Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Enrico Bombieri

Sull'analogo della formula di Selberg nei corpi di funzioni

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **35** (1963), n.5, p. 252–257.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1963_8_35_5_252_0>

Teoria dei Numeri. — *Sull'analogo della formula di Selberg nei corpi di funzioni* (*). Nota di ENRICO BOMBIERI, presentata (**) dal Socio B. SEGRE.

INTRODUZIONE. – In questa Nota ci proponiamo di estendere la classica formula di A. Selberg nella teoria dei numeri primi, al caso di un corpo di funzioni in caratteristica p, cioè, in altre parole, di trovare l'analogo di questa formula quando si consideri la geometria di una curva algebrica in un campo di Galois.

Come applicazione dei risultati trovati, mostreremo che è possibile determinare asintoticamente per via del tutto elementare il numero di punti della curva nell'estensione finita di grado n del campo base, quando $n \to \infty$.

Sebbene i risultati trovati siano ancora ben lontani dal profondo risultato ottenuto da A. Weil su questo argomento, riteniamo di un certo interesse l'introduzione del metodo aritmetico di A. Selberg in questi problemi di natura principalmente algebrica e geometrica.

I. IL TEOREMA OTTENUTO. – Sia C una curva algebrica di genere g definita su di un campo di Galois $[q]$ con q elementi. Indichiamo con N_m il numero di punti (contando anche i punti all'infinito) di C nell'estensione (unica) $[q^m]$ di grado m del campo base $[q]$. Supporremo inoltre C assolutamente irriducibile, e non singolare.

Dimostreremo qui, con metodo interamente elementare, il seguente:

TEOREMA 1. – *Si ha*

$$N_m \sim q^m \quad \textit{quando} \quad m \to +\infty. \tag{1}$$

A proposito del teorema 1 bisogna ricordare il risultato definitivo di A. Weil

$$|N_m - (q^m + 1)| \leq 2g(\sqrt{q})^m, \tag{2}$$

che però è stato ottenuto con i metodi più elevati della geometria moderna. Ci sembra inoltre che, applicando a questo problema il meccanismo delle « catene di formule di Selberg » da noi recentemente studiato nel caso classico (E. Bombieri [1]), si possa andare molto al di là del risultato puramente asintotico (1).

Per dimostrare il teorema 1, dovremo fare uso di funzioni aritmetiche costruite mediante i divisori interi di C, come pure del teorema di Riemann–Roch per la curva. Rimandando, per le definizioni e la teoria dei divisori, ai

(*) Lavoro eseguito nell'ambito dell'attività del gruppo di ricerca N° 40 del Comitato per la Matematica del C.N.R.

(**) Nella seduta del 9 novembre 1963.

libri di S. Lang [3] e M. Eichler [2], diamo qui i teoremi preliminari sulla geometria della curva dei quali faremo uso nel seguito.

Indicheremo con $a, b, c, \cdots$ divisori interi; con p_i divisori primi. Con $\deg(a)$ denoteremo il grado di a, con $l(a)$ la sua dimensione. Come è ben noto, $\deg(ab) = \deg(a) + \deg(b)$; grado e dimensione sono sempre numeri interi.

Se R è il gruppo abeliano libero dei divisori sulla curva, e H è il sottogruppo dei divisori principali, allora il gruppo quoziente R/H permette di istituire una nozione di equivalenza in R. R/H diventa così il gruppo delle classi di divisori. Le funzioni $\deg(a)$ e $l(a)$ sono funzioni di classi, in quanto prendono gli stessi valori per divisori appartenenti alla medesima classe. Se A è una classe di divisori, con chiari significati potremo allora scrivere $\deg(A)$ e $l(A)$.

Premesso questo, faremo uso dei seguenti fatti ben noti:

i) il numero di divisori interi in una classe A di dimensione $l(A)$ è esattamente

$$(q^{l(A)} - 1)/(q - 1); \tag{3}$$

ii) il numero di classi aventi il medesimo grado non dipende dal valore di quest'ultimo, ed è un numero

$$h \geq 1 \quad \text{finito}; \tag{4}$$

iii) la parte dovuta a Riemann del teorema di Riemann–Roch, cioè: se

$$\deg(A) > 2g - 2, \quad \text{allora} \quad l(A) = \deg(A) + 1 - g, \tag{5}$$

dove g è appunto il genere della curva.

