BOLLETTINO
UNIONE MATEMATICA
ITALIANA

LUIGI CAMPEDELLI

Una generalizzazione dell'indicatore $\varphi(n)$ del Gauss e un problema di geometria sopra una curva ellittica

Bollettino dell'Unione Matematica Italiana, Serie 2, Vol. **1** (1939), n.5, p. 473–478.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_1939_2_1_5_473_0>

Bollettino dell'Unione Matematica Italiana, Unione
Matematica Italiana, 1939.

Una generalizzazione dell'indicatore $\varphi(n)$ del Gauss e un problema di geometria sopra una curva ellittica.

Nota di L. Campedelli (a Firenze).

Sunto. - *Se* P *è un punto di una curva ellittica, si determina il numero dei punti* n-*pli della serie lineare* $g_n^{n-1} = |nP|$, *che non sono anche* h-*pli per una* $g_h^{h-1} = |hP|$, *con* h *divisore di* n. *Si giunge così ad una funzione aritmetica che dà una prima estensione dell'indicatore* $\varphi(n)$. *Si applica il risultato ottenuto ad un problema relativo alla serie segata sopra una cubica ellittica piana, dalle curve di dato ordine.*

1. In una nota apparsa nel primo fascicolo di questo « Bollettino », il prof. Conforto ha mostrato come, partendo da un problema di *bisezione* della serie canonica sopra una curva, s'incontri un'interessante identità aritmetica, facile a dimostrarsi [1].

Le ricerche numerative nel campo della Geometria algebrica, portano assai di frequente, per il gioco che vi hanno i numeri interi, a questioni di pertinenza della « Teoria dei numeri ». Vogliamo qui darne un esempio che, pur non essendo del tutto nuovo, potrà presentare qualche interesse.

2. Ecco di che si tratta.

Se n è un numero intero, e $p_1, p_2, \ldots, p_t$, sono i suoi fattori primi, il numero dei numeri primi con n e minori di n stesso, è dato dall'indicatore $\varphi(n)$ del Gauss. Se si domanda il numero $\varphi_2(n)$ delle coppie (ordinate) di numeri (distinti o no) non maggiori di n, il cui massimo comun divisore è primo con n, si trova una *fun-*

[1] Cfr. F. Conforto, *Un'identità aritmetica che si presenta nella geometria algebrica* (questo « Bollettino », serie II, anno I, n. 1, 1939-XVII).

zione aritmetica (²):

$$\varphi_2(n) = n^2\left(1-\frac{1}{p_1{}^2}\right)\left(1-\frac{1}{p_2{}^2}\right)\cdots\left(1-\frac{1}{p_t{}^2}\right), \tag{1}$$

la cui espressione è del tutto analoga a quella della $\varphi(n)$.

Più in generale, si ha che il numero $\varphi_k(n)$ dei gruppi ordinati di k numeri (distinti o no), non maggiori di n, il cui massimo comun divisore è primo con n, è dato da:

$$\varphi_k(n) = n^k\left(1-\frac{1}{p_1{}^k}\right)\left(1-\frac{1}{p_2{}^k}\right)\cdots\left(1-\frac{1}{p_t{}^k}\right). \tag{2}$$

E se ci interessa avere il numero dei gruppi di k numeri (distinti o no), non maggiori di n, che insieme ad n costituiscono $k+1$ numeri aventi come massimo comun divisore un numero assegnato d (divisore di n), dovremo sostituire in luogo di n il rapporto $\frac{n}{d}$ (e intendere che p_i siano i fattori primi del nuovo argomento).

Ebbene, nella geometria sopra una curva algebrica, questa funzione aritmetica $\varphi_k(n)$ s'incontra nel problema della determinazione del numero di certe trasformazioni cicliche secondo n sopra una curva di genere $\frac{k}{2}$ (³), ossia, sotto diverso aspetto, per $k=2$, nella ricerca di taluni particolari punti n–pli di una serie lineare, g_n^{n-1}, di gruppi di n punti sopra una curva ellittica (⁴).

