ALBERTO MARIO BEDARIDA

Sopra i numeri primi di due progressioni aritmetiche

Bollettino dell'Unione Matematica Italiana, Serie 1, Vol. **9** (1930), n.3, p. 144–148.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_1930_1_9_3_144_0>

Sopra i numeri primi di due progressioni aritmetiche.

Nota di A. M. Bedarida (a Genova).

Sunto. - *In questa Nota viene svolta un' applicazione del teorema che assegna i tipi di due progressioni aritmetiche che rappresentano gli stessi numeri primi; teorema stabilito dall' A. in un lavoro precedente. L' applicazione quì trattata riguarda uno studio sopra due progressioni aritmetiche, nelle quali i numeri primi di una di esse sono contenuti tutti nell' altra*

1. In questa Nota faremo un' applicazione del teorema che assegna i tipi di due progressioni aritmetiche che rappresentano gli stessi numeri primi. Questo teorema è stato stabilito nel mio lavoro: *Sopra le progressioni aritmetiche,* pubblicato nei « Rend. della R. Acc. delle Scienze Fis. e Mat. di Napoli » (1929). L'applicazione qui trattata riguarda uno studio sopra due progressioni aritmetiche, nelle quali i numeri primi di una di esse sono tutti contenuti nell'altra.

2. Si ha il teorema:

Se i numeri primi di una progressione aritmetica $\mathrm{m}x + \mathrm{r}$ *sono tutti contenuti in un'altra* $\mathrm{m}x' + \mathrm{r}'$, *sarà:* $\mathrm{m} \equiv 0 \pmod{m'}$ *ed* $\mathrm{r} - \mathrm{r}' \equiv 0 \pmod{m'}$; *escluso sia* $\mathrm{m} \equiv 1 \pmod{2}$ *e* $\mathrm{m}' \equiv 2 \pmod{4}$, *in cui sarà invece:* $\mathrm{m} \equiv 0 \left(\mathrm{mod.}\ \frac{m'}{2}\right)$, $\mathrm{m} \not\equiv 0 \pmod{m'}$ *ed* $\mathrm{r} - \mathrm{r}' \equiv 0 \left(\mathrm{mod.}\ \frac{m'}{2}\right)$ [1].

Sia δ il massimo comun divisore di m ed m': la progressione aritmetica $\frac{mm'}{\delta}x + r' + m'\gamma$, ove γ è una soluzione di una certa congruenza lineare, contiene tutti e soli i numeri primi comuni alle due considerate [2]. Allora, segue che le due progressioni aritmetiche:

$$(1) \qquad mx + r, \quad \frac{mm'}{\delta}x + r' + m'\gamma,$$

hanno gli stessi numeri primi. Per il teorema più sopra ricordato, (si osservi che il termine iniziale della seconda delle (1) può essere ridotto $\left(\mathrm{mod.}\ \frac{mm'}{\delta}\right)$, aggiungendo un conveniente multiplo di $\frac{mm'}{\delta}$) si potranno avere i due casi:

1°) le progressioni (1) siano identiche. Allora sarà:

$$m = \frac{mm'}{\delta}, \quad r = r' + m'\gamma + h\,\frac{mm'}{\delta},$$

quindi $\delta = m'$ e perciò:

$$m \equiv 0 \pmod{m'} \quad \text{con} \quad r - r' \equiv 0 \pmod{m'}.$$

2°) Le progressioni (1) non siano identiche. Allora, le ragioni dovranno essere una dispari, l'altra il doppio di questa, i termini iniziali uguali, oppure, quella la cui ragione è pari avrà quello dell'altra, aumentato della ragione di questa. Andiamo a vedere

(1) Tacitamente, si intenderà, che nelle progressioni aritmetiche qui considerate, i termini iniziali siano minori delle rispettive ragioni.

(2) Cfr. la mia Nota: *Sopra i sistemi di progressioni aritmetiche.* (« Rend. Acc. Lincei », 1929, 1° semestre).

intanto che, nel caso delle (1), non potrà aversi che $m \equiv 1 \pmod{2}$ e $\frac{mm'}{\delta} \equiv 0 \pmod{2}$ con $\frac{mm'}{\delta} \not\equiv 0 \pmod{4}$. Invero, se fosse $m \equiv 0$. $(\mathrm{mod.}\ 2)$ con $m \not\equiv 0 \pmod{4}$ e $\frac{mm'}{\delta} \equiv 1 \pmod{2}$, risultando $mm' \equiv \delta \equiv 0 \pmod{2}$, sarà anche $m' \equiv 0 \pmod{2}$, quindi dovrebbe essere $\delta \equiv 0 \pmod{4}$ e perciò $m \equiv 0 \pmod{4}$, il che non può aversi; perchè allora le (1) sarebbero identiche [1]. Nel caso attuale si ha dunque:

$$m \equiv 1 \pmod{2} \quad \text{e} \quad \frac{mm'}{\delta} \equiv 2 \pmod{4},$$

onde sarà:

$$m' \equiv 2 \pmod{4} \quad \text{e} \quad 2m = \frac{mm'}{\delta},$$

$$r = r' + m'\gamma + h\frac{mm'}{\delta} \quad \text{oppure} \quad r + m = r' + m'\gamma + h\frac{mm'}{\delta};$$

ossia:

$$\delta = \frac{m'}{2}, \quad r - r' \equiv 0 \left(\mathrm{mod.}\ \frac{m'}{2}\right);$$

perciò:

$$m \equiv 0 \left(\mathrm{mod.}\ \frac{m'}{2}\right), \; m \not\equiv 0 \ (\mathrm{mod.}\ m') \quad \text{con} \quad r - r' \equiv 0 \left(\mathrm{mod.}\ \frac{m'}{2}\right). \text{ C.v.d.}$$

3. Come corollario risulta:

Se i numeri primi di una progressione aritmetica $\mathrm{mx} + \mathrm{r}$ *sono tutti contenuti in un'altra* $\mathrm{m'x} + \mathrm{r'}$ *ed almeno una rappresenta il numero* 2, *allora è sempre* $\mathrm{m} \equiv 0\ (\mathrm{mod.}\ m')$, $\mathrm{r} - \mathrm{r'} \equiv 0\ (\mathrm{mod.}\ m')$.