Osserviamo infine che un divisore intero si scompone in modo unico nel prodotto di divisori primi. Il collegamento tra la teoria dei divisori interi e la quantità N_m è espresso dalla nota relazione

$$N_m = \sum_{\deg(p) \mid m} \deg(p), \tag{6}$$

dove la sommatoria è estesa appunto a tutti i divisori primi p per i quali m è un multiplo di $\deg(p)$.

II. LE FUNZIONI ARITMETICHE ASSOCIATE ALLA CURVA. – Poniamo per definizione

$$E_m = \sum_{\deg(a) = m} 1 \qquad \text{(si intende } a \text{ intero, e } m \geq 1), \; E_0 = 1 \tag{7}$$

$$e_m = \begin{cases} 1 & \text{se } m = 0 \\ 0 & \text{se } m \geq 1 \end{cases} \tag{8}$$

$$\mu_m = \sum_{a}' (-1)^k, \tag{9}$$

dove la Σ' è estesa a tutti i divisori interi a per i quali $\deg(a) = m$, e inoltre $a = p_1 \cdots p_k$, dove i p_j sono divisori primi distinti, per $m \geq 1$ e $\mu_0 = 1$.

Date due funzioni aritmetiche f_m e g_m, indicheremo con il simbolo $f_m \circ g_m$ la funzione aritmetica loro « prodotto di Cauchy », cioè

$$f_m \circ g_m = \sum_{h=0}^{m} f_h g_{m-h}. \tag{10}$$

Poniamo infine per definizione

$$N_m^{(k)} = \mu_m \circ (m^k E_m). \tag{11}$$

LEMMA 1. – *Valgono le seguenti identità:*

$$\mu_m \circ E_m = e_m, \tag{12}$$

$$N_m^{(1)} = N_m, \tag{13}$$

dove appunto N_m *è definita dalla* (6),

$$N_m^{(2)} = m N_m + N_m \circ N_m. \tag{14}$$

Dimostrazione. – Si ha:

$$\mu_m \circ E_m = \sum_{h=0}^{m} \left(\sum_{\deg(a)=h} 1 \right) \left(\sum_{\substack{\deg(a')=m-h \\ a'=p_1 \cdots p_k}} (-1)^k \right) = \sum_{\substack{\deg(a)+\deg(a')=m \\ a'=p_1 \cdots p_k}} (-1)^k =$$

$$= \sum_{\substack{\deg(aa')=m \\ a'=p_1 \cdots p_k}} (-1)^k = \sum_{\substack{\deg(b)=m \\ p_1 \cdots p_k \mid b}} (-1)^k = \sum_{\deg(b)=m} \left(\sum_{p_1 \cdots p_k \mid b} (-1)^k \right).$$

Calcoliamo adesso l'ultima sommatoria entro parentesi. Se $b = p_1^{h_1} \cdots p_s^{h_s}$, avremo una sola scelta con $k = 0$, in corrispondenza al fatto che $\mu_0 = 1$, e in generale avremo $\binom{s}{k}$ scelte di fattori di b composti esattamente da k fattori primi distinti. Ne segue che

$$\sum_{p_1 \cdots p_k \mid b} (-1)^k = \sum_{k=0}^{s} (-1)^k \binom{s}{k} = (1-1)^s = 0 \quad \text{se} \quad s > 0.$$

Se $s = 0$, vuol dire che $\deg(b) = 0$, cioè $m = 0$. Ma ora per definizione $E_0 = 1$, $\mu_0 = 1$, da cui la (12).

In modo analogo si dimostra la (13).

Per dimostrare la (14), osserviamo che il prodotto di convoluzione (10) è commutativo e associativo, e che vale sempre l'identità

$$m(f_m \circ g_m) = (m f_m) \circ g_m + f_m \circ (m g_m). \tag{15}$$

Dalla (12), moltiplicando per m, si ha

$$0 = m(\mu_m \circ E_m) = (m\mu_m) \circ E_m + N_m,$$

da cui, facendo il prodotto di convoluzione con N_m, si ricava

$$N_m \circ N_m = -(m\mu_m) \circ E_m \circ \mu_m \circ (m E_m) = -(m\mu_m) \circ (m E_m). \tag{16}$$

D'altra parte, si ha necessariamente

$$(17) \qquad m\mathrm{N}_m = (m\mu_m)\circ(m\mathrm{E}_m) + \mu_m\circ(m^2\,\hat{\mathrm{E}}_m) = (m\mu_m)\circ(m\mathrm{E}_m) + \mathrm{N}_m^{(2)}$$

e, combinando questa identità con la (16), si ha la (14).