3. Soffermiamoci su quest'ultima questione.

Sopra la curva ellittica C, prendiamo un punto P e consideriamo la serie lineare $g_n^{n-1} = |nP|$, d'ordine n e di dimensione $n-1$, individuata dal punto P contato n volte. Come è noto la g_n^{n-1} possiede n^2 punti n–pli, tra i quali si trova il punto P. Se h è un divisore di n $(n=ht)$ la serie $g_h^{h-1} = |hP|$ possiede h^2 punti h–pli, ciascuno dei quali, contato t volte, dà un punto n-plo della $g_n^{n-1} = |nP|$.

Ci domandiamo allora: quanti sono i punti n–pli della $g_n^{n-1} = |nP|$

(²) Cfr. L. Carlini, *Sopra un problema della teoria dei numeri* (« Periodico di Matematiche », anno VI, 1891); E. Cesàro, *A proposito d'una generalizzazione della funzione φ di Gauss* (ibid., anno VII, 1892).

(³) Cfr. G. Castelnuovo, *Memorie scelte* (Bologna, 1937-XV). Mem. I (1888) e VII (1893).

(⁴) Cfr. L. Campedelli, *Sulle superficie di ordine* 2n *con otto punti* n-*pli* (« Atti della R. Acc. delle Scienze di Torino », vol. 71, 1936-XIV).

che non sono anche punti di molteplicità h per una serie $g_h^{h-1} = |hP|$, con h divisore di n? Troveremo che il numero richiesto è dato dalla (1).

Indichiamo con u l'*integrale ellittico di prima specie* (con i *periodi* ω e ω') definito sulla curva ellittica C, e si supponga che nel punto P sia:

$$u \equiv 0 \qquad (\text{mod. } \omega, \omega').$$

Allora nei gruppi dei punti della $g_n^{n-1} = |nP|$ è:

$$\sum_{i=1}^{i=n} u_i \equiv 0 \qquad (\text{mod. } \omega, \omega').$$

ed i suoi punti n-pli cadono nei punti della C nei quali si ha:

$$u \equiv r\frac{\omega}{n} + s\frac{\omega'}{n} \qquad (\text{mod. } \omega, \omega'). \tag{3}$$

dove r ed s assumono tutti i valori $0, 1, \dots, n-1$, o — ciò che è lo stesso, ma più comodo per il seguito — i valori: $1, 2, \dots, n$.

Analogamente, nei punti dei gruppi della $g_h^{h-1} = |hP|$ si ha:

$$\sum_{i=1}^{i=h} u_i \equiv 0 \qquad (\text{mod. } \omega, \omega').$$

e i punti h-pli sono dati da:

$$u \equiv r'\frac{\omega}{h} + s'\frac{\omega'}{h} \qquad (\text{mod. } \omega, \omega') \tag{4}$$

$$(r' = 1, 2, \dots h; \quad s' = 1, 2, \dots, h).$$

Quindi dalla (3) si ottiene un punto n-plo della $g_n^{n-1} = |nP|$ che *non* è h-plo per una $g_h^{h-1} = |hP|$ con h divisore di n, cioè che non è anche un punto (4), per ogni coppia ordinata (r, s), con r ed s non divisibili ambedue per uno stesso divisore di $n (= ht)$.

