Bollettino
Unione Matematica
Italiana

Ferenc Karteszi

Nuova dimostrazione di una congruenza aritmetica

Bollettino dell'Unione Matematica Italiana, Serie 1, Vol. **14** (1935), n.3, p. 173–174.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=BUMI_1935_1_14_3_173_0>

Bollettino dell'Unione Matematica Italiana, Unione Matematica Italiana, 1935.

Nuova dimostrazione di una congruenza aritmetica.

Nota di FERENC KÀRTESZI (a Györ - Ungheria) (1).

Sunto. - *Vien stabilita la* (1) *poggiando sul teorema di* FERMAT.

In una Nota pubblicata nel precedente fascicolo di questo « Bollettino » (2), ho incidentalmente ottenuto — per via geometrica — che:

Se $p_1, p_2, \ldots, p_r$ *denotano i divisori primi (diversi dall'unità) di un intero* $n \geq 2$, *e se* k *è un qualunque numero intero positivo, risulta*

$$N(k, n) \equiv 0 \pmod{n}, \tag{1}$$

ove, per abbreviare, si è posto:

$$N(k, n) = k^n - \sum_i k^{\frac{n}{p_i}} + \sum_{j,h} k^{\frac{n}{p_j p_h}} - \ldots + (-1)^r k^{\frac{n}{p_1 p_2 \cdots p_r}}, \tag{2}$$

le sommatorie essendo qui estese alle combinazioni degli indici 1, 2,..., r *ad* 1 *ad 1, a* 2 *a* 2 *ecc..*

Mi pare metta conto di mostrare come la (1) possa dedursi direttamente — ed in modo semplicissimo — dal teorema di FERMAT, ciò che appunto faccio nelle righe che seguono.

1. Osserviamo anzitutto che, se K, π, p denotano interi positivi arbitrari di cui l'ultimo sia primo, sussiste la congruenza:

$$K^{p^\pi} - K^{p^{\pi-1}} \equiv 0 \pmod{p^\pi}. \tag{3}$$

Nella (3) può intanto ovviamente supporsi $p \geq 2$. Se K, p^π sono primi fra loro, in base al teorema di FERMAT risulta:

$$K^{\varphi(p^\pi)} = K^{p^\pi - p^{\pi-1}} \equiv 1 \pmod{p^\pi},$$

donde segue subito la (3). Se — per contro — K non è primo con p^π, eppertanto è un multiplo di p, si ha palesemente:

$$K^{p^\pi} - K^{p^{\pi-1}} \equiv 0 \pmod{p^{p^{\pi-1}}};$$

(1) Tengo a ringraziare sentitamente il chiar.mo prof. BENIAMINO SEGRE che ha avuto la bontà di volgere in lingua italiana questo mio lavoro e quello più sotto citato, arrecando ad ambedue i lavori numerosi perfezionamenti.

(2) Cfr. F. KÀRTESZI, *Intorno a certi cicli di* n *punti su di un'ellisse*, questo « Bollettino », tomo XIV (1935), p. 83.

e da qui ancora si trae la (3), notando che — per $p \geq 2$ — è $p^{\pi-1} \geq \pi$.

2. La (2) mostra senz'altro che $N(k^{p^\pi}, m) - N(k^{p^{\pi-1}}, m)$ si può esprimere come una somma di differenze del tipo $\pm(K^{p^\pi} - K^{p^{\pi-1}})$: dunque, in virtù del n. 1, qualunque siano gl'interi positivi k, m, π ed il numero primo p, si può asserire che è:

$$N(k^{p^\pi}, m) - N(k^{p^{\pi-1}}, m) \equiv 0 \pmod{p^\pi}. \tag{4}$$

Supposto ora che n si decomponga in fattori primi nel modo seguente:

$$n = p_1^{\pi_1} p_2^{\pi_2} \dots p_r^{\pi_r},$$

sempre in forza della (2) si ha:

$$N(k, n) = N\left(k^{p_i^{\pi_i}}, \frac{n}{p_i^{\pi_i}}\right) - N\left(k^{p_i^{\pi_i - 1}}, \frac{n}{p_i^{\pi_i}}\right) \quad \text{per } i = 1, 2, \dots, r.$$

Da qui, avendo riguardo alla (4), si deduce:

$$N(k, n) \equiv 0 \pmod{p_i^{\pi_i}} \quad \text{per } i = 1, 2, \dots, r;$$

e queste r congruenze appunto provano la (1).