
BOLLETTINO UNIONE MATEMATICA ITALIANA

EDOARDO STORCHI

Un teorema dedotto dal teorema di Wilson che caratterizza i numeri primi della forma $12h + 7$

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. 2
(1947), n.3, p. 229–231.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1947_3_2_3_229_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/>

**Un teorema dedotto dal teorema di Wilson
che caratterizza i numeri primi della forma $12h + 7$.**

Nota di EDOARDO STORCHI (a Milano).

Sunto - Se la congruenza più restrittiva deducibile del teorema di WILSON atta a caratterizzare i numeri primi di una data forma.

Sia p un numero primo della forma $12h + 7$; allora notoriamente

$$(1) \quad 1 \cdot 2 \cdot 3 \cdot 4 \dots \frac{p-5}{2} \cdot \frac{p-3}{2} \cdot \frac{p-1}{2} \equiv (-1)^\mu \pmod{p}$$

dove μ è il numero dei non resti quadratici di p minori di $\frac{p}{2}$ ⁽¹⁾.

D'altra parte gli stessi fattori costituenti il primo membro della (1) sono legati dalle seguenti congruenze:

$$(2) \quad \left\{ \begin{array}{l} 2 \cdot \frac{p-1}{2} \equiv -1 \equiv -1 \cdot 1 \\ 4 \cdot \frac{p-3}{2} \equiv -6 \equiv -2 \cdot 3 \\ 6 \cdot \frac{p-5}{2} \equiv -15 \equiv -3 \cdot 5 \quad (\text{mod. } p) \\ \dots \dots \dots \\ \frac{p-1}{3} \cdot \frac{p-\frac{p-4}{3}}{2} \equiv -\frac{p-1}{6} \cdot \frac{p-4}{3} \\ \quad \quad \quad \left(\text{cioè } \frac{p-1}{3} \cdot \frac{p+2}{3} \equiv -\frac{p-1}{6} \cdot \frac{p-4}{3} \right) \end{array} \right.$$

che, moltiplicate membro a membro, dànno:

$$(3) \quad 2 \cdot 4 \cdot 6 \cdot 8 \dots \frac{p-1}{3} \cdot \frac{p-1}{2} \cdot \frac{p-3}{2} \dots \frac{p+2}{3} \equiv (-1) \cdot \frac{p-1}{6} ! 1 \cdot 3 \cdot 5 \cdot 7 ! \dots \frac{p-4}{3} \pmod{p}.$$

Si osservi come il secondo membro della (3) sia numericamente inferiore del primo membro. Potremo allora vantaggiosa-

(1) DIRICHLET, 1828, 409-408, Werke p. 107. Vedasi, *Dickson History*, vol. I, pag. 275, L. BIANCHI, « Boll. U. M. I. », 1922, pagg. 41-43.

Desidero qui a proposito segnalare una mia dimostrazione estremamente semplice di questo teorema. Per il citato teorema di WILSON nel caso in

mente modificare la congruenza (1) sostituendovi al prodotto $2 \cdot 4 \cdot 6 \dots$
 $\dots \frac{p-1}{3} \cdot \frac{p-1}{2} \frac{p-3}{2} \dots \frac{p+2}{3}$ il prodotto $-\frac{p-1}{6}! \cdot 1 \cdot 3 \cdot 5 \cdot 7 \dots \frac{p-4}{3}$.

Si trova:

$$-3 \cdot 5 \cdot 7 \cdot 9 \dots \left(\frac{p-1}{3} - 1 \right) \frac{p-1}{6}! \cdot 1 \cdot 3 \cdot 5 \dots \frac{p-4}{3} \equiv (-1)^\mu \pmod{p}$$

cui p sia primo della forma $4k+3$ vale l'una o l'altra delle due congruenze:

$$a) \quad 1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \equiv 1 \pmod{p} \quad b) \quad 1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \equiv -1 \pmod{p}.$$