Invero, in tale ipotesi, non può aversi $m' \equiv 2 \pmod{4}$, perchè la progressione $m'x + r'$ non rappresenterebbe numeri primi.

4. Notiamo che per m' pari, il caso $m \equiv 0 \left(\mathrm{mod.}\ \frac{m'}{2}\right)$ con $m \not\equiv 0$ $(\mathrm{mod.}\ m')$, contemplato nel teorema ora dimostrato è *l'unico*, perchè per $\frac{m'}{2} \equiv 0 \pmod{2}$, cioè $m' \equiv 0 \pmod{4}$, sarà m pari: allora le (1) non potranno essere che identiche e perciò, necessariamente, con $m \equiv 0 \left(\mathrm{mod.}\ \frac{m'}{2}\right)$ sarebbe anche $m \equiv 0\ (\mathrm{mod.}\ m')$. E risulterà allora $m \equiv 0 \pmod{4}$; si potrà quindi dire: *Se una progressione aritmetica* $\mathrm{mx} + \mathrm{r}$ *ha i suoi numeri primi tutti contenuti in un'altra* $\mathrm{m'x} + \mathrm{r'}$ *e la ragione di questa è multipla di* 4, *anche la ragione della prima sarà multipla di* 4.

[1] Cfr. la mia Nota cit. nei « Rend. dell'Acc. di Napoli », [n.i 2 e 7, 2)].

Si osservi che questa multiplicità di 4 non è, in generale, invertibile.

5. Il teorema del n.° 2 si può invertire in questo modo:
Se in due progressioni aritmetiche mx + r, m'x + r' *si ha:*

$$m \equiv 0 \pmod{m'}, \quad r - r' \equiv 0 \pmod{m'};$$

oppure:

$$m \equiv 0 \left(\mathrm{mod.}\ \frac{m'}{2}\right), \quad m \not\equiv 0 \pmod{m'}, \quad r - r' \equiv 0 \left(\mathrm{mod.}\ \frac{m'}{2}\right)$$

con m' ≡ 2 (mod. 4) *e se la progressione* mx + r *ha numeri primi, ne avrà anche la progressione* m'x + r' *e tra questi vi saranno tutti quelli della prima.*

Se $m \equiv 0 \pmod{m'}$, $r - r' \equiv 0 \pmod{m'}$ è chiaro che ogni numero rappresentato dalla prima è pure rappresentato dalla seconda; in particolare, avendo la prima numeri primi, risulterà r' primo con m', quindi avrà pure numeri primi la seconda e tra questi vi saranno tutti quelli della prima. Se poi è $m \equiv 0 \left(\mathrm{mod.}\ \frac{m'}{2}\right)$, $m \not\equiv 0 \pmod{m'}$, $r - r' \equiv 0 \left(\mathrm{mod.}\ \frac{m'}{2}\right)$, $m' \equiv 2 \pmod{4}$, risulterà $m \equiv 1 \pmod{2}$ ed ogni numero rappresentato da $mx + r$ sarà pure rappresentato da $\frac{m'}{2} x + r'$ ed avendo la prima numeri primi, ne avrà pure la seconda. Ma $m'x + r'$ ha gli stessi numeri primi di $\frac{m'}{2} x + r'$ e quindi anche nel secondo caso il teorema è provato.

6. Da quanto precede risulta anche:
Se una progressione aritmetica mx + r *ha i suoi numeri primi tutti contenuti in un'altra* m'x + r', *allora, anche ogni numero della prima è contenuto nella seconda; escluso il caso di* m ≡ 1 (mod. 2) *ed* m' ≡ 2 (mod. 4), *in cui ogni numero dispari della prima e nessun altro suo numero, è anche contenuto nella seconda* (1).

In questo caso si rilevi che, essendo m dispari, la progressione $mx + r$ rappresenta tanto numeri pari quanto numeri dispari; mentre la progressione $m'x + r'$, essendo m' pari, quindi r' dispari, rappresenta unicamente numeri dispari.

7. In modo esplicito si può notare che, mentre per una progressione aritmetica che abbia tutti i suoi numeri contenuti in

(1) Cfr. il n.° 4, ε) della mia Nota cit. della R. Acc. di Napoli.

un' altra, avviene che la ragione della prima è sempre un multiplo della seconda [1]; per una progressione aritmetica che abbia, invece, i suoi numeri primi tutti contenuti in un' altra, come si è ora veduto, oltre al caso che la ragione della prima sia ancora multipla della ragione della seconda, si presenta il caso che sia multipla della metà della seconda e non multipla di questa seconda ragione. Similmente può dirsi per la differenza dei termini iniziali, rispetto alla ragione della seconda progressione.

[1] Invero, se $mx + r$ è una progressione i cui numeri sono tutti contenuti in un' altra $m'x + r'$, supponendo come è lecito $r' = r$, esisterà un intero x tale che sia $m = m'x$.