BOLLETTINO UNIONE MATEMATICA ITALIANA

GIOVANNI RICCI

Sul teorema di Dirichlet relativo alla progressione aritmetica

Bollettino dell'Unione Matematica Italiana, Serie 1,
Vol. **12** (1933), n.5, p. 304-309.

Unione Matematica Italiana

<[http:
//www.bdim.eu/item?id=BUMI_1933_1_12_5_304_0](http://www.bdim.eu/item?id=BUMI_1933_1_12_5_304_0)>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

*Articolo digitalizzato nel quadro del programma
bdim (Biblioteca Digitale Italiana di Matematica)
SIMAI & UMI*

<http://www.bdim.eu/>

Sul teorema di Dirichlet relativo alla progressione aritmetica.

Nota di GIOVANNI RICCI (a Pisa).

Sunto. - *Si dimostra, semplicemente e senza far uso della teoria dei caratteri (mod. a), un teorema che si accosta a quello classico di DIRICHLET relativo all'esistenza di infiniti numeri primi in una progressione aritmetica; precisamente si dimostra l'esistenza in ogni tale progressione di infiniti numeri della forma np (p primo, $n \leq \alpha$, α confine superiore precisato). Quando la differenza della progressione sia uno qualunque degli interi 4, 5, 6, 9, 10, 12, 15, 18, 30 il confine superiore α risulta tale da garantire lo stesso risultato di DIRICHLET. Si espongono conseguenze.*

1. Un classico teorema di DIRICHLET assicura che nella progressione aritmetica $ax + b$ (a, b interi; $(a, b) = 1$; $x = 1, 2, 3, \dots$) esistono infiniti numeri primi; la dimostrazione di questo teorema è molto laboriosa e riposta⁽¹⁾, e i tentativi di dimostrarlo con mezzi più semplici hanno avuto successo, per quanto io sappia, soltanto per $b = 1$ e $b = -1$. Credo quindi che possa presentare interesse, per la sua semplicità e per il fatto che non ricorre alla teoria dei

⁽¹⁾ Ved. p. es. E. LANDAU, *Handbuch der Primzahlen*, 24 Kap., p. 422 e segg..

caratteri (mod. a), la dimostrazione del teorema che segue, il qual teorema pur rimanendo lontano dal risultato di DIRICHLET ci si accosta un pò e per qualche caso particolare ($a=4, 5, 6, 9, 10, 12, 18, 30$; b primo con a e del resto qualunque) arriva a dare lo stesso risultato di DIRICHLET.

Il teorema in questione è il seguente:

Siano a, b interi con $a > 0$ e $(a, b) = 1$. Nella progressione aritmetica

$$a + b, 2a + b, 3a + b, \dots$$

esistono infiniti numeri della forma np , dove p è primo e n (primo con a) non supera il numero

$$(1) \quad x = \frac{a}{\log a + C + \sum_{p|a} \frac{\log p}{p-1}},$$

dove $C = 0.5772\dots$ è la costante di EULER-MASCHERONI e la somma Σ si intende estesa a tutti i divisori primi p di a .

^{p^{ta}} Inoltre il numero $N(\eta)$ degl'interi positivi $ax + b \leq \eta$ della forma np sopradetta ha l'ordine di grandezza $\frac{\eta}{\log \eta}$.

2. Questo teorema permette anche di scegliere, fra le $\varphi(a)$ (φ indicatore di EULER) progressioni aritmetiche essenzialmente distinte corrispondenti ad uno stesso valore di a , alcune di esse in guisa da garantire che almeno una contiene infiniti numeri primi. Vale appunto il seguente corollario:

Se $n_1 = 1, n_2, \dots, n_r$ sono tutti gl'interi positivi non maggiori del numero x dato dalla (1) e primi con a , ed è $r > 1$, formiamo gli r loro prodotti ad $r-1$ ad $r-1$

$$m_1 = n_2 n_3 \dots n_r, \quad m_2 = n_1 n_3 \dots n_r, \dots, \quad m_r = n_1 n_2 \dots n_{r-1}; \quad (m_i = n_i m_i).$$

Se $(a, b) = 1$, una almeno delle r progressioni aritmetiche

$$ax + m_1 b, \quad ax + m_2 b, \dots, \quad ax + m_r b \quad (x=1, 2, 3, \dots)$$

contiene infiniti numeri primi.

