Bollettino
Unione Matematica Italiana

Emilio Gagliardo

Le funzioni simmetriche semplici delle radici n-esime primitive dell'unità.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **8** (1953), n.3, p. 269–273.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1953_3_8_3_269_0>

Bollettino dell'Unione Matematica Italiana, Zanichelli, 1953.

Le funzioni simmetriche semplici delle radici n-esime primitive dell'unità.

Nota di Emilio Gagliardo (a Genova).

Sunto. - *Vedi prime righe della Nota.*

1. Ci proponiamo di determinare una semplice espressione delle funzioni simmetriche $S_k(n)$ costituite dalla somma delle potenze k-esime (k intero) delle radici n-esime primitive dell'unità. ([1]) Importa osservare che il risultato cui perveniamo non si può dedurre, come è ovvio, dalla nota equazione alla quale soddisfano le radici n-esime primitive dell'unità ([2]):

$$\prod_{d|n}\left(x^{\frac{n}{d}}-1\right)^{\mu(d)}=0$$

ove d varia tra i divisori naturali di n, e $\mu(m)$ è la funzione di Möbius che vale 0 se m è divisibile per un quadrato, e invece vale $(-1)^r$ se m è il prodotto di r fattori primi distinti maggiori di 1; in particolare $\mu(1)=1$.

Fa eccezione soltanto il caso particolare in cui n è la potenza di un numero primo: $n=p^s$ [perchè in questo caso l'equazione assume la forma più esplicita ([3]):

$$\frac{x^{p^s}-1}{x^{p^{s-1}}-1}=x^{(p-1)p^{s-1}}+x^{(p-2)p^{s-1}}+\ldots+x^{p^{s-1}}+1=0.$$

2. Consideriamo l'espressione di Dedekind ([4]):

$$S(n)=R(n)-\sum_i R\left(\frac{n}{p_i}\right)+\sum_{i<j}R\left(\frac{n}{p_ip_j}\right)-\ldots+(-1)^r R\left(\frac{n}{p_1p_2\cdots p_r}\right)$$

([1]) Per mezzo di queste funzioni si possono costruire, come è noto, tutte le altre funzioni simmetriche, e in particolare i coefficienti dell'equazione cui soddisfano le dette radici.

([2]) Cfr. B. L. Van der Waerden, *Moderne Algebra*, I., (1950) p. 127, oppure: H. Hasse, *Vorlesungen über Zahlentheorie*, (1950) p. 172.

([3]) Cfr. H. Hasse, cit. prec., p. 177; L. E. Dickson, *Höhere Algebra* (1929) p. 150.

([4]) Cfr. « Jour. für Math. », 54, 1857, pp. 21-25.

($p_1, \ldots, p_r$ fattori primi distinti di n) ove nel nostro caso $R(m)$ indica la somma di tutte le radici m–esime dell'unità. Essa fornisce allora la somma delle radici n–esime primitive: infatti una radice n–esima primitiva compare solo nel termine $R(n)$; al contrario una radice non primitiva è radice ν–esima primitiva con ν sottomultiplo di n (ed è quindi radice di ordine qualsiasi multiplo di ν) e chiamando q il numero dei fattori primi p_i contenuti in ν ad esponente minore che in n si vede (seguendo la dimostrazione generale di DEDEKIND) che la radice in esame compare una volta nel termine $R(n)$, $\binom{q}{1}$ volte nel termine $\sum_i R\left(\frac{n}{p_i}\right)$, $\binom{q}{2}$ volte nel termine $\sum_{i<j} R\left(\frac{n}{p_i p_j}\right), \ldots, \binom{q}{q}$ volte nel termine $\sum_{i_1<\ldots<i_q} R\left(\frac{n}{p_{i_1}\ldots p_{i_q}}\right)$ mentre non compare più negli eventuali termini successivi; ne segue che la radice in esame viene sommata un numero di volte eguale a: $1-\binom{q}{1}+\binom{q}{2}-\ldots+(-1)^q\binom{q}{q}=\left(1+(-1)\right)^q=0$ ossia non dà contributo, come deve essere non essendo radice primitiva.

