PROBABILITÀ CHE IL MASSIMO COMUNE DIVISORE DI *n* NUMERI SCELTI AD ARBITRIO SIA UN NUMERO DATO.

In: « *Rendiconti del R. Istituto Lombardo di Scienze e Lettere* », vol. LX, fasc. 11-15, Milano 1927, pp. 3-8.

REALE ISTITUTO LOMBARDO DI SCIENZE E LETTERE
Estratto dai *Rendiconti*. — Vol. LX — Fasc. XI-XV — 1927.

PROBABILITÀ CHE IL MASSIMO COMUNE DIVISORE DI n NUMERI SCELTI AD ARBITRIO SIA UN NUMERO DATO.

Nota di BRUNO DE FINETTI

ULRICO HOEPLI
LIBRAIO DEL R. ISTITUTO LOMBARDO DI SCIENZE E LETTERE
—
MILANO
1927

La probabilità che un numero sia divisibile per un numero assegnato, a, è $\frac{1}{a}$, se si considerano come casi ugualmente probabili gli a resti possibili.

La probabilità che n numeri siano contemporaneamente divisibili per il numero a, data l'indipendenza delle n probabilità, è $\left(\frac{1}{a}\right)^n$; la probabilità opposta $1 - \frac{1}{a^n}$.

La probabilità che α sia la massima potenza di a per cui n numeri sono contemporaneamente divisibili sarà uguale alla probabilità che essi siano divisibili per a^α moltiplicata per quella che, essendo divisibili per a^α, non lo siano anche per $a^{\alpha+1}$. Ma conosciamo la probabilità che gli n numeri siano divisibili per a^α, $a^{\alpha+1}$, e sono rispettivamente $\left(\frac{1}{a^\alpha}\right)^n$, $\left(\frac{1}{a^{\alpha+1}}\right)^n$, e quest'ultima è uguale al prodotto della probabilità che sussista la divisibilità per a^α, per quella che, verificata tale ipotesi sussista la divisibilità per $a^{\alpha+1}$. Quindi

$$\frac{\left(\frac{1}{a^{\alpha+1}}\right)^n}{\left(\frac{1}{a^\alpha}\right)^n} = \frac{1}{a^n}$$

è la probabilità che n numeri divisibili per a^α lo siano per $a^{\alpha+1}$, e la probabilità opposta che cercavamo è $1 - \frac{1}{a^n}$.

Quindi α ha la probabilità

$$\left(\frac{1}{a^{\alpha}}\right)^{n}\left(1-\frac{1}{a^{n}}\right)$$

di essere la massima potenza di a per cui n numeri sono divisibili, o, in altre parole, di essere la massima potenza di a nel massimo comune divisore degli n numeri, che indicheremo brevemente con D_n.

La probabilità $p_n(a)$ che $D_n = a$ sarà il prodotto delle probabilità indipendenti che ogni numero primo abbia in D_n la stessa massima potenza che in a, e, scomposto a in fattori primi:

$$a = \prod \left\{ h^{Mp(h,a)} \mid h,\ N_p \right\}$$

avremo:

$$p_n(a) = \prod \left\{ \left(\frac{1}{h^{Mp(h,a)}}\right)^{n}\left(1-\frac{1}{h^{n}}\right) \mid h,\ N_p \right\} =$$

$$= \prod \left\{ \left(\frac{1}{h^{Mp(h,a)}}\right)^{n} \mid h,\ N_p \right\} \prod \left\{ \left(1-\frac{1}{h^{n}}\right) \mid h,\ N_p \right\} =$$

$$= \left(\frac{1}{\prod \left\{ h^{Mp(h,a)} \mid h,\ N_p \right\}}\right)^{n} \prod \left\{ \left(1-\frac{1}{h^{n}}\right) \mid h,\ N_p \right\} = \frac{1}{a^{n}} \prod \left\{ \left(1-\frac{1}{h^{n}}\right) \mid h,\ N_p \right\}$$

e indicando

$$k_n = \prod \left\{ \left(1-\frac{1}{h^{n}}\right) \mid h,\ N_p \right\}$$

$$\underline{\underline{p_n(a) = k_n\, a^{-n}.}} \quad (*)$$

k_n rappresenta la probabilità che $D_n = 1$, ossia la probabilità che n numeri siano primi tra loro: $k_n = p_n(1)$.

