Rendiconti di Matematica
(2) 1983 Vol. 3, Serie VII

Sulla probabilità del *k-MCD* di *m* naturali scelti a caso

di **M. CERASOLI - F. EUGENI** (L'Aquila) - **B. RIZZI** (Roma)

SUMMARY - *In this paper a probabilistic application of the classical Möbius function appears. We assign a probability measure on the naturals with the aid of the Riemann zeta function. Therefore we find the probability that the k-MCD of m naturals chosen at random belong to a prefixed set. So we discover again a result by de Finetti and we generalize another result by Cesaro in number theory. The evaluation of these probabilities utilizes Dirichlet series and thus a convolution algebra.*

1. La probabilità di Dirichlet.

Sia A una parte dell'insieme $\mathbf{N}=\{1, 2, ...\}$ dei numeri naturali. Come è noto (cfr. BACLAWSKI-ROTA [2]), si può dare un significato alla frase «la probabilità che un naturale scelto a caso in **N** appartenga ad A è uguale ad α» definendo sia la misura di probabilità, sia la locuzione «scelto a caso». Preso **N** come spazio delle alternative, rappresentante l'evento certo, la *densità aritmetica* $d(A)$ dell'insieme A è definita (se si indica con $|E|$ la cardinalità dell'insieme E)

$$d(A)=\lim_{n\to\infty}\frac{1}{n}|\{1, 2, ..., n\}\cap A|$$

quando il limite esiste finito. La densità aritmetica tuttavia, non è una misura di probabilità (almeno secondo il significato più diffuso di questa terminologia), non essendo ad esempio σ-additiva. È noto comunque (cfr. ad es. [9]) che se p e q sono primi distinti ed M_p, M_q indicano rispettivamente gli insiemi dei multipli di p e q, si ha $d(M_p\cap M_q)=d(M_p)\,d(M_q)$. Nasce quindi l'esigenza di definire su **N** una misura di probabilità che goda di una proprietà analoga alla

precedente, per la quale cioè gli eventi M_p ed M_q siano *stocasticamente indipendenti.*

Una siffatta misura di probabilità si può definire ricorrendo alla funzione *zeta* di Riemann

$$\zeta(s)=\sum_{n\in\mathbf{N}} n^{-s}, \quad s>1.$$

Prefissati infatti un numero reale $s>1$ e una parte A di **N**, consideriamo l'evento, che indichiamo ancora con A, «un naturale scelto a caso in **N** appartiene ad A». La probabilità di A è definita ponendo:

$$P_s(A)=\sum_{n\in A} n^{-s}/\zeta(s).$$

Si verifica facilmente che P_s è una misura di probabilità su **N** tale che

$$P_s(M_p\cap M_q)=P_s(M_p)\,P_s(M_q)$$

quali che siano i primi distinti p e q.

Se $\mathcal{B}(\mathbf{N})$ è la σ-algebra di Boole delle parti di **N**, lo spazio di probabilità $(\mathbf{N}, \mathcal{B}(\mathbf{N}), P_s)$ sarà detto *spazio di probabilità di Dirichlet* e P_s *probabilità di Dirichlet.* Così per l'evento A, la locuzione «scelto a caso» significa che la probabilità di A è presa nella famiglia continua di Dirichlet al variare di $s>1$.

Si può inoltre affermare [2] che tutte le volte che $d(A)$ esiste, risulta

$$\lim_{s\to 1+} P_s(A)=d(A).$$

2. Probabilità del *k-MCD* di m naturali scelti a caso.

Ricordiamo ora che per *k-MCD* (cfr. COHEN [7]), $k\geq 1$, di $m\geq 1$ naturali $x_1, x_2, \ldots, x_m$ si intende *il più grande divisore comune degli m numeri, che sia potenza k-esima. Si indica con*

$$D_{m,k}=(x_1, x_2, \ldots, x_m)_k.$$

Per $k=1$ si ha il *MCD* e per $m=1$, $(x_1)_k$ è il massimo divisore di x_1 che sia potenza k-esima.