Contiamo allora il numero di codeste coppie (r, s). Per questo cominciamo col ricercare quante fra le n^2 coppie (r, s) sono costituite da numeri multipli di p_1. I multipli di p_1 non maggiori di n, sono:

$$p_1, 2p_1, \dots, \frac{n}{p_1}p_1,$$

cioè in numero di $\frac{n}{p_1}$, e con essi si possono formare

$$\left(\frac{n}{p_1}\right)^2$$

coppie (r, s). Quindi le coppie (r, s) con r ed s non divisibili per p_1, sono in numero di

$$(5) \qquad n^2 - \left(\frac{n}{p_1}\right)^2 = n^2\left(1 - \frac{1}{p_1^2}\right).$$

Passiamo a contare quante fra le coppie (5), sono formate da numeri divisibili per p_2 (e non per p_1). Con i multipli di p_2 (non maggiori di n) si possono formare $\left(\frac{n}{p_2}\right)^2$ coppie ordinate (r, s), ma tra queste se ne hanno

$$\left(\frac{n}{p_1 p_2}\right)^2$$

costituite da multipli di p_1 e di p_2, e quindi non computate in (5). Per conseguenza le coppie (r, s) i cui elementi non sono divisibili nè per p_1 nè per p_2, sono in numero di:

$$n^2\left(1 - \frac{1}{p_1^2}\right) - \left(\frac{n}{p_2}\right)^2 + \left(\frac{n}{p_1 p_2}\right)^2 = n^2\left(1 - \frac{1}{p_1^2}\right)\left(1 - \frac{1}{p_2^2}\right).$$

Così continuando, o, se si preferisce, procedendo per induzione, si trova che il numero delle coppie ordinate (r, s) di numeri non maggiori di n, ed il cui massimo comun divisore è primo con n, è dato appunto dalla funzione aritmetica $\varphi_2(n)$ definita dalla (1).

4. Il ragionamento svolto è un'immediata estensione di quello che si segue di solito per determinare l'*indicatore* $\varphi(n)$ del GAUSS [5], e del tutto analoghe sono le proprietà della $\varphi(n)$ e della $\varphi_2(n)$.

Limitiamoci a ricordare la più importante, che per noi è una immediata conseguenza del significato geometrico che abbiamo trovato per la (1). Si deduce infatti da questo che *la somma dei valori della funzione aritmetica* $\varphi_2(h)$ *relativa a tutti i divisori di un numero intero* n, *è uguale a* n^2*:*

$$\Sigma\varphi_2(h) = n^2,$$

ossia, come si dice col linguaggio della teoria dei numeri:

L'integrale numerico della $\varphi_2(n)$ *è uguale ad* n^2.

Questa proprietà caratterizza la $\varphi_2(n)$, cioè dalla sola conoscenza di questo fatto, da noi acquisito *a priori*, si sarebbe potuti pervenire a scrivere l'espressione della $\varphi_2(n)$ stessa, in base ad un noto risultato del DEDEKIND [6], al quale qui si è preferito non fare ricorso per restare in un campo più elementare.

[5] Cfr., p. es., P. G. LEJEUNE DIRICHLET, *Lezioni sulla teoria dei numeri*, pubblicate da R. DEDEKIND (trad. A. FAIFOFER), § 11 e sgg. (Venezia, 1881).

[6] Cfr. DIRICHLET, op. cit., appendice VII. Vedi anche CESÀRO, loc. cit..

5. All' espressione (2) della $\varphi_k(n)$ si giunge estendendo in modo ovvio le considerazioni aritmetiche del n. 3, mediante le quali si è stabilita la (1).

6. Applichiamo il risultato ottenuto ad un problema che, per meglio lumeggiarne l' interesse, conviene presentare sotto forma proiettiva. Sia ancora C una curva ellittica, che, per semplicità, supponiamo priva di punti multipli, e quindi di ordine m in un iperspazio ad $m-1$ dimensioni, anzi, per metterci nel caso più semplice possibile, prendiamo addirittura una cubica piana, C_3. Si consideri allora la serie lineare g_{3n}^{3n-1} segata sulla C_3 dalle curve piane F_n, d' ordine n. La g_{3n}^{3n-1} possiede $9n^2$ punti $3n$-pli, che sono segnati sulla C_3 dalle F_n aventi con la C_3 stessa un contatto $3n$-punto, cioè d' ordine $3n-1$.

