Bollettino
Unione Matematica
Italiana

Ferenc Karteszi

Intorno a certi cicli di n punti su di un ellisse

Bollettino dell'Unione Matematica Italiana, Serie 1, Vol. **14** (1935), n.2, p. 83–86.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_1935_1_14_2_83_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 1935.

Intorno a certi cicli di n punti su di un'ellisse.

Nota di FERENC KÀRTESZI (a Györ - Ungheria).

Sunto. - *Risolvendo una questione di teoria dei numeri, si determina quanti sono i cicli di* n *punti su di un'ellisse* Γ, *tali che il circolo osculatore a* Γ *in un qualunque punto di uno di tali cicli, abbia a passare pel punto del ciclo ad esso successivo.*

Si vogliano determinare i cicli di n punti distinti

$$P_1 \equiv P_{n+1}, \quad P_2, \quad P_3, \dots, \quad P_n$$

di un'ellisse Γ (che non si riduca ad una circonferenza), tali che il circolo osculatore a Γ in P_i tagli ancora Γ precisamente nel punto P_{i+1} (per $i = 1, 2, \dots, n$). Qui mostreremo come questo problema possa venir ricondotto a quello della *divisione della circonferenza in* $3^n - (-1)^n$ *parti uguali*; proveremo inoltre ch'esso ammette sempre *soluzioni tutte distinte e costituite da punti reali, in numero di*:

$$\frac{1}{n}\left\{ 3^n - \sum_i 3^{\frac{n}{p_i}} + \sum_{j,h} 3^{\frac{n}{p_j p_k}} - \dots + (-1)^r 3^{\frac{n}{p_1 p_2 \cdots p_r}} \right\},$$

ove $p_1, p_2, \ldots, p_r$ sono i divisori primi di n (distinti dall'unità), e le sommatorie vanno estese alle combinazioni degli indici $1, 2, \ldots, r$ ad 1 ad 1, a 2 a 2, ecc..

1. Consideriamo la circonferenza $\mathcal{C}$ avente per diametro l'asse maggiore di Γ, e sia Ω una delle omologie ortogonali affini che mutano Γ in $\mathcal{C}$. Senza scapito di generalità potremo supporre che $\mathcal{C}$ sia di raggio unitario, talchè — riferita $\mathcal{C}$ agli assi di Γ — sarà lecito rappresentare i punti di $\mathcal{C}$ (al modo di ARGAND e GAUSS) coi numeri complessi z di modulo uguale ad 1.

Presi su Γ due punti P_1 e P_2, di cui z_1 e z_2 siano gli omologhi su $\mathcal{C}$ secondo Ω, se il circolo osculatore a Γ in P_1 passa per P_2, dovranno — in base ad un noto teorema di SIMSON [1] — la tangente in P_1 a Γ e la retta P_1P_2 risultare equinclinate sopra un asse di Γ; e viceversa. In forza della Ω, ciò equivale a supporre che la tangente in z_1 a $\mathcal{C}$ e la retta z_1z_2 siano equinclinate su quell'asse, il che — in virtù di proprietà elementari del cerchio — si traduce analiticamente colla:

$$z_2 = z_1^{-3} \quad [2].$$

Il problema posto in principio, è quindi così ridotto alla determinazione di n numeri complessi distinti (aventi modulo unitario):

$$(1) \qquad z_1, \quad z_2, \quad z_3, \ldots, \quad z_n.$$

legati dalle:

$$(2) \qquad z_2 = z_1^{-3}, \quad z_3 = z_2^{-3}, \ldots, \quad z_n = z_{n-1}^{-3}, \quad z_1 = z_n^{-3}.$$

Ciascuno di essi deve ovviamente verificare la

$$(3) \qquad z^{(-3)^n} = z,$$

ossia è una radice dell'unità d'indice $3^n - (-1)^n$; e con ciò quel problema è precisamente ricondotto alla divisione di $\mathcal{C}$ in $3^n - (-1)^n$ parti uguali. La condizione che due qualunque dei numeri complessi (1) siano fra loro distinti, equivale al fatto che essi verifichino la (3) senza che per uno di essi in pari tempo risulti

$$z^{(-3)^m} = z, \qquad \text{con } m \text{ intero positivo} < n;$$

e di tale condizione passiamo ora ad occuparci.

[1] Cfr. p. es. F. SEVERI, *Complementi di geometria proiettiva* (Bologna, Zanichelli, 1906), p. 277.

[2] Anche quest'ultimo risultato è sostanzialmente noto: ved. F. JOACHIMSTHAL, *Démonstration d'un théorème de Mr. Steiner*, « Journ. für die reine und ang. Math. », t. 36 (1848), pp. 95-96.