Vogliamo determinare, operando in $(\mathbf{N}, \mathcal{B}(\mathbf{N}), P_s)$, la probabilità dell'evento $(D_{m,k}\in A_k)$=«scelti a caso $m\geq 1$ naturali, il loro *k-MCD*,

$k \geq 1$, appartiene ad un prefissato insieme A_k di potenze k-esime». Pertanto sia X_1 la variabile aleatoria intera definita su $\mathbf{N}$ con distribuzione di probabilità

$$P_s(X_1=k)=P_s(\{k\})=k^{-s}/\zeta(s).$$

La variabile aleatoria X_1 prende il valore k se il numero estratto a caso da $\mathbf{N}$ è k. Fissato $a \in \mathbf{N}$ sia $(a|X_1)$ l'evento «a divide X_1». Allora

$$P_s(a \mid X_1)=P_s(X_1=ka \text{ per qualche } k \in \mathbf{N})$$

$$=P_s\Big(\bigcup_{k \in \mathbf{N}} (X_1=ka)\Big)=\sum_{k \in \mathbf{N}} (ka)^{-s}/\zeta(s) = a^{-s}.$$

Consideriamo ora le variabili aleatorie $X_1, X_2, \ldots, X_m$ tra loro indipendenti ed equidistribuite con X_1, e sia D_m il loro *MCD*. La probabilità che a divida D_m è

$$P_s(a \mid D_m)=\prod_{j=1}^{m} P_s(a \mid X_j)=a^{-ms}. \tag{2.1}$$

Per determinare la probabilità che $a \mid D_{m,k}$ occorre una caratterizzazione dei divisori del *k-MCD*. A tale riguardo introduciamo la *funzione aritmetica* q_k, $k \geq 1$, che ad ogni $a \in \mathbf{N}$ associa il minimo naturale r tale che ar sia un potenza k-esima. Si ha quindi il

LEMMA. 2.1. *La funzione q_k è moltiplicativa, cioè*

$$(a, b)=1 \Rightarrow q_k(ab)=q_k(a)\, q_k(b) \tag{2.2}$$

ma non completamente moltiplicativa per $k \geq 2$. Risulta, per $a \in \mathbf{N}$

$$q_k(a)=\begin{cases} \prod_{pr \,\|\, a,\ r \neq ck} p^{k-r} & k \geq 2 \\ 1 & k=1 \end{cases} \tag{2.3}$$

DIM. Siano $a, b \in N$ con $(a, b)=1$; si può scrivere

$$a=p_1^{a_1} \ldots p_h^{a_h} c^k, \quad a_i \equiv r_i \pmod{k}, \quad 0<r_i<k;$$

$$b=q_1^{b_1} \ldots q_s^{b_s} d^k, \quad b_i \equiv t_i \pmod{k}, \quad 0<t_i<k.$$

Pertanto $q_k(a)=p_1^{k-r_1} \ldots p_h^{k-r_h}$, $q_k(b)=q_1^{k-t_1} \ldots q_s^{k-t_s}$ e calcolato $q_k(ab)$ seguono (2.2) e la (2.3). Per $k \geq 2$ si ha $q_k(p^k)=1$, p primo, mentre

è $q_k(p)=p^{k-1}$ e dunque $q_k(p^k)\neq q_k(p)^k$, che dimostra la non completa moltiplicatività di q_k.

Sussiste ora il seguente lemma che caratterizza i divisori del *k-MCD.*

LEMMA. 2.2. *Dati m naturali* $x_1, \dots, x_m$, *per ogni* $k\in N$ *risulta la seguente equivalenza*

$$a \mid (x_1, \dots, x_m)_k \Leftrightarrow aq_k(a) \mid x_i \quad \forall\, i=1,2,\dots,m. \tag{2.4}$$

DIM. Se $aq_k(a)|x_i$, per essere $aq_k(a)$ una potenza k-esima risulta anche $(x_1, \dots, x_m)_k=b^k aq_k(a)$, $b\geq 1$, dunque $a|D_{m,k}$. Inversamente se $a|D_{m,k}$, poiché $D_{m,k}|D_m$ e $D_m|x_i$ per $i=1,\dots,m$, si ha intanto che $a|x_i$ e quindi $x_i=y_i a$. Ora se $a|(ay_1, \dots, ay_m)_k$ segue che necessariamente $q_k(a)|y_i$. Infatti posto per $a>1$,

$$a=p_1^{t_1} p_2^{t_2} \dots p_s^{t_s} b^k, \text{ con } b\geq 1,\ t_i\geq 0,$$

$(p_i, a)=1$, $t_i=h_i k+r_i$, $r_i\neq 0$ è $q_k(a)=p_1^{k-t_1} \dots p_s^{k-t_s}$.