Inoltre il numero complessivo degl'interi primi $\leq \eta$ contenuti in esse ha l'ordine di grandezza $\frac{\eta}{\log \eta}$.

Infatti detto $N_i(\eta)$ il numero degl'interi $\leq \eta$ della forma $n_i p$ ($i=1, 2, \dots, r$) contenuti nella progressione $ax + m_i b$, e posto $N(\eta) = \Sigma N_i(\eta)$, pel teorema precedente esistono tre numeri reali $\eta_0, \delta_1, \delta_2$ tali che per $\eta \geq \eta_0$ risulta

$$\delta_1 \frac{\eta}{\log \eta} < N(\eta) = \sum_{i=1}^r N_i(\eta) < \delta_2 \frac{\eta}{\log \eta}$$

e quindi almeno per un valore l dell'indice i risulta $N_l(\tau) \rightarrow +\infty$ per $\tau \rightarrow +\infty$.

Dall'uguaglianza $ax + m, b \equiv n, p$ segue

$$a \frac{x}{n_i} + m, b \equiv p$$

e inversamente: dunque $N_l(\tau)$ viene ad essere il numero degli interi primi $\leq \frac{\tau}{n_i}$ contenuti nella progressione $ax + m, b$. D'onde l'asserto.

3. Aggiungiamo le seguenti ovvie

OSSERVAZIONI. — a) Se $x_0(p)$ è il minimo intero positivo per cui $ax_0(p) + b \equiv 0 \pmod{p}$, con $p > a + |b|$, ($a > 0$), risulta $ax_0(p) + b \geq p$ e il teorema di DIRICHLET ci assicura che per infiniti valori di p vale il segno $\equiv$: val quanto dire

$$\lim_{p \rightarrow \infty} \frac{x_0(p)}{p} = \frac{1}{a}$$

Il teorema che ci proponiamo di dimostrare si può tradurre in una formula analoga, ma in generale più debole. Detto n_0 il massimo intero primo con a che non supera α , il nostro teorema ci assicura che è

$$\lim_{p \rightarrow \infty} \frac{x_0(p)}{p} \leq \frac{n_0}{a}$$

b) È evidente che ogni progressione aritmetica $cax + b$ (a, b, c interi; $(b, ac) = 1$) è contenuta nella progressione aritmetica $ax + b$. Inversamente, assegnato l'intero c e la progressione aritmetica $ax + b$ con $(a, b) = 1$, esiste almeno un intero b' , primo con ca , tale che la progressione aritmetica $cax + b'$ risulta contenuta nella data. Infatti basta assumere $b' = c_1 a + b$, dove c_1 è il prodotto dei divisori di c che non entrano in b , convenendo di porre $c_1 = 1$ se di tali divisori non ne esistono.

4. CONSEGUENZE. — Per $a = 12, 18, 30$ risulta rispettivamente $\alpha < 4, 5, 7$; si conclude che la forma np con $n < \alpha$ è possibile soltanto per $n = 1$. In base all'osservazione b) concludiamo:

Il numero $N(\tau)$ degli interi primi $\leq \tau$ contenuti in ciascuna progressione aritmetica $ax + b$, dove $(a, b) = 1$ ed a è uno qualunque degli interi

4, 5, 6, 9, 10, 12, 15, 18, 30

ha l'ordine di grandezza $\frac{\tau}{\log \tau}$.

Come esempio osserviamo il caso $a = 60$ per quale $\alpha < 12$. Pertanto:

In ogni progressione aritmetica $60x + b$, con $(60, b) = 1$, esistono infiniti numeri di una almeno delle tre forme p , $7p$, $11p$. Inoltre, una almeno delle tre progressioni aritmetiche $60x + 7b$, $60x + 11b$, $60x + 77b$ contiene infiniti numeri primi.