Ebbene, diremo che un punto Q, $3n$-plo della g_{3n}^{3n-1}, *appartiene all' ordine* n, quando tra le F_n che hanno in Q un contatto $3n$-punto con la C_3, non ne è alcuna costituita da una F_h (con h divisore di $n=ht$) contata t volte.

I punti $3n$-*pli della* g_{3n}^{3n-1} *appartenenti all' ordine* n, *sono in numero di*

$$3^2\varphi_2(n).$$

Sia P un flesso della cubica, e, come è lecito, prendiamo in esso per l' integrale ellittico u il valore:

$$u \equiv 0 \qquad (\text{mod. } \omega,\ \omega').$$

Allora nei punti dei gruppi della g_{3n}^{3n-1} segata dalle F_n, si ha:

$$\sum_{i=1}^{i=3n} u_i \equiv 0 \qquad (\text{mod. } \omega,\ \omega'). \tag{6}$$

e se h è un divisore di $n(=ht)$, per la g_{3h}^{3h-1} segata dalle F_h è:

$$\sum_{i=1}^{i=3h} u_i \equiv 0 \qquad (\text{mod. } \omega,\ \omega'). \tag{7}$$

I punti $3n$-pli della (6) appartenenti ad n, sono dunque quelli che non provengono dal contare t volte un punto $3h$-plo di una serie come la (7). Possiamo allora applicare il risultato ottenuto nel n. 3? Evidentemente solo quando le serie (7) diano tutte le serie multiple di P e sottomultiple della (6), o, comunque, quando nessuna delle serie $g_k^{k-1} = |kP|$ (con k divisore di $3n$) abbia tra i suoi punti k-pli dei punti che siano anche $3n$-pli per la g_{3n}^{3n-1}, appartenenti all' ordine n.

Ma per la $g_k^{k-1} = |kP|$ (con k divisore di $3n$) possono presentarsi i tre casi seguenti:

a) la g_k^{k-1} è una delle serie (7);

b) la g_k^{k-1} non è una delle (7), ma lo è un suo multiplo (diverso dalla g_{3n}^{3n-1});

c) nessun multiplo della g_k^{k-1} (diverso dalla g_{3n}^{3n-1}) è una serie (7).

Nel caso b) i punti k-pli della g_k^{k-1}, contati convenientemente. dànno altrettanti punti $3n$-pli della (6), ma non appartenenti all'ordine n, in quanto quei punti si ritrovano fra i punti $3h$-pli di una (o più) serie (7).

Nel caso c) invece tra i punti k-pli della g_k^{k-1}, ne sono alcuni che contati m volte (con $3n = km$) dànno dei punti $3n$-pli della g_{3n}^{3n-1} appartenenti all'ordine n.

Quindi se, per qualunque k divisore di $3n$, si verificano i casi a) e b), il numero ricercato è:

$$\varphi_2(3n). \tag{8}$$

Se invece per qualche k si presenta il caso c), il numero dei punti $3n$-pli della g_{3n}^{3n-1}, appartenenti all'ordine n, è maggiore di quello dato dalla (8).

Ma affinchè si verifichi il caso c), occorre e basta che sia $k = n$ e che n non sia multiplo di tre. In tal caso i punti della g_n^{n-1} che, contati tre volte, dànno dei punti $3n$-pli per la g_{3n}^{3n-1} appartenenti all'ordine n, sono in numero di $\varphi_2(n)$. Quindi il numero totale dei predetti punti $3n$-pli per la g_{3n}^{3n-1} è:

$$\varphi_2(3n) + \varphi_2(n),$$

e poichè n è primo con 3, si ha:

$$\varphi_2(3n) + \varphi_2(n) = 3^2\varphi_2(n).$$

La (8) risponde invece al nostro problema nel solo caso in cui n sia multiplo di tre, nel quale è ancora:

$$\varphi_2(3n) = 3^2\varphi_2(n).$$

Si giunge così alla conclusione enunciata, con un risultato che è facile estendere dalla cubica piana ad una curva ellittica iperspaziale.