Tutto ciò sussiste ovviamente anche se invece di considerare le radici si considerano le loro potenze k–esime: indicando con $S_k(n)$ e con $R_k(n)$ la somma delle potenze k–esime delle radici n–esime primitive e l'analoga somma estesa a tutte le radici n–esime si ha:

$$(1)\quad S_k(n)=R_k(n)-\sum_i R_k\left(\frac{n}{p_i}\right)+\sum_{i<j} R_k\left(\frac{n}{p_i p_j}\right)-\ldots+(-1)^r R_k\left(\frac{n}{p_1 p_2\cdots p_r}\right).$$

3. Per calcolare, come ci siamo proposti, $S_k(n)$ siamo ora condotti a calcolare il valore di $R_k(m)$.

Supponiamo per ora $k>0$.

Le radici m–esime dell'unità sono date da: $e^{\frac{2\pi i h}{m}}$ $(h=1, 2, \ldots, m)$ e la somma delle loro potenze k–esime è quindi:

$$\sum_{h=1}^{m} e^{\frac{2\pi i hk}{m}}=\sum_{h=1}^{m}\cos\frac{2\pi hk}{m}+i\sum_{h=1}^{m}\sin\frac{2\pi hk}{m}$$

Per la simmetria delle radici m–esime rispetto all'asse reale (simmetria che si conserva elevandole tutte alla potenza k–esima) la parte immaginaria è certo nulla.

Quanto alla parte reale essa ([5]) vale m se m è divisore di k, ed è nulla in caso contrario.

Introduciamo il massimo comune divisore (n, k) di n e k; sia:

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_r^{\alpha_r} \qquad (\alpha_i>0,\ p_i \text{ fattori primi di } n)$$

([5]) Cfr. F. SBRANA, « Rend. Acc. Lincei », vol. XXXI, (1922) serie 5ª, 2° sem. fascicolo 12°, p. 547.

$$(n,\ k) = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r} \qquad (0 \leq \beta_i \leq \alpha_i)$$

$$\frac{n}{(n,\ k)} = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \dots p_r^{\alpha_r - \beta_r}$$

Dobbiamo ora distinguere due casi diversi:

I° caso: Sia $\mu\left(\frac{n}{(n,\ k)}\right) = 0$. Ciò avviene se $\frac{n}{(n,\ k)}$ contiene qualche suo fattore primo a esponente maggiore di 1 ossia se c'è qualche indice i per cui: $\alpha_i - 1 > \beta_i$.

Allora nessuno dei numeri che figurano come argomento delle R_k nel secondo membro della (1) è divisore di k, perchè nessuno di questi numeri che sono tutti divisori di n è divisore di $(n,\ k)$; ne segue che in tale caso tutte queste R_k sono nulle e quindi è: $S_k(n) = 0$.

II° caso: Sia invece: $\mu\left(\frac{n}{(n,\ k)}\right) = (-1)^s$ ove s sia il numero dei fattori primi (ora tutti distinti) di $\frac{n}{(n,\ k)}$, (se n è divisore di k è $s = o$; se k è primo con n è $s = r$).

Ciò avviene se per tutti i vavori di i è: $\alpha_i - 1 \leq \beta_i$; e precisamente per s valori di i (siano: $i = 1, 2, \dots, s$) deve essere: $\alpha_i - 1 = \beta_i$, mentre per i rimanenti (cioè: $i = s + 1, \dots, r$), ricordando che è: $\alpha_i \geq \beta_i$ per ogni valore dell'indice i, deve essere: $\alpha_i = \beta_i$.

I numeri p_i con $i = 1, 2, \dots, s$ devono sempre figurare a denominatore negli argomenti delle funzioni R_h del secondo membro della (1) perchè nei termini in cui essi non figurano tutti a denominatore gli argomenti non possono essere divisori di k essendo divisori di n e non di $(n,\ k)$ e quindi le R_k di questi argomenti sono nulle.

Le altre R_k si riducono ai loro argomenti.