Dall'ipotesi $(ay_1, \dots, ay_m)_k = ha$ e per essere ha un potenza k-*ma* risulta $h=h_1 q_k(a)$ da cui $h_1 q_k(a)|y_i a$, $h_1 q_k(a)|y_i$, $q_k(a)|y_i$.

Possiamo ora dimostrare il

TEOREMA. 2.1. *La distribuzione di probabilità del k-MCD delle variabili aleatorie* $X_1, X_2, \dots, X_m$, *è*

$$P_s(D_{m,k}=a^k)=a^{-kms}/\zeta(kms). \tag{2.5}$$

DIM. Con riferimento alla (2.1) si ha

$$P_s(a|D_{m,k})=\prod_{j=1}^{m} P_s(aq_k(a)|X_j)=(aq_k(a))^{-s}.$$

Consideriamo adesso per $t\in\mathbf{N}$ l'evento $B_t=$«a^t divide $D_{m,k}$». La probabilità che a^t sia la massima potenza di a che divide $D_{m,k}$ è quindi:

$$P_s(B_t\cap B^c_{t+1})=P_s(B_t)-P_s(B_t\cap B_{t+1})=$$

$$=[a^t q_k(a^t)]^{-ms}-[a^{t+1} q_k(a^{t+1})]^{-ms}=$$

$$=a^{-tms}[q_k(a^t)^{-ms}-(aq_k(a^{t+1}))^{-ms}].$$

La probabilità (2.5) che si vuol calcolare è invece il prodotto delle probabilità che ogni numero primo abbia in $D_{m,k}$ la stessa massima

potenza che ha nella fattorizzazione canonica di a^k.

Se per ogni p primo è $\alpha(p, a) \geq 0$ il massimo esponente con cui p appare nella fattorizzazione di a, e quindi $\alpha(p, a)\, k$ è quello che appare in a^k, avremo:

$$P_s(D_{m,k}=a^k)=\prod_p p^{-\alpha(p,a)kms}\left[q_k\left(p^{\alpha(p,a)k}\right)^{-ms}-\right.$$

$$\left.-q_k\left(p^{\alpha(p,a)k+1}\right)^{-ms}p^{-ms}\right]=a^{-kms}\prod_p\left[1-(p^{k-1})^{-ms}p^{-ms}\right]=$$

$$=a^{-kms}\prod_p(1-p^{-kms})=a^{-kms}/\zeta(kms).$$

Quando $k=1$, effettuato il limite per $s\to 1^+$ si ritrova il risultato: «la probabilità che m naturali scelti a caso in **N** abbiano il *MCD* uguale ad a è $a^{-m}/\zeta(m)$». Questa affermazione è stata ottenuta da B. de FINETTI [8] considerando lo spazio di equiprobabilità costruito sull'insieme finito $\{0, 1, \ldots, a-1\}$ delle classi di resto modulo a. Si veda anche CESARO [5].

Dal precedente teorema segue che se A_k è un insieme di potenze k-esime, allora

$$P_s(D_{m,k}\in A_k)=\sum_{n\in A_k} n^{-ms}/\zeta(kms). \tag{2.6}$$

Quando $k=1$ ed $s\to 1^+$ si ritrova, per $m=2$ il risultato di Cesaro [6]. Si noti che l'esistenza del $\lim_{s\to 1^+} P_s(D_{m,k}\in A_k)$ è assicurata a priori, tranne ovviamente il caso in cui sia $m=k=1$.

3. La densità di Cesaro generalizzata.

Sia $\{1, 2, \ldots, n\}^m$ l'insieme delle m-ple ordinate di naturali non superiori ad n, e sia A una parte arbitraria di **N**. La *densità di Cesaro* [6] $d_m(A)$ si costruisce considerando l'insieme $B_m(A)$ delle *m-ple* ordinate di naturali tali che il loro *MCD* sia in A e ponendo

$$d_m(A)=\lim_{n\to\infty} n^{-m}\left|\{1, 2, \ldots, n\}^m \cap B_m(A)\right|$$

quando il limite esiste finito.