2. Determiniamo, più generalmente, qual'è il numero $N(k, n)$ delle radici dell'equazione

(4) $$z^{k^n-1}=1, \quad (n, k \text{ interi}; n \geq 2, |k| \geq 2),$$

che non soddisfano ad alcuna equazione del tipo

(5) $$z^{k^m-1}=1, \quad \text{con } m \text{ intero positivo } < n.$$

Supposto intanto k positivo, e tenuto conto delle proprietà delle radici primitive dell'unità, è subito visto che una radice comune alle (4), (5) soddisfa pure la

(6) $$z^d=1,$$

ove d è m. c. d. dei numeri k^n-1, k^m-1; e viceversa, ogni radice della (6) verifica pure le (4), (5).

Osservando che d deve necessariamente dividere $k^{n-m}-1$ ed in virtù dell'algoritmo euclideo per la determinazione del m. c. d., si ha tosto che — denotando con δ il m. c. d. di m ed n — risulta:

$$d=k^\delta-1.$$

Dunque le radici della (4) in discorso, sono precisamente quelle che non verificano un'equazione della forma

$$z^{k^\delta-1}=1, \quad \text{con } \delta \text{ intero positivo } < n \text{ e } \textit{divisore di } n,$$

e cioè quelle che non soddisfano ad alcuna delle

(7) $$z^{k^{\frac{n}{p_i}}-1}=1 \qquad (\text{per } i=1, 2, \ldots, r),$$

ove $p_1, p_2, \ldots, p_r$ denotano i divisori primi (>1) di n.

Se le (7) non avessero a due a due radici comuni, il numero $N(k, n)$ sarebbe manifestamente

(8) $$(k^n-1)-\sum_i\left(k^{\frac{n}{p_i}}-1\right).$$

Ma poichè, per $r>1$, le equazioni (7) che corrispondono a valori j, h diversi fra loro dell'indice i, hanno precisamente in comune le radici dell'equazione

$$z^{k^{\frac{n}{p_j p_h}}-1}=1 \qquad (j, h=1, 2, \ldots, r),$$

così l'espressione (8) va modificata; e — in definitiva — con un procedimento di uso corrente in teoria dei numeri, si ricava che è:

$$N(k, n)=(k^n-1)-\sum_i\left(k^{\frac{n}{p_i}}-1\right)+\sum_{j,h}\left(k^{\frac{n}{p_j p_h}}-1\right)-\ldots+(-1)^r\left(k^{\frac{n}{p_1 p_2 \cdots p_r}}-1\right)$$

ossia, in base all'identità

$$\binom{r}{0} - \binom{r}{1} + \binom{r}{2} - \ldots + (-1)^r \binom{r}{r} = 0,$$

si ottiene:

$$N(k, n) = k^n - \sum_i k^{\frac{n}{p_i}} + \sum_{j,h} k^{\frac{n}{p_j p_h}} - \ldots + (-1)^r k^{\frac{n}{p_1 p_2 \cdots p_r}}.$$

Quando si supponga k negativo, valgono ancora considerazioni analoghe alle precedenti; e si giunge in tal guisa alla *formula*

$$N(k, n) = |k|^n - \sum_i |k|^{\frac{n}{p_i}} + \sum_{j,h} |k|^{\frac{n}{p_j p_h}} - \ldots + (-1)^r |k|^{\frac{n}{p_1 p_2 \cdots p_r}},$$

valida in ogni caso. Per $k = -3$, essa fornisce il risultato geometrico enunciato in principio.

3. Chiudiamo questa breve Nota con un'osservazione. Se $z = z_1$ è una qualunque delle $N(k, n)$ radici della (4) di cui al n. 2, ad essa resta associato un ciclo di n radici $z_1, z_2, \ldots, z_n$, soddisfacenti alle condizioni

$$z_2 = z_1^k, \quad z_3 = z_2^k, \ldots, \quad z_n = z_{n-1}^k, \quad z_1 = z_n^k,$$

che generalizzano le (2). Si prova facilmente che tale ciclo consta di n radici fra loro distinte ed appartenenti tutte al gruppo delle $N(k, n)$ suddette, e ch'esso risulta univocamente determinato da una qualunque delle sue radici. Ne consegue che:

Se $p_1, p_2, \ldots, p_r$ *denotano i divisori primi (diversi dall'unità) di un intero* $n \geq 2$, *e se* k *è un qualunque numero intero positivo, risulta*

$$k^n - \sum_i k^{\frac{n}{p_i}} + \sum_{j,h} k^{\frac{n}{p_j p_h}} - \ldots + (-1)^r k^{\frac{n}{p_1 p_2 \cdots p_r}} \equiv 0 \pmod{n}.$$

Questo risultato ha una curiosa analogia col classico teorema di FERMAT:

$$k^{\varphi(n)} \equiv 1 \pmod{n} \qquad \text{per } k \text{ primo con } n,$$

ove:

$$\varphi(n) = n - \sum_i \frac{n}{p_i} + \sum_{j,h} \frac{n}{p_j p_h} - \ldots + (-1)^r \frac{n}{p_1 p_2 \cdots p_r},$$

e ad esso si identifica quando n è **primo**.