5. DIMOSTRAZIONE. — Per dare l'idea dei mezzi impiegati dirò subito che la dimostrazione si basa sulle quattro formule seguenti, nelle quali le somme sono estese a tutti i numeri primi p che soddisfano alle condizioni ivi indicate, e valevoli per $\xi \rightarrow +\infty$ ⁽¹⁾

$$(I) \quad \log([\xi]!) = \xi \log \xi - \xi + o(\xi) \quad (2)$$

$$(II) \quad \sum_{p \leq \xi} \log p = \xi + o(\xi)$$

$$(III) \quad \sum_{p \leq \xi} \frac{1}{p} = \frac{\xi}{\log \xi} + o\left(\frac{\xi}{\log \xi}\right)$$

$$(IV) \quad \sum_{p \leq \xi} \frac{\log p}{p-1} = \log \xi - C + o(1),$$

(C costante di EULER-MASCHERONI).

Che sia $N(\eta) = O\left(\frac{\eta}{\log \eta}\right)$ è evidente poichè (per la (III))

$$N(\eta) \leq \alpha \sum_{p \leq \eta} \frac{1}{p} = \frac{\alpha \eta}{\log \eta} + o\left(\frac{\eta}{\log \eta}\right) = O\left(\frac{\eta}{\log \eta}\right);$$

dunque il significato del teorema enunciato è

$$(2) \quad \frac{\eta}{\log \eta} = O(N(\eta)).$$

Si può supporre, senza alterare la generalità che sia $0 < b < a$. Consideriamo, per $\xi \geq a + 1$, il prodotto

$$A(\xi) = (a+b)(2a+b) \dots ([\xi]a+b).$$

Essendo $A(\xi) > a \cdot 2a \dots [\xi]a$ risulta per la (I)

$$\log A(\xi) > [\xi] \log a + \log([\xi]!) \geq (\xi - 1) \log a + \xi \log \xi - \xi + o(\xi)$$

da cui si ricava

$$(3) \quad \log A(\xi) \geq \xi \log \xi + (\log a - 1)\xi + o(\xi).$$

Andiamo a determinare una opportuna espressione maggiorante

(1) Ved. E. LANDAU, op. cit., p. 72, p. 195, p. 196, p. 200.

(2) Con $[\xi]$ si denota la parte intera del numero reale ξ .

per $\log A(\xi)$. Denotiamo con $l(p)$ l'esponente della massima potenza di p che divide $A(\xi)$, in guisa che è

$$(4) \quad \log A(\xi) = \sum_p l(p) \log p.$$

e valutiamo $l(p)$. Distinguiamo vari casi:

1°) Se p divide a , risulta $l(p) = 0$.

2°) Se $p > \xi$, abbiamo $p^2 > \xi^2 \geq (a+1)\xi > a[\xi] + b$, quindi tra i fattori di $A(\xi)$ uno al più è divisibile per p e nessuno lo è per p^2 . Risulta dunque $l(p) \leq 1$.

3°) Se $p \leq \xi$ e p non divide a , abbiamo evidentemente

$$l(p) \leq \left(\left\lfloor \frac{\xi}{p} \right\rfloor + 1 \right) + \left(\left\lfloor \frac{\xi}{p^2} \right\rfloor + 1 \right) + \dots + \left(\left\lfloor \frac{\xi}{p^k} \right\rfloor + 1 \right) < \xi \left(\frac{1}{p} + \frac{1}{p^2} + \dots \right) + k$$