Cesaro, facendo uso di questa definizione e della sua identità

$$(3.1) \qquad \sum_{x_1, \dots, x_m=1}^{n} F((x_1, \dots, x_m)) = \sum_{d=1}^{n} f(d) [n/d]^m$$

dove $[n/d]$ è la parte intera di n/d, f ed F sono funzioni aritmetiche tali che $F(n) = \sum_{d \mid n} f(d)$, ha dimostrato quanto segue.

Se F coincide con l'indicatore I_A di A e se $m \geq 2$ allora

$$(3.2) \qquad d_m(A) = \lim_{n \to \infty} n^{-m} \sum_{x_1, \dots, x_m=1}^{n} I_A((x_1, \dots, x_m)) = P_m(A)$$

sotto l'ipotesi che la funzione f associata ad $F = I_A$ sia limitata. Questa relazione generalizza al *MCD* nel caso di f limitata, la proposizione enunciata in [6] a proposito della densità dell'evento che un numero scelto a caso in **N** appartenga ad A e precisamente: «se la densità di A esiste, allora essa uguaglia il $\lim_{s \to 1+} P_s(A)$».

Introduciamo adesso una densità più generale, detta g-densità. Siano dati una funzione g: $\mathbf{N}^m \to \mathbf{N}$, ed una parte A di **N**. Sia $B_m(g, A)$ l'insieme delle m-ple $(x_1, \dots, x_m)$ di naturali non superiori ad n e tali che $g(x_1, \dots, x_m) \in A$. Definiamo allora la *g-densità inferiore* $d'_m(g, A)$ e la *g-densità superiore* $d''_m(g, A)$ rispettivamente ponendo

$$d'_m(g, A) = \min \lim_{n \to \infty} n^{-m} |\{1, 2, \dots, n\}^m \cap B_m(g, A)|$$

$$d''_m(g, A) = \max \lim_{n \to \infty} n^{-m} |\{1, 2, \dots, n\}^m \cap B_m(g, A)|.$$

Nel caso in cui i due limiti sono finiti e coincidono, ne indichiamo il valore comune con $d_m(g, A)$ e lo chiamiamo *g-densità* di A. Ci interesseremo in particolare del caso in cui $g(x_1, \dots, x_m) = (x_1, \dots, x_m)_k$, le cui densità corrispondenti indicheremo rispettivamente con $d'_{m,k}$, $d''_{m,k}$, $d_{m,k}$. Il seguente teorema costituisce nello stesso tempo la generalizzazione della formula di Cesaro (3.1) e di una identità di CASHWELL-EVERETT (cfr. [4]).

TEOREMA. 3.1. *Dati m, k, n, **N** sia $(x_1, \dots, x_m)$ una m-pla di naturali non superiori ad n ed*

$$M(n) = \max_{1 \leq x_i \leq n} \{(x_1, \dots, x_m)_k\}.$$

Inoltre se $1 \leq d \leq M(n)$ sia $N(d) = [n/(dq_k(d))]$. Se f, h sono funzioni aritmetiche ed $f * h$ è la convoluzione di Dirichlet definita da

$$(f*h)(n)=\sum_{d\mid n} f(d)\,h(n/d),$$

allora vale l'identità

$$\sum_{x_1,\dots,x_m=1}^{n}(f*h)((x_1,\dots,x_m)_k)=$$

$$=\sum_{d=1}^{M(n)} f(d)\sum_{x_1,\dots,x_m=1}^{N(d)} h(q_k(d)(x_1,\dots,x_m)_k).$$

DIM. Posto per brevità $D=(x_1,\dots,x_m)_k$, $M=M(n)$, si ha:

$$\sum_{x_i=1}^{n}(f*h)(D)=\sum_{x_i=1}^{n}\sum_{d\mid D} f(d)\,h(D/d)=\sum_{d=1}^{M} f(d)\sum_{x_i=1}^{n} v(D/d)$$

essendo v una funzione nulla sui razionali non interi e coincidente con h sui naturali. Per il lemma 2.2 i soli valori x_i che danno contributo a priori non nullo sono quelli per cui $dq_k(d)\mid x_i$ per $i=1,\dots,m$. Dunque nella seconda somma dell'ultimo membro sono significativi solo i termini relativi agli indici $x_i=y_i\,dq_k(d)$ per i quali gli y_i assumono i valori $1,2,\dots,N(d)$. Poiché $dq_k(d)$ è una potenza k-esima, è anche $D=(y_1,\dots,y_m)_k\,dq_k(d)$ e pertanto l'ultima espressione coincide con il secondo membro di (3.2).