Siamo adesso in grado di dimostrare il

LEMMA DI SELBERG PER LE CURVE:

$$m\mathrm{N}_m + \mathrm{N}_m\circ\mathrm{N}_m = 2mq^m + O(q^m),$$

dove la costante in $O(\cdots)$ *dipende unicamente dalla curva.*

Dimostrazione. – Dalle proposizioni *i*), *ii*), *iii*) e dalla definizione della quantità E_m si ricava subito che

$$(18) \qquad \mathrm{E}_m = h(q^{m+1-g} - 1)/(q-1), \quad \text{quando } m > 2g-2,$$

e dove h è il numero di classi di divisori aventi il medesimo grado. Se invece $0 \leq m \leq 2g-2$, E_m è una funzione razionale di q.

Calcoliamo adesso il valore asintotico della nuova funzione aritmetica $\mathrm{E}_m\circ(m\mathrm{E}_m)$. Tenendo presente l'espressione (18) per E_m quando $m > 2g-2$, avremo, calcolando direttamente il valore di questa funzione aritmetica mediante la (10), che:

$$(19) \qquad \mathrm{E}_m\circ(m\mathrm{E}_m) = (h/(q-1))\,m^2 q^{1-g}\,\mathrm{E}_m/2 + \mathrm{R}_1(q)\,m\mathrm{E}_m +$$
$$+ \mathrm{R}_2(q)\,\mathrm{E}_m + \mathrm{R}_3(q) + \mathrm{R}_4(q)\,m + \mathrm{R}_5(q)\,m^2, \quad \text{quando } m > 4g-4,$$

e dove le funzioni $\mathrm{R}_i(q)$ sono funzioni razionali dipendenti da q e dalla curva, ma che non dipendono da m. La dimostrazione della (19) non presenta nessuna difficoltà, in quanto a noi non interessa il valore esatto delle $\mathrm{R}_i(q)$.

Ora osserviamo che si ha sempre la disuguaglianza

$$(20) \qquad |\mu_m| \leq \mathrm{E}_m,$$

che è evidente dal confronto della (9) con la (7). Ne segue in particolare che $|\mu_m\circ m^k| \leq \mathrm{E}_m\circ m^k = O(q^m)$ per $m \to \infty$, e dove la costante in $O(\cdots)$ dipende da q e dalla curva, ma non da m.

Effettuiamo adesso la convoluzione dei due membri della (19) con la funzione aritmetica μ_m. A causa della (12) del lemma 1, si ha

$$(21) \qquad \mu_m\circ\mathrm{E}_m\circ(m\mathrm{E}_m) = m\mathrm{E}_m = (h/(q-1))\,mq^{m+1-g} + O(m),$$

mentre la convoluzione al secondo membro ci dà

$$(22) \qquad (h/(q-1))\,q^{1-g}\,\mathrm{N}_m^{(2)}/2 + \mathrm{R}_1(q)\,\mathrm{N}_m + O(q^m)$$

tenendo appunto presente l'osservazione successiva alla disuguaglianza (20). Confrontando la (21) con la (22) ricaviamo

$$(23) \qquad \mathrm{N}_m^{(2)} = 2mq^m + O(\mathrm{N}_m) + O(q^m).$$

Ricordando l'identità (14), la (23) è proprio il lemma di Selberg per le curve, con un resto in più $O(\mathrm{N}_m)$. D'altra parte, questo resto viene certamente assorbito nell'altro resto $O(q^m)$, poiché dalla (23) e dalla (14), ricordando che $\mathrm{N}_m \geq 0$, è immediato che $\mathrm{N}_m = O(q^m)$.

È ora abbastanza facile ricavare la dimostrazione del teorema 1 dalla formula del tipo di Selberg ora trovata. Poniamo infatti $N_m/q^m = a_m$. Dal lemma di Selberg avremo

$$(24) \qquad m a_m + \sum_{i=1}^{m-1} a_i a_{m-i} = 2m + O(1), \qquad a_i \geq 0$$

e dove la costante in $O(\cdots)$ dipende unicamente da q e dalla curva in esame, ma non da m.