Possiamo trovare facilmente un modo di esprimere k_n mediante una serie. Osserviamo che D_n è sempre un numero naturale, e quindi la somma delle $p_n(a)$ variando a nei numeri naturali dovrà dare 1:

$$\sum_{a=1}^{\infty} p_n(a) = 1.$$

$$\sum_{a=1}^{\infty} p_n(a) = \sum_{a=1}^{\infty} k_n\, a^{-n} = k_n \sum_{a=1}^{\infty} \frac{1}{a^{n}} = 1$$

$$k_n = \frac{1}{\sum_{a=1}^{\infty} \frac{1}{a^{n}}} = \frac{1}{1+\frac{1}{2^{n}}+\frac{1}{3^{n}}+\frac{1}{4^{n}}+\ldots}$$

(*) Il caso particolare $n=2$, $a=1$ costituisce il « problema di Tscebytsceff », che si enuncia di solito: *probabilità che una frazione sia irreducibile.*

e si ha quindi

$$p_n(a) = \frac{1}{a^n} \cdot \frac{1}{\sum_{h=1}^{\infty} \frac{1}{h^n}}.$$

La trasformazione del prodotto infinito in serie costituisce un noto teorema d'Eulero, al quale si deve anche la formola generale che dà k per indice pari

$$k_{2m} = \frac{(2m)!}{2^{2m-1} B_m \pi^{2m}} \qquad \text{(Peano, Form. Math. V § 4. 11 · 1) (*)}$$

In particolare:

$$k_2 = \frac{6}{\pi^2} = 0 \cdot 60793 \qquad k_4 = \frac{90}{\pi^4} = 0 \cdot 92394 \qquad \text{(Ibid. 7·3 e 7·4)}$$

Per n dispari si può interpolare fra k_{n-1} e k_{n+1}, perchè, se $n > m$, $k_n > k_m$. Si può dimostrare che, aumentando n, k_n tende a 1:

$$\lim_{n=\infty} k_n = 1.$$

Intanto è certo $k_n < 1$, perchè $\frac{1}{k_n} > 1$, qualunque sia n.

Dimostriamo ora che, assegnato un numero positivo ε comunque piccolo, esiste un numero naturale n per cui

$$k_n > 1 - \varepsilon.$$

Infatti, qualunque sia M:

$$\sum_{h=1}^{\infty} \frac{1}{h^n} = 1 + \sum_{h=2}^{M} \frac{1}{h^n} + \sum_{h=M+1}^{\infty} \frac{1}{h^n} < 1 + \sum_{h=2}^{M} \frac{1}{h^n} + \sum_{h=M+1}^{\infty} \frac{1}{h^2}.$$

$\sum_{h=M+1}^{\infty} \frac{1}{h^2}$ rappresenta il resto della serie $\sum_{h=1}^{\infty} \frac{1}{h^2}$, convergente, $\left(\text{la somma vale } \frac{\pi^2}{6}\right)$, e quindi esiste certo un numero M per cui $\sum_{h=M+1}^{\infty} \frac{1}{h^2} < \frac{\varepsilon}{2}$. Ora che M è un numero determinato consideriamo il termine

$$\sum_{h=2}^{M} \frac{1}{h^n}.$$

(*) Nel Formulario è attribuita ad Eulero solo la 7·3 relativa a k_2, e le altre a Bernoulli. Sono invece tutte di Eulero: cfr. G. Enestrom, Bibliotheca math., Serie II, T. 4, 1890, p. 22-24.

È certo

$$\sum_{h=2}^{M} \left(\frac{1}{h}\right)^n < (M-1)\left(\frac{1}{2}\right)^n$$

ed è noto che, essendo $\frac{1}{2} < 1$, si può sempre determinare n in modo che

$$\left(\frac{1}{2}\right)^n < \frac{\varepsilon}{2(M+1)}.$$

Allora

$$(M-1)\left(\frac{1}{2}\right)^n < \frac{\varepsilon}{2}$$

$$\sum_{h=2}^{M} \frac{1}{h^n} < \frac{\varepsilon}{2}.$$

Quindi per tali valori di M, n:

$$1 + \sum_{h=2}^{M} \left(\frac{1}{h}\right)^n + \sum_{h=M+1}^{\infty} \left(\frac{1}{h}\right)^2 < 1 + \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = 1 + \varepsilon$$

e a fortiori

$$\frac{1}{k_n} = \sum_{h=1}^{\infty} \frac{1}{h^n} < 1 + \varepsilon$$

e finalmente

$$k_n > \frac{1}{1+\varepsilon} > 1 - \varepsilon.$$

E ciò sussiste anche per tutti gli indici maggiori di n. Si ha

$$\lim_{n=\infty} k_n = 1 \qquad \text{c. v. d.}$$

Quindi

$$\lim_{n=\infty} p_n(a) = \begin{cases} 1 & a = 1 \\ 0 & a \neq 1. \end{cases}$$