D'altra parte per il teorema di FERMAT:

$$\left[1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \right]^{p-1} \equiv 1 \pmod{p}$$

ossia:

$$\left[\left(1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \right)^{\frac{p-1}{2}} + 1 \right] \cdot \left[\left(1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \right)^{\frac{p-1}{2}} - 1 \right] \equiv 0 \pmod{p}$$

Sussiste dunque l'una o l'altra delle due congruenze:

$$c) \quad \left[1 \cdot 2 \cdot 3 \cdot 4 \dots \frac{p-1}{2} \right]^{\frac{p-1}{2}} \equiv 1, \quad d) \quad \left[1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \right]^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Precisamente sussiste la $a)$ quando sussiste la $c)$ e viceversa. Infatti dalla $a)$ elevando ambo i membri alla potenza d'esponente $\frac{p-1}{2}$ si ottiene la $c)$ e d'altra parte se sussiste la $c)$ non può valere la $b)$ perchè da questa elevando ambo i membri alla potenza d'esponente dispari $\frac{p-1}{2}$ si otterrebbe la $d)$ che è incompatibile con la $c)$ e allora sussiste necessariamente la $a)$. In modo identico si prova che se sussiste la $b)$ sussiste pure la $d)$ e viceversa. Ma $\left[1 \cdot 2 \cdot 3 \dots \frac{p-1}{2} \right]^{\frac{p-1}{2}} = 1^{\frac{p-1}{2}} \cdot 2^{\frac{p-1}{2}} \cdot 3^{\frac{p-1}{2}} \dots \frac{p-1}{2}^{\frac{p-1}{2}}$ e i numeri $1^{\frac{p-1}{2}}, 2^{\frac{p-1}{2}}, 3^{\frac{p-1}{2}} \dots \frac{p-1}{2}^{\frac{p-1}{2}}$ sono $\equiv \pm 1 \pmod{p}$ a seconda che i numeri $1, 2, 3, 4, \dots \frac{p-1}{2}$ siano resti quadratici o non resti quadratici di p ; segue

$$\left[1 \cdot 2 \cdot 3 \cdot 4 \dots \frac{p-1}{2} \right]^{\frac{p-1}{2}} \equiv (-1)^\mu \pmod{p}$$

dove μ è il numero dei non resti quadratici di p minori di $\frac{p}{2}$.

Per quanto si è detto si conclude allora:

$$1 \cdot 2 \cdot 3 \cdot 4 \dots \frac{p-1}{2} \equiv (-1)^\mu \pmod{p}$$

e questa relazione prova il teorema.

da cui:

$$\left[3 \cdot 5 \cdot 7 \cdot 9 \dots \frac{p-4}{3} \right]^2 \frac{p-1}{3} ! \equiv (-1)^{\mu-1} \pmod{p}$$

Vale dunque il

TEOREMA. « Condizione caratteristica affinchè il numero $p = 12h + 7$ sia primo è che il numero:

$$(4) \quad [3 \cdot 5 \cdot 7 \dots (4h + 1)]^2 (2h + 1)! - (-1)^{\mu+1}$$

sia divisibile per p ».

È questa la congruenza più restrittiva finora nota che valga a caratterizzare i numeri primi di una data forma e rappresenta la semplificazione numerica estrema della (1).

Così per stabilire secondo il corollario (1) del teorema di WILSON se il numero $19 = 12 \cdot 1 + 7$ è primo occorre verificare se il numero piuttosto rilevante $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \pm 1 = 362880 \pm 1$ è divisibile per 19. Secondo la (4) basta constatare se $[3 \cdot 5]^2 \cdot 3! - 1 = 1349$ è divisibile per 19. Analogamente per stabilire la primitività di 31 anzichè verificare se $15! \pm 1 = 1307674367000 \pm 1$ è divisibile per 31 basta controllare se $[3 \cdot 5 \cdot 7 \cdot 9]^2 \cdot 5! = 945^2 \cdot 120 + 1$ è divisibile per 31.

Con lievi modifiche il teorema può estendersi a tutti gli altri numeri primi della forma $4k + 3$ sfruttando lo stesso semplice procedimento dimostrativo.