Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

# Rendiconti

Franco Pellegrino

## Teorema di Wilson e numeri primi gemelli

*Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8*, Vol. **35** (1963), n.5, p. 258–262.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1963_8_35_5_258_0>

**Teoria dei numeri.** — *Teorema di Wilson e numeri primi gemelli.* Nota di FRANCO PELLEGRINO, presentata (*) dal Socio G. SANSONE.

1. Supposto (1) che $\bar{x} \in N_1$ soddisfi l'equazione

$$a^x \equiv 1 \pmod{m} \qquad (a \in N_1 ; m \in N_2) \tag{1}$$

risulta

$$\frac{a^{\bar{x}} - 1}{m} \in N_0 , \qquad \text{e quindi} \qquad \frac{a^{\bar{x}} - 1}{m} = \left[\frac{a^x}{m}\right] .$$

Ne segue che la (1) è equivalente alla

$$\frac{a^x}{m} - \left[\frac{a^x}{m}\right] = \frac{1}{m} \qquad (a \in N_1 ; m \in N_2) \tag{2}$$

epperò: Condizione necessaria e sufficiente perché $\bar{x}$ soddisfi alla (1) è che $a^{\bar{x}}/m$ differisca dalla sua parte intera per $1/m$.

È poi evidente che se la (1) è possibile dev'essere $(a , m) = 1$.

In particolare da quanto detto segue che è

$$\frac{a^{\varphi(m)}}{m} - \left[\frac{a^{\varphi(m)}}{m}\right] = \frac{1}{m} \qquad (a \in N_1 ; m \in N_2) \tag{3}$$

allora e allora soltanto che è $(a , m) = 1$. Nelle ipotesi $a \in N_1$, $m \in N_2$ vale dunque il teorema inverso di quello di Eulero, teorema di cui la (3) dà una forma diversa che conduce all'enunciato: *condizione necessaria e sufficiente perché* $m \in N_2$ *sia primo con* $a \in N_1$ *è che* $a^{\varphi(m)}/m$ *differisca dalla sua parte intera per* $1/m$. Possiamo anche dire che i numeri $m \in N_1$ primi con $a \in N_2$ sono tutti e soli gli zeri della funzione aritmetica $f_a$ definita ponendo

$$\begin{cases} f_a(m) = \dfrac{a^{\varphi(m)}}{m} - \left[\dfrac{a^{\varphi(m)}}{m}\right] - \dfrac{1}{m} & (\forall m \in N_2) \\ f_a(1) = 0 . \end{cases} \tag{4}$$

La condizione precedente è certo non soddisfatta se $a^{\varphi(m)}/m$ è intero. Ci si può quindi chiedere quali sono gli $m \in N_2$ tali che risulti $a^{\varphi(m)}/m \in N_1$. In proposito si trova facilmente che: Condizione necessaria e sufficiente perché prefissato $a \in N_1$ sia $a^{\varphi(m)}/m \in N_1$, con $m \in N_2$, è che

$$\delta = (a , m) \in N_2 \quad \text{e} \quad m | \delta^{\varphi(m)} . \tag{5}$$

Posto infatti $a = a' \delta$ , $m = m' \delta$ si ha

$$\frac{a^{\varphi(m)}}{m} = \frac{(a')^{\varphi(m)} \delta^{\varphi(m)}}{\delta m'} = (a')^{\varphi(m)} \frac{\delta^{\varphi(m)-1}}{m'}$$

(*) Nella seduta del 9 novembre 1963.

(1) Per i simboli qui adoperati si rimanda al lavoro: FRANCO PELLEGRINO: *Lineamenti di una teoria delle funzioni aritmetiche*, I, « Rend. Mat. », vol. XV, fasc. 3–4, Roma 1956.

e

$$((a')^{\varphi(m)}, m') = 1 .$$

2. Considerazioni analoghe a quelle che permettono di scrivere la (1) sotto la forma (2), e quindi il teorema di Eulero sotto la forma (3), ci dicono che la condizione di Wilson

$$(6) \qquad (n-1)! \equiv -1 \pmod{n} \qquad (n \in N_2)$$

è equivalente all'equazione

$$(7) \qquad \frac{(n-1)!}{n} - \left[\frac{(n-1)!}{n}\right] = \frac{n-1}{n} \qquad (n \in N_2) .$$