Da questo teorema discendono due corollari che vale la pena di sottolineare.

COROLLARIO. 3.1. *L'identità* (3.2), *quando h coincide con la funzione u costantemente uguale ad* 1, *diviene, posto* $f*u=F$

$$\sum_{x_1,\dots,x_m=1}^{n} F((x_1,\dots,x_m)_k)=\sum_{d=1}^{M(n)} f(d)\,N(d)^m \tag{3.3}$$

che per $k=1$ *è l'identità di Cesaro* (3.1).

È sufficiente osservare che per $k=1$ è $M(n)=n$, $q_1(d)=1$.

COROLLARIO. 3.2. *L'identità* (3.2) *per* $m=1$ *diviene*

$$\sum_{a=1}^{n}(f*h)((a)_k)=\sum_{d=1}^{M(n)} f(d)\sum_{a=1}^{N(d)} h((a)_k\,q_k(a))$$

essendo $(a)_k$ *il più grande divisore di a che è una potenza k-esima, relazione che per* $k=1$ *si riduce alla identità di Cashwell-Everett.*

4. g-densità di particolari eventi.

Ci proponiamo ora, prefissato un insieme $A_k \subseteq \mathbf{N}$ di potenze k-esime, di determinare le g-densità $d'_{m,k}(A_k)$, $d''_{m,k}(A_k)$ dell'evento «il k-MCD di m naturali, scelti a caso in $\mathbf{N}$, appartiene ad A_k», evento che ha nello spazio di Dirichlet probabilità (2.6).

Cominciamo con l'osservare che se $(x_1, \dots, x_m)$ è una m-pla di $\{1, 2, \dots, n\}^m$ ed $M(n)$ è definito come nel teorema (3.1), allora

$$\min_{n \to \infty} \lim M(n) = \begin{cases} \infty & \text{se } k=1 \\ 1 & \text{se } k \geq 2 \end{cases}$$

$$\max_{n \to \infty} \lim M(n) = \infty .$$

È evidente il risultato per $k=1$ poiché in tal caso risulta $M(n)=n$. Per $k \geq 2$ si osservi che non esiste il limite di $M(n)$ per $n \to \infty$ in quanto, presi i due insiemi $\mathcal{J} = \{p_1, p_2, \dots\}$ dove p_n indica il numero primo n-esimo, e $Q_k = \{1, 2^k, 3^k, \dots\}$ si ha

$$\lim_{n \to \infty} M(n) = \begin{cases} 1 & \text{per } x_i \in \mathcal{J} \\ \infty & \text{per } x_i \in Q_k . \end{cases}$$

LEMMA. 4.1. *Per $k \geq 2$ sia A_k un insieme di potenze k-esime, I_k il suo indicatore ed $f_k = I_k * \mu$, dove μ è la funzione di Möbius classica. Allora $|f_k|$ è l'indicatore dell'insieme dei naturali che sono il prodotto di una potenza di A_k per un numero libero da quadrati.*

DIM. Sappiamo che se $k \geq 2$ ogni naturale n si può decomporre in un solo modo nel prodotto di una potenza a^k per un numero b_k libero da potenze k-esime. Dunque nel calcolo di

$$f_k(n) = (I_k * \mu)(n) = \sum_{d \mid n} I_k(d)\, \mu(n/d)$$

l'unico addendo, eventualmente significativo, che deve essere considerato è $I_k(a^k)\, \mu(b_k)$; negli altri infatti d non è una potenza k-esima oppure n/d non è libero da potenze k-esime. Dunque $f_k(n)$ vale 1 se $a^k \in A_k$ e b_k, libero da quadrati, è il prodotto di un numero pari di fattori primi (o si riduce all'unità); $f_k(n)$ vale -1 se $a^k \in A_k$ e b_k, libero da quadrati, è il prodotto di un numero dispari di fattori primi; $f_k(n)$

è nullo se $a^k \notin A_k$ oppure se b_k non è libero da quadrati. La funzione $|f_k|$ vale allora 1 in tutti gli n che sono il prodotto di un elemento di A_k per un numero libero da quadrati, zero nei rimanenti.

