

Mauro Cerasoli e Franco Eugeni

Un'osservazione sulle disposizioni circolari.

Sommario. Si prova direttamente (1) la coincidenza tra la classica formula di Moreau (2) delle disposizioni circolari con ripetizione con quella derivante dal teorema di Polya (3). Si trovano anche legami aritmetico-funzionali tra dette disposizioni e quelle semplici, con funzioni espressioni la soluzione del classico problema delle collane aperiodiche.

* * *

È noto che se $m, n \in N_1 = \{1, 2, 3, \dots\}$, indicando con $\mathcal{D}_m(n)$ il numero delle disposizioni circolari con ripetizione di m oggetti di classe n (ad n ad n) si ha:

$$\mathcal{D}_m(n) = \sum_{p|n} \frac{1}{p} \sum_{d|p} \mu\left(\frac{p}{d}\right) m^d$$

la somma essendo estesa rispettivamente ai divisori p di n e d di p ed essendo μ la ben nota funzione di Möbius.

(1) Questa nota è nata da una strettissima collaborazione tra gli Autori nell'ambito degli Istituti matematici delle Facoltà di Scienze e Ingegneria dell'Univ. de L'Aquila e non è possibile discriminare i singoli contributi.

(2) Cfr. C. Moreau [1]. I numeri [1], [2], ... indicano i numeri d'ordine dei lavori riportati nella bibliografia.

(3) Cfr. L. Comtet [2].

Introdotte le funzioni aritmetiche:

$$\begin{aligned} N(n) &= n \\ u(n) &= 1 \\ D_m(n) &= m^N(n) = m^n \end{aligned} \quad \forall n \in N_1$$

$$\mu(n) = \begin{cases} (-1)^r & n = p_1 \dots p_r \text{ primi dist.} \\ 1 & n = 1 \\ 0 & \text{altrimenti} \end{cases}$$

dove m^n è il numero di disposizioni (rettilinee) con ripetizione di m oggetti ad n ad n , e ricordando che se $f, g \in N_1^c$ (\mathcal{C} campo complesso) si definisce il prodotto (4) alla Dirichlet ponendo:

$$(f \times g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

può scriversi:

$$\mathcal{D}_m = \frac{1}{N} (m^N \times \mu) \times u$$

da cui ricordando che si pone (5):

$$\begin{aligned} \partial f &= f \times \mu \\ \int f &= f \times u \end{aligned}$$

può scriversi essendo u l'inversa della μ :

$$\partial \mathcal{D}_m = \frac{1}{N} \partial m^N = \frac{1}{N} \partial D_m.$$

(4) Cfr. F. Pellegrino [3].

(5) F. Eugeni [6] cfr. la (3, 4) e la nota (16).

Del resto seguendo Mac Mahon (6) e più recentemente Polya (7) può anche dirsi che è:

$$\mathcal{D}_m(n) = \frac{1}{n} \sum_{d|n} \varphi\left(\frac{n}{d}\right) m^d$$

e quindi:

$$\mathcal{D}_m = \frac{1}{N} (\varphi \times m^N).$$

Proviamo direttamente l'identità dei secondi membri delle formule esprimenti \mathcal{D}_m .

Poichè N è una funzione incondizionatamente (o completamente) moltiplicativa (8), essa è distributiva rispetto al prodotto alla Dirichlet e si ha:

$$N \mathcal{D}_m = m^N \times \mu \times Nu = m^N \times \mu \times N = m^N \times \varphi,$$

e pertanto è provata la coincidenza dei secondi membri delle formule di Moreau e di Polya.

Per proseguire le nostre considerazioni è indispensabile, sia pur trascurando gli ovvii dettagli, trattare a sommi capi la soluzione di Rota (comunicataci verbalmente) del problema delle collane aperiodiche.

Siano $D = \{1, 2, 3, \dots, n\}$, R un insieme di cardinalità m ed $f, g \in R^D$. Si pensi agli elementi di D come vertici di un poligono regolare di n vertici ed agli elementi di R come m tipi di perline (o colori) da sistemare nei vertici del poligono, così da formare *collane*: una $f \in R^D$ può essere pensata come una collana. Se C_n è il *gruppo ciclico* generato dalla permutazione $(123 \dots n)$ allora si dirà che

(6) Mac Mahon [5].

(7) L. Comtet [2] (cfr. pag. 263 opera citata).

(8) F. Pellegrino [4] (cfr. la (17, 2) e teorema seguente).

f e g sono in relazione \sim se esiste una $\sigma \in C_n$ tale che $f\sigma = g$. Si prova facilmente che \sim è una relazione d'equivalenza e chiamo *modello* una classe di equivalenza. Diremo che $f \in R^D$ è *aperiodica* se:

$$f\sigma = f \Rightarrow \sigma = \varepsilon$$

dove ε è la permutazione identica di C_n . Una $f \in R^D$ è *periodica* se esiste almeno un $\sigma \in C_n$, $\sigma \neq \varepsilon$ tale che $f\sigma = f$. Si prova agevolmente che:

$$G_f = \{\sigma \in C_n : f\sigma = f\}$$

è un *sottogruppo* di C_n . Possiamo così associare ad $f \in R^D$ il sottogruppo G_f che chiameremo il *periodo* di f . Le funzioni periodiche corrispondono così biunivocamente ai sottogruppi di C_n e quindi ai divisori di n .

Ad ogni sottogruppo G di C_n associamo i due numeri $f(G)$ e $g(G)$ così definiti:

$f(G)$ = il numero di funzioni di periodo G ,

$g(G)$ = il numero di funzioni il cui periodo contiene G come sottogruppo.