La relazione (24) risulta collegata con alcuni teoremi di tipo tauberiano che si presentano appunto nello studio di questo tipo di problemi.

Poniamo $s_m = \sum_{i \leq m} a_i$, e sommiamo i due membri della (24) da 1 fino a n. Ricaviamo così immediatamente che

$$(25) \qquad \sum_{k \leq m} a_k (s_{m-k} + k) = m^2 + O(m), \qquad a_k \geq 0.$$

La (25) è proprio un sistema di condizioni asintotiche studiato da P. Erdös [4] con metodi interamente elementari.

Dal teorema di P. Erdös si deduce allora che

$$(26) \qquad s_m = m + O(1).$$

Per passare di qui al teorema 1, faremo uso di un risultato di E. Wirsing [5]:

LEMMA DI WIRSING. – *Siano f_1 e f_2 due funzioni reali definite in $(0, \infty)$ e sia*

$$\overline{\lim_{x \to +\infty}} (1/x) \int_0^x f_i^2(y)\, dy = F_i \qquad (i = 1, 2).$$

Sia ancora

$$R(x) = (1/x) \int_0^x f_1(y) f_2(x-y)\, dy,$$

e supponiamo che

$$\overline{\lim_{x \to \infty}} (1/x) \int_0^x R(y)\, dy = 0.$$

Allora si ha la relazione

$$(28) \qquad \overline{\lim_{x \to \infty}} (1/x) \int_0^x R^2(y)\, dy \leq (F_1 F_2)/2.$$

È facile vedere che questo lemma ha un analogo, valido nel caso che si considerino somme discrete invece di integrali.

Poniamo adesso $a_k = 1 + r_k$. Sostituendo nella (24) e tenendo presente la (26) si ricava

$$(29) \qquad m r_m + \sum_{k \leq m} r_k r_{m-k} = O(1),$$

ed ancora si ha

$$|r_m| \leq 1 + O(1/m). \tag{30}$$

Quest'ultima disuguaglianza discende subito da

$$0 \leq m a_m \leq 2m + O(1),$$

che è immediata conseguenza della (24).

Sia adesso A una costante tale che

$$\overline{\lim_{m \to +\infty}} \frac{1}{m} \sum_{k \leq m} r_k^2 = A. \tag{31}$$

Se $mR_m = \sum_{k \leq m} r_k r_{m-k}$, avremo dalla (29) che

$$R_m = -r_m + O(1/m); \tag{32}$$

sicché, in base alla (26), otteniamo

$$\sum_{k \leq m} R_k = O(\log m) = o(m).$$

Ne segue, dal lemma di Wirsing, che

$$(1/m) \sum_{k \leq m} R_k^2 \leq A^2/2 + o(1) \tag{33}$$

onde, ricordando la (32) e la (30), si ricava la disuguaglianza

$$A \leq A^2/2. \tag{34}$$

D'altra parte, è evidente che $A \leq 1$ a causa della (30). Ne segue $A = 0$, cioè

$$\sum_{k \leq m} r_k^2 = o(m). \tag{35}$$

Infine, dalla disuguaglianza di Schwarz, si ha che

$$\left| \sum_{k \leq m} r_k r_{m-k} \right| \leq \sum_{k \leq m} r_k^2 = o(m).$$

Applicando questa disuguaglianza alla (29), ricaviamo finalmente

$$m |r_m| \leq o(m), \tag{36}$$

vale a dire $r_m \sim 0$, $a_m \sim 1$, e cioè $N_m/q^m \sim 1$.

Il nostro teorema è così completamente dimostrato.

BIBLIOGRAFIA.

[1] E. BOMBIERI, *Sulle formule di A. Selberg generalizzate per classi di funzioni aritmetiche e le applicazioni al problema del resto nel Primzahlsatz*, « Riv. Mat. Univ. Parma » [2], *3*, 393–440 (1962).

[2] M. EICHLER, *Einführung in die Theorie der algebraischen Zahlen und Funktionen*, Birkhäuser Verlag, Basel (1963).

[3] S. LANG, *Introduction to algebraic geometry*, Interscience Publishers, N° 5 (1958).

[4] P. ERDÖS, *On a tauberian theorem connected with the new proof of the prime number theorem*, « Jour. Ind. Math. Soc. », XIII, 133–147 (1949).

[5] E. WIRSING, *Elementare Beweise des Primzahlsatzes mit Restglied*. II (in corso di stampa).