Notiamo che il lemma si estende solo parzialmente al caso $k=1$ poiché esistono insiemi A per i quali le funzioni $I_A * \mu = f_A$ non sono limitate. Ad esempio, se A è l'insieme dei numeri primi, ed $a = p_1 p_2 \dots p_n$ è il prodotto dei primi n primi, risulta

$$f_A(a) = (I_A * \mu)(a) = \sum_{i=1}^{n} I_A(p_i)\, \mu(a/p_i) = n(-1)^{n-1}.$$

Tuttavia se I_A è moltiplicativa, con il che lo è anche la corrispondente f_A, posto $n = \Pi p^{\alpha(p,n)}$, dalla relazione

$$f_A(n) = \prod_p f_A(p^\alpha) = \prod_p (I_A * \mu)(p^\alpha) = \prod_p [I_A(p^\alpha) - I_A(p^{\alpha-1})]$$

segue che f_A per $k=1$ è della stessa natura delle f_k del lemma 4.1. Esistono comunque anche indicatori non moltiplicativi per i quali f_A assume solanto i valori $-1, 0, 1$. Uno di questi è ad esempio l'indicatore dell'insieme $\{h\}$ con $h \neq 1$.

TEOREMA. 4.1. *Sia A_k un insieme di potenze k-esime, I_k il suo indicatore ed $f_k = I_k * \mu$. Se $m \geq 2$ si ha*

$$d'_{m,k}(A_k) = \begin{cases} \sum_{d \geq 1} f_1(d)\, d^{-m} & \text{se } k=1 \\ f_k(1) & \text{se } k \geq 2, \end{cases}$$

$$d''_{m,k}(A_k) = \sum_{d \geq 1} f_k(d)\, (q_k(d)\, d)^{-m}.$$

DIM. Sia $B_{m,k}(A_k)$ l'insieme delle m-ple con k-MCD in A_k, allora

$$|\{1, 2, \dots, n\}^m \cap B_{m,k}(A_k)| = \sum_{x_1, x_2, \dots, x_m = 1}^{n} I_k((x_1, \dots, x_m)_k).$$

Per il teorema d'inversione di Möbius risulta $I_k = f_k * u$ mentre per il Corollario 3.1 occorre valutare il

$$\lim_{n \to \infty} n^{-m} \sum_{d=1}^{M(n)} f_k(d)\, N(d)^m$$

che per la seguente relazione di CESARO [6] sulle parti intere:

$$\left[\frac{n}{r}\right]^m = \left(\frac{n}{r}\right)^m - m\varepsilon\left(\frac{n}{r}\right)^{m-1} \qquad \begin{matrix} 0<\varepsilon<1 \\ 1\leq r\leq n \end{matrix}$$

si riduce alla valutazione dei limiti

$$\lim_{n\to\infty} \sum_{d=1}^{M(n)} f_k(d)\,(dq_k(d))^{-m}, \quad \lim_{n\to\infty} \frac{1}{n} \sum_{d=1}^{M(n)} f_k(d)\,(dq_k(d))^{1-m}.$$

Si noti ora la diseguaglianza

$$|f_k(d)| \leq \Big|\sum_{q\mid d} \mu(q)\, I_k(q/d)\Big| \leq \sum_{q\mid d} 1^q \leq \tau(d)$$

dove $\tau(d)$ è il numero di divisori di d. Sia $k=1$, allora $M(n)=n$, $q_k(d)=1$ ed il primo limite converge in tal caso assolutamente a

$$\sum_{d\geq 1} f_k(d)\, d^{-m}$$

per la limitazione

$$\Big|\sum_{d=1}^{n} f_k(d)\, d^{-m}\Big| \leq \sum_{d\geq 1} \tau(d)\, d^{-m} = \zeta^2(m).$$

