
BOLLETTINO UNIONE MATEMATICA ITALIANA

FRANCESCO SAVERIO ROSSI

Sul carattere di una particolare congruenza.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. 12
(1957), n.4, p. 694–697.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1957_3_12_4_694_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 carattere di una particolare congruenza.

Nota di FRANCESCO SAVERIO ROSSI (a Lanciano)

Sunto. - *Si stabiliscono alcune relazioni che generalizzano il teorema di WILSON per alcune classi di numeri primi.*

Summary. - *Some relations that generalize WILSON'S theorem about some classes of prime numbers are here determined.*

§ 1. Tra le proprietà dei numeri primi, così difficili e riposte, ve ne sono alcune veramente indicative per certe categorie di esse come quella che andiamo ad esporre.

È noto che, per p primo, vale il teorema di WILSON

$$(1) \quad (p-1)! \equiv -1 \pmod{p}$$

dal quale, poi, facilmente si trae la relazione

$$(2) \quad k!(p-k-1)! \equiv (-1)^{k+1} \pmod{p}.$$

È chiaro che, se vale la (2) o la (1), p risulta primo, in quanto sui numeri composti esistono relazioni diverse da esse.

La (2) permette di affrontare, nel tentativo di risolverla, una interessante questione, quella cioè di
« Risolvere l'equazione congruenziale

$$(3) \quad (p-x)! \equiv \lambda \pmod{p}$$

con

$$1 \leq \lambda < p, \quad x < p.$$

Intanto, per p primo, è valida la (1); e quindi, addizionando la (3) alla (1), si giunge alla relazione

$$(4) \quad (x-1)!\lambda + (-1)^{x-1} \equiv 0 \pmod{p}$$

dalla quale si trae la conclusione:

« Un'eventuale soluzione di (3) importa la condizione che p divida l'espressione a primo membro di (4). »

Se poi addirittura p è della forma $(x-1)!\lambda + (-1)^{x-1}$, il numero λ uguale a $\frac{p - (-1)^{x-1}}{(x-1)!}$.

Seguono subito alcune conseguenze:

« Se un numero primo è della forma $2\lambda + 1$ (tutti i numeri primi dispari lo sono), allora $x=3$ risolve la congruenza (3). Per cui

$$(5) \quad (p-3)! \equiv \lambda \pmod{p}.$$

Per $x=4$, la (4) dà per p il valore parametrico $6\lambda - 1$: onde per i numeri primi della forma $p = 6\lambda - 1$, viene ad essere risolta la congruenza

$$(6) \quad (p-4)! \equiv \lambda \pmod{p}.$$

Ma un numero primo della forma $6\lambda - 1$ lo è pure dell'altra $2(3\lambda - 1) + 1$; onde, insieme con la (6), viene verificata pure

$$(6') \quad (p-3)! \equiv 3\lambda - 1 \pmod{p}$$

(4) Estensioni della (2) sono riportate dal « Periodico di Matematiche », Fascic. di nov. 1930, Ser. IV, vol. X, n° 5 p. 335-Comunic. di A. GUARESCHI.

Per $x=5$, la (4) fornisce $24\lambda + 1 \equiv 0 \pmod{p}$.

Allora, per i numeri primi della forma $24\lambda + 1$ si ha:

$$(p-5)! \equiv \lambda; \quad (p-3)! \equiv 12\lambda \pmod{p}.$$

Per $x=6$, p risulta, o divisore o proprio della forma $120\lambda - 1$.

Se p è proprio di tale forma, allora

$$(p-6)! \equiv \lambda; \quad (p-3)! \equiv 60\lambda - 1 \pmod{p}.$$

A conclusione di quanto sopra, si può affermare, generalizzando, che per i numeri primi della forma $p = (h-1)! \lambda + (-1)^{h-1}$, sussiste la congruenza, $\pmod{p}$, $(p-h)! \equiv \lambda$ con l'altra

$$(7) \quad \begin{aligned} (p-3)! &\equiv \frac{1}{2}(h-1)! \lambda, \quad \text{se } p \text{ è dispari;} \\ (p-3)! &\equiv \frac{1}{2} h! \lambda - 1, \quad \text{se } h \text{ è pari.} \end{aligned}$$

Queste relazioni rappresentano, in un certo senso, una generalizzazione del teorema di WILSON sui numeri primi, per alcune classi di essi.

§ 2. Per i numeri composti occorre distinguere quelli che sono uguali a 4 o alla potenza o al doppio di una potenza di un numero primo dispari da quelli che non lo sono.

Sussiste la proposizione:

«Se il numero m è composto, $\neq 4$, p^x , $2p^x$, allora, essendo $a_1, a_2, \dots, a_{\varphi(m)}$ i numeri primi con m e minori di esso, il prodotto dei primi k fra gli a_i per i primi $\varphi(m) - k$ numeri stessi, è congruo $a/(-1)^k \pmod{m}$. Per convenzione $a_1 = 1$.

Si può proporre, per un assegnato numero composto di tale ultimo tipo, la risoluzione della congruenza

$$(8) \quad a_1 a_2 \dots a_{\varphi(m)-x} \equiv \lambda \pmod{m}.$$

Si deduce agevolmente di qua che, se sussiste la (8), deve m risultare divisore dell'espressione

$$(9) \quad (a_1 a_2 \dots a_x) \lambda + (-1)^x$$

Se poi il numero m è addirittura di questa forma, allora

(2) Cfr. M. CIPOLLA-Enciclopedia delle Matematiche Elementari a c. di L. BERZOLARI, G. VIVANTI e D. GIGLI Art. IV «Teoria dei Numeri» p. 278 Vol. I. P. I. Hoepli 1932-Milano.

1) per $x = 1$, essendo $m = \lambda - 1$, $a_1 a_2 \dots a_{\phi(m)-1} \equiv \lambda \pmod{m}$.

2) per $x = 2$, (e quindi $m = a_2 \lambda + 1$), $a_1 a_2 \dots a_{\phi(m)-2} \equiv \lambda \pmod{m}$.

Ora, se poniamo $a_2 = 2$, si deduce che tale ultima congruenza è sempre valida per i numeri composti dispari.

§ 3. Per i numeri naturali esclusi nel par. 2, valgono proprietà analoghe a quelle sui numeri primi, sulle quali non insistiamo ⁽³⁾.

OSSERVAZIONE. - Se il parametro λ è uguale a 1, nel caso della relazione (7), viene conseguita una notevole riduzione della congruenza di WILSON.

Es.:

$$p = 119, \quad (113)! \equiv 1 \quad \text{e} \quad (116)! \equiv 59 \pmod{119}.$$

⁽³⁾ « Per 2, 4, o la potenza o il doppio di una potenza di un numero primo dispari, vale il teorema di GAUSS; $a_1 a_2 \dots a_{\phi(m)} \equiv -1 \pmod{m}$, m essendo il numero naturale ed $a_1, a_2, a_3 \dots$ i numeri primi con m e minori di esso. Cfr. C. F. GAUSS « *Disquisitiones Arithmeticae* Lipsia 1801 Art. 70. Ved. F. S. ROSSI, *Sopra alcune congruenze notevoli*, Lanciano 1941. Tip. Mancini pag. 3.