle radici distinte $(\bmod b)$ della (7), il numero degl'interi positivi non superiori a ξ che soddisfano la (6) è minore o al più uguale a

$$h(b)\left(\left[\frac{\xi}{g(b)}\right] + 1\right).$$

L'intero primo p entra in ogni fattore $G(m)$ del prodotto

$$G(1)G(2) \dots G([\xi]) \tag{9}$$

a una potenza il cui esponente non supera $\left[\frac{\log |G(m)|}{\log p}\right]$, e quindi per la seconda delle (4) non supera

$$k = k(p, \xi) = \left[\frac{n\xi \log a' + \log \gamma'}{\log p}\right]. \tag{10}$$

Ne segue che detto $l(p)$ l'esponente della massima potenza di p che divide il prodotto (9) abbiamo

$$\begin{aligned} l(p) &\leqq h(p)\left(\left[\frac{\xi}{g(p)}\right] + 1\right) + h(p^2)\left(\left[\frac{\xi}{g(p^2)}\right] + 1\right) + \dots + h(p^k)\left(\left[\frac{\xi}{g(p^k)}\right] + 1\right) \\ &\leqq \xi \cdot \sum_{i=1}^{k} \frac{h(p^i)}{g(p^i)} + \sum_{i=1}^{k} h(p^i) \\ &\leqq \xi \cdot \sum_{i=1}^{\infty} \frac{h(p^i)}{g(p^i)} + \sum_{i=1}^{k} h(p^i). \end{aligned} \tag{11}$$

D'altronde sappiamo [1] che, qualunque sia l'intero positivo c, risulta $h(p^c) \leqq nD^2$, essendo D il discriminante di $F(y)$; inoltre se p non divide D allora $h(p^c) = h(p) \leqq n$.

Sappiamo pure [2] che se p è un numero primo dispari, e p^r è la massima potenza di p che divide $a^{g(p)} - 1$, allora

$$g(p^s) = g(p) \text{ se } s \leqq r, \quad g(p^s) = p^{s-r} g(p) \text{ se } s > r;$$

se a è della forma $4h + 1$, e 2^r è la massima potenza di 2 che divide $a - 1$, allora

$$g(2^s) = 1 \text{ se } s \leqq r, \quad g(2^s) = 2^{s-r} \text{ se } s > r;$$

se a è della forma $4h + 3$ e 2^r è la massima potenza di 2 che divide $a + 1$ allora

$$g(2) = 1, \quad g(2^s) = 2 \text{ se } 2 \leqq s \leqq r, \quad g(2^s) = 2^{s-r} \text{ se } s > r.$$

Pel significato di $g(p)$, essendo per p dispari $|a^{g(p)} - 1| \geqq p^r$ ricaviamo $a'^{g(p)} \geqq p^r - 1$ da cui

$$(12) \quad g(p) \geqq \frac{r \log p}{\log a'} \frac{\log (p^r - 1)}{\log p^r} > \frac{r \log p}{\log a'} \left(1 + \frac{1}{(p^r - 1) \log (p^r - 1)}\right)^{-1}.$$

Tenendo conto di queste proposizioni ricordate abbiamo, qualunque sia l'intero primo p pari o dispari:

$$\sum_{i=1}^{\infty} \frac{h(p^i)}{g(p^i)} \leqq nD^2 \sum_{i=1}^{\infty} \frac{1}{g(p^i)} \leqq \frac{nD^2}{g(p)} \left(r + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots\right)$$

da cui

$$\xi \sum_{i=1}^{\infty} \frac{h(p^i)}{g(p^i)} \leqq \frac{nD^2}{g(p)} \left(r + \frac{1}{p-1}\right) \xi = O(\xi).$$

Analogamente, per la (10)

$$\sum_{i=1}^{k} h(p^i) \leqq nD^2 k(p, \xi) \leqq \frac{nD^2}{\log p} (n\xi \log a' + \log \gamma') = O(\xi).$$

Dalla (11) si ricava dunque

$$(13) \qquad l(p) = O(\xi).$$

Da questa relazione si può trarre di nuovo la dimostrazione della (2); infatti, fissati gl'interi primi $p_1, p_2, \ldots, p_t$ in numero finito qualunque, e detto $d(\xi)$ il massimo divisore del prodotto (9)

[1] T. NAGELL, *Généralisation d'un théorème de Tchebytcheff*, « Journal de Mathématiques », s. 8, t. 4, 1921, pp. 343-356.