Per $k>1$ si ha invece

$$\min \lim_{n\to\infty} \sum_{d=1}^{M(n)} f_k(d)\,(dq_k(d))^{-m} = f_k(1)$$

e

$$\max \lim_{n\to\infty} \sum_{d=1}^{M(n)} f_k(d)\,(dq_k(d))^{-m} = \sum_{d\geq 1} f_k(d)\,(dq_k(d))^{-m}.$$

Il secondo limite tende a zero quando $n\to\infty$. Infatti per $m>2$ è $|f_k(d)|\leq\tau(d)$, come visto, e quindi

$$\sum_{d=1}^{M(n)} f_k(d)\,(dq_k(d))^{1-m} = \sum_{d\geq 1} \tau(d)\, d^{1-m} = \zeta^2(m-1).$$

Se $m=2$ può scriversi

$$\Big|\sum_{d=1}^{M(n)} f_k(d)\,(dq_k(d))^{-1}\Big| \leq \sum_{d=1}^{n} \tau(d)\, d^{-1};$$

per una nota formula asintotica (cfr. APOSTOL [1], pag. 70) risulta

$$\sum_{d=1}^{n} \tau(d)\, d^{-1} = \frac{1}{2}\log^2 n + 2\gamma \log n + 0(1)$$

essendo γ la costante di Eulero-Mascheroni. Quindi anche in questo caso il secondo limite tende a zero.

Il Teorema ora dimostrato costituisce, quando $k=1$ ed $m\geq 2$, un miglioramento della (3.1) di Cesaro, provata sotto l'ipotesi di f limitata. Nel Lemma 4.1 abbiamo provato che, se $k\geq 2$, f_k è necessariamente limitata, ma, come si è notato in precedenza, per $k=1$ ciò può non valere se f_k non è moltiplicativa. In conclusione possiamo affermare quanto segue.

PROPOSIZIONE. 4.1. *Per* $k=1$, $m\geq 2$ *la densità dell'evento «il MCD di m naturali scelti a caso appartiene ad un prefissato insieme A» esiste quale che sia A ed uguaglia il limite (per* $s\to 1^+$*) della probabilità di Dirichlet del medesimo evento.*

DIM. Infatti dal Teorema 4.1 risulta

$$d'_{m,1}(A) = d''_{m,1}(A) = \sum_{d\geq 1} f_1(d)\, d^{-m} = \sum_{d\geq 1} (I_A * \mu)(d)\, d^{-m}$$

$$= \sum_{a\in A} a^{-m}/\zeta(m)$$

e, d'altro canto, per la (2.6) si ha

$$\lim_{s\to 1^+} P_s(D_{m,1}\in A) = \lim_{s\to 1^+} \sum_{a\in A} a^{-ms}/\zeta(ms).$$

Il Teorema 4.1 per $k\geq 2$, $m\geq 2$ generalizza il risultato di Cesaro al $k-MCD$, ma in senso negativo, poiché come ora proveremo non esiste in tal caso la g-densità. Più precisamente vale il

TEOREMA. 4.2. *Per* $k\geq 2$, $m\geq 2$ *non esiste la g-densità dell'evento «il k-MCD di m naturali scelti a caso in* **N** *appartiene ad un prefissato insieme* A_k *di potenze k-esime»; inoltre la densità inferiore* $d'_{m,k}$ *coincide con il limite di* $P_s(D_{m,k}\in A_k)$ *per* $s\to 1^+$ *quando e solo quando* A_k *è l'insieme di tutte le potenze k-esime (evento certo). La densità superiore non può coincidere con il limite.*

DIM. Se per m, $k\geq 2$ risultasse $d'_{m,k}(A_k) = d''_{m,k}(A_k)$ devrebbe neces-

sariamente essere dal teorema 4.1.

$$\sum_{d\geq 1} f_k(d)\,(dq_k(d))^{-m}=f_k(1)$$

e quindi $f_k(d)=0$ per $d>1$. Allora $I_k(a)=\sum_{d\mid a} f_k(d)=f_k(1)$ per ogni $a\in\mathbf{N}$, dunque non potendo essere I_k identicamente nullo (A_k non è vuoto) è $f_k(1)=1$ ed I_k costantemente 1. Ma allora I_k indica N che non è un A_k.