Allora sarà:

$$g(G) = \sum_{H \supseteq G} f(H)$$

essendo H un sottogruppo di C_n e quindi per il teorema d'inversione di Rota (9) risulta:

$$f(G) = \sum_{H \supseteq G} g(H) \mu(G, H)$$

(9) G.C. Rota [6]. Si tratta del teorema d'inversione che generalizza il classico teorema d'inversione di Möbius nel prodotto di Dirichlet all'algebra introdotta da Rota.

dove μ è la funzione (9) di Möbius-Rota del reticolo dei sottogruppi di C_n . Se $G = \{\varepsilon\}$ è il sottogruppo di C_n costituito dalla sola identità, allora $f(\{\varepsilon\})$ è il numero di funzioni aperiodiche. Se il sottogruppo H è di ordine d , un divisore di n , allora $g(H) = m^{n/d}$. Inoltre il reticolo dei sottogruppi di C_n è isomorfo al reticolo dei divisori di n e pertanto (9) è:

$$\mu(\{\varepsilon\}, H) = \mu(1, d) = \mu(d)$$

quindi:

$$f(\{\varepsilon\}) = \sum_{d|n} \mu(d) m^{n/d}$$

è il numero di funzioni aperiodiche definite su un n -insieme ed a valori in un m -insieme rispetto al gruppo ciclico C_n . Denotato con $\mathcal{A}_m(n)$ tale numero, può dirsi che:

$$\mathcal{A}_m = m^N \times \mu = \partial m^N = \partial D_m$$

Segue anche invertendo (10) secondo Möbius:

$$\int \mathcal{A}_m = \mathcal{A}_m \times u = D_m.$$

Indicato ora con $M_m(n)$ il numero di modelli aperiodici di funzioni da un n -insieme in un m -insieme rispetto al gruppo C_n , si ha:

$$M_m(n) = \frac{1}{n} \sum_{d|n} \mu(d) m^{n/d}$$

(10) Il principio d'inversione di Möbius con il nostro simbolismo dice che se $G = \int g$ allora $g = \partial G$. Cfr. ad esempio F. Eugeni [6].

e quindi:

$$M_m = \frac{1}{N} (\mu \times m^N) = \frac{1}{N} \partial D_m$$

ed essendo

$$\frac{1}{N} \partial D_m = \partial \mathcal{D}_m$$

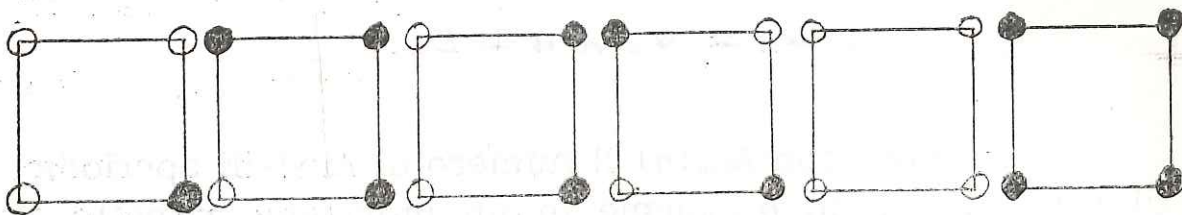
si ha

$$M_m = \partial \mathcal{D}_m$$

ed invertendo secondo Möbius:

$$\mathcal{D}_m = \int M_m = M_m \times u.$$

Ad esempio per $m = 2$ ed $n = 4$ risulta $\mathcal{D}_2(4) = 6$ ed $M_2(4) = 3$, quelle di fig. 1 sono le collane o disposizioni circolari, di due oggetti a quattro a quattro, le prime 3 essendo quelle aperiodiche, ed R è un insieme di due colori, atto a caratterizzare in figura le ripetizioni.



Si noti inoltre che se n è primo, diciamo p , allora la espressione di $M_m(n)$ diventa:

$$\begin{aligned} \frac{1}{p} \sum_{d|p} \mu(d) m^{p/d} &= \frac{1}{p} [\mu(1) m^p + \mu(p) m] = \\ &= \frac{1}{p} (m^p - m) = \frac{m}{p} (m^{p-1} - 1) \end{aligned}$$

e quest'ultimo è un naturale. Se p è primo con m allora esso deve dividere $m^{p-1}-1$, pertanto segue:

$$p \text{ primo, } (m, p) = 1 \implies m^{p-1} \equiv 1 (p)$$

ritrovando così il classico Teorema di Fermat sulle congruenze per via combinatoria.

Ci sembra possa valere la pena di indagare ulteriormente nel significato di analoghe formule che estendano quelle trovate ai razionali, nell'ordine di idee di quanto ha fatto B. RIZZI (cfr. [7]).

- [1] C. Moreau, *Sur les permutations circulaires distinctes*, Nouvelles Annales de M., 11 (1872), 309-314.
- [2] L. Comtet, *Advanced Combinatorics*, D. Ridel, Pub. 1974.
- [3] F. Pellegrino, *Lineamenti di una teoria delle funzioni aritmetiche*, Rend. Mat. e Appl. (5) 15 (1976).
- [4] F. Pellegrino, *Elementi moltiplicativi dell'anello delle funzioni aritmetiche*, Rend. di Mat., vol. 26, 1967.
- [5] P.A. Mac-Mahon, *Proc. London Math. Soc.* 23 (1891-2), 305-313.
- [6] G.C. Rota, *Theory of Mobius functions*, Z. Wahrsch. 2 (1964 b) 340-368.
- [6] F. Eugeni, *Numeri primitivi e indicativi generalizzati*, Rend Matematica, vol. 6 serie VI, Roma (1973).
- [7] B. Rizzi, *Sull'estensione delle nozioni di condizionata ed incondizionata additività*, La Ricerca, gen.-apr. 1977.