dove k è tale che $p^{k+1} > a[\xi] + b$, cioè si può prendere

$$k = k(p, \xi) = \left\lfloor \frac{\log(a[\xi] + b)}{\log p} \right\rfloor.$$

Essendo $\log(a[\xi] + b) = \log \xi + O(1)$ si conclude che è

$$(5) \quad l(p) \leq \xi \frac{1}{p-1} + \frac{\log \xi + O(1)}{\log p}.$$

Sia $\beta \geq 1$ e denotiamo con $M_\beta(\xi)$ il numero dei divisori primi distinti del prodotto $A(\xi)$ tutti maggiori di $\beta\xi$. Per ciascuno di tali divisori primi risulta

$$l(p) = 1, \quad \log p = \log \xi + O(1).$$

Servendoci della (4) costruiamo l'espressione maggiorante cercata:

$$\begin{aligned} \log A(\xi) &= \sum_{p \leq \xi} l(p) \log p + \sum_{\xi < p \leq \beta\xi} l(p) \log p + M_\beta(\xi) \log \xi + O(1) \\ &\leq \xi \left\{ \sum_{p \leq \xi} \frac{\log p}{p-1} - \sum_{p/a \leq p \leq \xi} \frac{\log p}{p-1} \right\} + \log \xi + O(1) + \sum_{p \leq \xi} 1 - \sum_{p/a} 1 + \\ &+ \sum_{\xi < p \leq \beta\xi} \log p + M_\beta(\xi) \log \xi + O(1), \end{aligned}$$

e in base alle formule (II), (III), (IV) ricaviamo

$$\begin{aligned} \log A(\xi) &\leq \xi \left\{ \log \xi - C - \sum_{p/a \leq p \leq \xi} \frac{\log p}{p-1} + o(1) \right\} + \\ &+ \log \xi + O(1) \left\{ \frac{\xi}{\log \xi} + o\left(\frac{\xi}{\log \xi} \right) \right\} + \beta\xi - \xi + o(\xi) + M_\beta(\xi) \log \xi + O(1) \end{aligned}$$

da cui

$$\log A(\xi) \leq \xi \log \xi + \xi \left\{ \beta - C - \sum_{p/a \leq p \leq \xi} \frac{\log p}{p-1} \right\} + o(\xi) + M_\beta(\xi) \log \xi + O(1).$$

Confrontando questa con la (3) e tenendo conto della posizione (1) otteniamo

$$(6) \quad M_p(\xi) \geq \left(\frac{a}{\sigma} - \beta\right) \frac{\xi}{\log \xi} + o\left(\frac{\xi}{\log \xi}\right)$$

e quindi $\frac{\xi}{\log \xi} = O(M_p(\xi))$ tutte le volte che $\beta < \frac{a}{x}$.

Diciamo h il minimo intero primo con a e maggiore di α (1). Scegliamo β in guisa da avere

$$\frac{a}{x} > \beta > \frac{a}{h}.$$

Per ogni $\xi > \xi_0 = \frac{b}{\beta h - a}$ e ogni $x \leq [\xi]$ risulta

$$\frac{ax + b}{\beta \xi} \leq \frac{a[\xi] + b}{\beta \xi} \leq \frac{a}{\beta} + \frac{b}{\beta \xi} < \frac{a}{\beta} + \frac{b}{\beta \xi_0} = h;$$

si conclude che ad ogni fattore primo di $A(\xi)$ computato in $M_p(\xi)$ (e quindi maggiore di $\beta \xi$) corrisponde un termine della progressione aritmetica $ax + b$ avente la forma np con

$$p > \beta \xi, \quad n < h. \quad (n, a) = 1$$

e quindi anche $n \leq x$. Ricordando il significato del numero $N(\tau)$ che figura nell'enunciato, si conclude che non appena $\xi > \xi_0$ vale la limitazione $N(a[\xi] + b) \geq M_p(\xi)$, ed essendo $\beta < \frac{a}{x}$ per la (6) risulta

$$\frac{\xi}{\log \xi} = O(N(a[\xi] + b)),$$

e quindi anche la (2). Il teorema risulta così dimostrato.

(1) Si noti che per $a \geq 4$ risulta $\alpha < a - 1$, quindi questa scelta di R è possibile.