Mostriamo adesso che il

$$\lim_{s\to 1^+}\sum_{a\in A_k} a^{-ms}/\zeta(mks)=\sum_{a\in A_k} a^{-m}/(mk)$$

coincide con $d'_{m,k}(A_k)$ se e solo se A_k è l'insieme di tutte le potenze k-esime. Consideriamo (cfr. [3]) la funzione

$$\mu_k(n)=\begin{cases}\mu(\sqrt[k]{n}) & \text{se } n=a^k \text{ per qualche } a\in\mathbf{N}\\ 0 & \textit{altrimenti.}\end{cases}$$

Si può allora scrivere, ricordando note proprietà della serie di Riemann,

$$\sum_{a\in A_k} a^{-m}/\zeta(mk)=\sum_{a\geq 1}\mu(a)\,a^{-mk}\sum_{b\geq 1} I_k(b)\,b^{-m}=\sum_{b\geq 1}(\mu_k * I_k)(b)\,b^{-m}.$$

Per coincidere tale limite con la densità inferiore deve essere $(\mu_k * I_k)(b)=0$ se $b>1$ ma poiché la precedente non può essere nulla anche in $b=1$, altrimenti per la legge di annullamento del prodotto di convoluzione sarebbe nulla anche I_k, è $\mu_k * I_k=\delta$, l'elemento neutro rispetto al prodotto di convoluzione. Ma allora per l'unicità dell'inversa di μ_k (che è l'indicatore $\square_k$ delle potenze k-esime, cfr. [3]), risulta $I_k=\square_k$. Resta da provare che il limite non può coincidere con la densità superiore, e cioè che non può esistere un I_k soddisfacente l'identità

$$I_k * \mu_k=(I_k * \mu)\,q_k^{-m} \tag{4.1}$$

da cui risulterebbe $f_k=I_k * \mu=q_k^m(I_k * \mu_k)$. Da questa relazione, poiché per il lemma 4.1 f_k assume i valori $-1, 0, 1$ segue che $f_k(a)=0$ se $a\neq b^k$. Dunque sotto tali ipotesi la (4.1) implica $(I_k * \mu)(a)=(I_k * \mu_k)(a)$ se $a=b^k$, $(I_k * \mu_k)(a)=(I_k * \mu)(a)$ se $a\neq b^k$. Dunque se I_k fosse l'eventuale indicatore tale che $f_k(a)=0$ se $a\neq b^k$, per questa funzione risulterebbe $I_k * \mu=I_k * \mu_k$ e quindi $\mu=\mu_k$, che è assurdo per $k\geq 2$.

BIBLIOGRAFIA

[1] T. M. Apostol: *Introduction to Analitic Number Theory,* Springer Verlag, 1976. Berlin.

[2] K. Baclawski - G. C. Rota: *An Introduction to Probability and Random Processes,* dispense, M. I. T.

[3] L. Berardi - F. Eugeni: *La derivata numerica ed applicazioni,* Per. di Mat. (5), (1979), 53-80.

[4] E. D. Cashwell - C. J. Everett: *The ring of number theoretic functions,* Pacific J. Math. 9, (1959), 975-985.

[5] E. Cesaro: *Probabilité de certaines faits arithmétiques,* Mathesis, 4 (1884), 233-235 (anche in Opere Scelte dell'U. M. I.).

[6] E. Cesaro: *Sur le plus grand diviseur de plusieurs nombres,* Ann. Mat. Pura e Appl., (2) 13 (1885), 291-294 (anche in Opere Scelte dell'U.M.I.).

[7] E. Cohen: *An extension of Ramanujan's sum, II,* Duke Math. J. 22 (1955) 543-550.

[8] B. De Finetti: *Probabilità che il massimo comun divisore di n numeri scelti ad arbitrio sia un numero dato,* Rend. R. Ist. Lomb. Sc. Let. II, LX (1927), 638-643.

[9] M. Kač: *Statistical Independence in Probability, Analysis and Number Theory,* Wiley, 1959, New York.

Lavoro pervenuto alla Redazione il 23 dicembre 1981
ed accettato per la pubblicazione il 30 aprile 1982
su parere favorevole di G. Koch e di R. Scozzafava.

Gubbio - Tipografia Oderisi Editrice - 1983