[2] Ved. p. es. M. CIPOLLA, *Teoria dei numeri. Analisi indeterminata*, « Enciclop. Mat. elem. », vol. I, Milano, 1929, p. 281.

composto esclusivamente con questi fattori primi si ricava

$$\log d(\xi) = \sum_{i=1}^{t} l(p_i) \log p_i = \sum_{i=1}^{t} \log p_i \, O(\xi) = O(\xi)$$

e confrontando con la (5) segue per assurdo la (2).

Sia adesso p primo dispari non divisore di D; allora per le osservazioni che precedono e per la (12) otteniamo

$$\sum_{i=1}^{\infty} \frac{h(p^i)}{g(p^i)} \leqq h(p) \sum_{i=1}^{\infty} \frac{1}{g(p^i)} \leqq \frac{n}{g(p)} \left(r + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots \right) \leqq$$

$$\leqq \frac{n \log a'}{\log p} \left(1 + \frac{1}{r(p-1)} \right) \left(1 + \frac{1}{(p^r - 1) \log (p^r - 1)} \right)$$

$$\sum_{i=1}^{k} h(p^i) \leqq \frac{n}{\log p} (n\xi \log a' + \log \gamma').$$

Per la (11) si conclude

$$l(p) \leqq \frac{n(n+1) \log a'}{\log p} \xi + \frac{n \log a'}{r(p-1) \log p} \xi + \frac{O(1)}{\log p} + \tag{14}$$

$$+ \frac{1}{(p^r - 1) \log (p^r - 1)} \frac{O(\xi)}{\log p}.$$

Siamo adesso in grado di costruire un'espressione maggiorante di $\Phi(\xi)$, poichè

$$\Phi(\xi) = \sum_{p} l(p) \log p = O(\xi) + \sum_{p}' l(p) \log p$$

essendo la somma Σ' estesa agl'interi primi p dispari, maggiori di D. Posto $\eta = \xi \log^{1-\varepsilon} \xi$, denotiamo con $N_\varepsilon(\xi)$ il numero dei divisori primi distinti del prodotto (9) tutti maggiori di η; abbiamo per la (14)

$$\Phi(\xi) \leqq O(\xi) + \sum_{p \leqq \eta}' l(p) \log p + N_\varepsilon(\xi) \{ n(n+1) \log a' \cdot \xi + O(1) + O(\log^{\varepsilon - 1} \xi) \}.$$

Si vede subito che, essendo $\sum_{p \leqq \eta}' 1 = O\left(\frac{\xi}{\log^\varepsilon \xi} \right)$, risulta per la (14):

$$\sum_{p < \eta}' l(p) \log p = O\left(\frac{\xi^2}{\log^\varepsilon \xi} \right),$$

dunque

$$\Phi(\xi) \leqq O\left(\frac{\xi^2}{\log^\varepsilon \xi} \right) + N_\varepsilon(\xi) \{ n(n+1) \log a' \cdot \xi + O(1) + O(\log^{\varepsilon - 1} \xi) \}.$$

Confrontando questa con la (5) si ricava subito

$$N_\varepsilon(\xi) \geqq \frac{\xi}{2(n+1)} + O\left(\frac{\xi}{\log^\varepsilon \xi} \right) \tag{15}$$

che costituisce la proposizione a).

3. Per dimostrare la proposizione b) osserviamo che il numero degl'interi primi non superiori a $\alpha\xi \log \xi$ è dato dall'espressione

$$\frac{\alpha\xi \log \xi}{\log (\alpha\xi \log \xi)} + O\left(\frac{\alpha\xi \log \xi}{\log^2 (\alpha\xi \log \xi)}\right) = \alpha\xi + O\left(\frac{\xi \log \log \xi}{\log \xi}\right).$$

Basta quindi supporre $\alpha < \frac{1}{2(n+1)}$ per ottenere dalla (15) la la proposizione b).