Si ha quindi in questo secondo caso:

$$S_k(n) = (-1)^s \frac{n}{p_1 \cdots p_s} + (-1)^{s+1} \sum_{1}^{n-r}{}_i \frac{n}{p_1 \cdots p_s p_{s+i}} +$$

$$+ (-1)^{s+2} \sum_{1}^{n-r}{}_{i<j} \frac{n}{p_1 \cdots p_s p_{s+i} p_{s+j}} + \dots + (-1)^n \frac{n}{p_1 \cdots p_s p_{s+1} \cdots p_r} =$$

$$= (-1)^s \frac{n}{p_1 \cdots p_s} \left[1 - \Sigma \frac{1}{p_{s+i}} + \Sigma \frac{1}{p_{s+i} p_{s+j}} - \dots + (-1)^{r-s} \frac{1}{p_{s+1} \cdots p_r}\right] =$$

$$= (-1)^s \frac{n}{p_1 \cdots p_s} \left(1 - \frac{1}{p_{s+1}}\right)\left(1 - \frac{1}{p_{s+2}}\right) \dots \left(1 - \frac{1}{p_r}\right) =$$

$$= (-1)^s \frac{n}{p_1 \cdots p_s} \frac{\left(1 - \frac{1}{p_1}\right) \cdots\cdots \left(1 - \frac{1}{p_r}\right)}{\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)}$$

Introduciamo la funzione di GAUSS: $\varphi(m) = m\left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_h}\right)$ ove $q_1, \ldots, q_h$ sono i fattori primi distinti di m e ricordiamo che nel caso che stiamo trattando è: $\frac{n}{p_1 \cdots p_s} = (n, k)$.

Abbiamo quindi (nel secondo caso):

$$S_k(n) = (-1)^s (n, k) \frac{\frac{1}{n}\varphi(n)}{\frac{(n, k)}{n}\varphi\left(\frac{n}{(n, k)}\right)} = (-1)^s \frac{\varphi(n)}{\varphi\left(\frac{n}{(n, k)}\right)}$$

I risultati ottenuti nei due diversi casi si compendiano nell'unica formula che ci eravamo proposti di trovare:

$$S_k(n) = \frac{\mu\left(\frac{n}{(n, k)}\right)\varphi(n)}{\varphi\left(\frac{n}{(n, k)}\right)} \tag{2}$$

4. Concludiamo con alcune osservazioni complementari: osserviamo che se k è negativo posto $-k = h$ si ha: $S_k(n) = S_h(n)$ infatti le radici n-esime primitive sono di modulo unitario e a due a due complesse coniugate; quindi facendo di ognuna di esse l'inverso (prima di elevarle alla potenza h-esima) si ritrovano le stesse radici (in un ordine diverso).

Per $k = 0$ è ovviamente $S_0(n) = \varphi(n)$ infatti $S_0(n)$ si riduce al numero delle radici n-esime primitive che è, come noto, $\varphi(n)$.

Abbiamo con ciò calcolato $S_k(n)$ con k intero qualsiasi.

Vogliamo osservare che il prodotto di tutte le radici n-esime primitive è 1 essendo esse a due a due complesse coniugate e di modulo unitario.

Nel caso particolare $k = 1$, volendo cioè calcolare la somma delle radici n-esime primitive dell'unità si ottiene dalla (2): $S(n) = \mu(n)$; e ricordando la definizione di radici n-esime primitive dell'unità ne segue:

$$\sum_\nu e^{\frac{2\pi i\nu}{n}} = \sum_\nu \cos\frac{2\pi\nu}{n} + i \sum_\nu \sin\frac{2\pi\nu}{n} = \mu(n)$$

$$(\nu < n, \ \nu \text{ primo con } n)$$

ma essendo $\mu(n)$ reale si ottiene:

$$\sum_{\nu} \cos \frac{2\pi\nu}{n} = \mu(n) \qquad \sum_{\nu} \sin \frac{2\pi\nu}{n} = 0$$

$$(\nu < n, \ \nu \text{ primo con } n)$$

La prima di queste due relazioni era già stata trovata da KLUYVER (6).

Osserviamo infine che dalla (2) segue:
$S_h(n) = S_k(n)$ se è: $h \equiv k$ (mod. n).