Più in generale, invece della probabilità che D_n sia uguale a un numero dato, potremo cercare la probabilità che D_n goda di certe proprietà, ossia che appartenga a una certa classe di numeri u. Se u è una classe di numeri interi, la probabilità che D_n sia un u è

$$p_n(u) = \Sigma\,[p_n(a) \mid a, u] = k_n\,\Sigma\left[\frac{1}{a^n} \mid a, u\right].$$

Consideriamo qualche caso più interessante.

1. Probabilità che D_n sia potenza di a (escluso $a^0 = 1$), ove $a > 1$.

$$p_n(a^N) = k_n \Sigma \left[\frac{1}{b^n} \mid b, a^N \right] = k_n \sum_{h=1}^{\infty} \frac{1}{a^{hn}} = k_n \sum_{h=1}^{\infty} \left(\frac{1}{a^n} \right)^h = \frac{k_n}{a^n - 1} .$$

La probabilità che D_n sia una potenza di a maggiore di a è

$$p_n(a^{1+N}) = p_n(a^N) - p_n(a) = k_n \left(\frac{1}{a^n - 1} - \frac{1}{a^n} \right) = \frac{k_n}{a^n (a^n - 1)} .$$

2. Probabilità che D_n sia una potenza emmesima

$$p_n(N^m) = k_n \Sigma \left[\frac{1}{a^n} \mid a, N^m \right] = k_n \sum_{h=1}^{\infty} \frac{1}{h^{mn}} = k_n \frac{1}{k_{mn}} .$$

Sarà più interessante considerare la probabilità che D_n sia una potenza emmesima esclusa l'unità:

$$p_n([1 + N]^m) = p_n(N^m) - p_n(1) = k_n \left(\frac{1}{k_{mn}} - 1 \right) = k_n \frac{1 - k_{nm}}{k_{nm}} .$$

Ad esempio la probabilità che D_n sia un numero quadrato (escluso $1^2 = 1$) è

$$p_n([1 + N]^2) = k_n \frac{1 - k_{2n}}{k_{2n}} ;$$

per $n = 2$

$$p_2([1 + N]^2) = k_2 \frac{1 - k_4}{k_4} = \frac{\pi^2}{15} - \frac{6}{\pi^2} = 0{\cdot}05005.$$

La probabilità che il m. c. d. di due numeri sia un quadrato perfetto (1 escluso) è 0·05005.

3. Probabilità che D_n sia numero primo

$$p_n(N_p) = k_n \left(\frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{5^n} + \frac{1}{7^n} + \frac{1}{11^n} + \frac{1}{13^n} + \ldots \right)$$

Eseguendo il calcolo di $p_2(N_p)$ sui primi 33 numeri naturali si ha

$$0{\cdot}273 < p_2(N_p) < 0{\cdot}287.$$

Approssimativamente il m. c. d. D_2 di due numeri ha le probabilità

0·61 0·28 0·11

di essere 1, numero primo, numero composto.

4. Probabilità che D_n sia multiplo di a. Si verifica, eseguendo la sommatoria, che è $p_n(a \times N) = a^{-n}$, come si sapeva già.

In particolare:

probabilità che D_n sia pari : $p_n(2 \times N) = \left(\frac{1}{2}\right)^n$

" " " " dispari : $p_n(2 \times N_0 + 1) = 1 - \left(\frac{1}{2}\right)^n$

" " " " " e maggiore di 1 : $p_n(2 \times N + 1) = 1 - \left(\frac{1}{2}\right)^n - k_n$.

Così:

$p_2(2 \times N) = 0{\cdot}25$	$p_2(2 \times N_0 + 1) = 0{\cdot}75$	$p_2(2 \times N + 1) = 0{\cdot}142$
$p_4(2 \times N) = 0{\cdot}0625$	$p_4(2 \times N_0 + 1) = 0{\cdot}9375$	$p_4(2 \times N + 1) = 0{\cdot}01356$

Milano, 23 marzo 1927. V.