Può dirsi cioè che: *Condizione necessaria e sufficiente perché* $n \in N_2$ *sia primo è che n sia soluzione della* (7). Tale equazione, il cui insieme delle soluzioni in $N_2$ coincide con $\mathcal{S}$, potrà quindi essere chiamata « l'equazione dei numeri primi ». Potremo anche dire che $\mathcal{S}$ è l'insieme degli zeri della funzione aritmetica $f_{\mathcal{S}}$ definita ponendo

$$(8) \qquad \begin{cases} f_{\mathcal{S}}(n) = \dfrac{(n-1)!}{n} - \left[\dfrac{(n-1)!}{n}\right] - \dfrac{n-1}{n} & \forall\, n \in N_2 \\ f_{\mathcal{S}}(1) = 1 . \end{cases}$$

La (7) ci dice anche che: *Condizione necessaria e sufficiente perché* $n \in N_2$ *sia primo è che* $\dfrac{(n-1)!}{n}$ *differisca dalla sua parte intera per* $\dfrac{n-1}{n}$.

La condizione precedente è certo non soddisfatta se $\dfrac{(n-1)!}{n}$ è intero. È ciò che avviene notoriamente per ogni numero composto diverso da 4.

Per $n = 4$, il primo termine della (7) non è intero, ma $\dfrac{(4-1)!}{4}$ non differisce dalla sua parte intera per $\dfrac{4-1}{4}$ e tutto ciò spiega perché la nota condizione perché un numero sia composto ammette l'eccezione $n = 4$.

Dalla (7) segue anche che

$$(9) \qquad \lim_{\substack{n \to \infty \\ p_n \in \mathcal{S}}} \left\{ \frac{(p_n-1)!}{p_n} - \left[\frac{(p_n-1)!}{p_n}\right] \right\} = 1 .$$

3. È noto che si ha

$$(10) \qquad \left[\frac{n}{mq}\right] = \left[\frac{\left[\frac{n}{m}\right]}{q}\right] \qquad (n, m, q \in N_1) .$$

Posto allora

$$(11) \qquad \left[\frac{ab}{c}\right] = qa + r \qquad (a, b, c \in N_2 \; ; \; r \in N_0 - N_a)$$

si ha

$$q = \left[\frac{\left[\frac{ab}{c}\right]}{a}\right] = \left[\frac{b}{c}\right]$$

e quindi la (11) si scrive

$$\left[\frac{ab}{c}\right] = \left[\frac{b}{c}\right] a + r \qquad (a, b, c \in N_2 \; ; \; r \in N_0 - N_a). \tag{12}$$

In particolare, se

$$a \mid \left[\frac{ab}{c}\right] \tag{13}$$

risulta

$$\left[\frac{ab}{c}\right] = \left[\frac{b}{c}\right] a, \qquad (a, b, c \in N_2) \tag{14}$$

(ed è da osservare che se $ab/c$ non è intero, la (13) può verificarsi solo se $a < c$).

Così risulta, com'è facile convincersi,

$$\left[\frac{h a^{\varphi(m)}}{m}\right] = h \left[\frac{a^{\varphi(m)}}{m}\right] \qquad (a, m \in N_1 \; ; \; (a, m) = 1 \; ; \; h \in N_1 - N_m) \tag{15}$$

nonché

$$\left[\frac{(n-1)!}{n}\right] = (n-1) \left[\frac{(n-2)!}{n}\right], \qquad (4 \neq n \in N_2) \tag{16}$$

relazione quest'ultima evidente per $n$ composto diverso da 4. Per $n \in \mathcal{S}$ basta osservare che la (7) ci dice che il primo membro della (16) è divisibile per $n - 1$ ed applicare indi la (14).

4. Sia P un elemento di I tale che

$$P(n) = \begin{cases} 1 & \forall n \in \mathcal{S} \\ 0 & \forall n \in N_1 - \mathcal{S}. \end{cases} \tag{17}$$

Una tale funzione P è rilegata in modo semplice alla K avendosi, com'è facile convincersi,

$$\int P = K \; ; \tag{18}$$

$$\partial K = P. \tag{19}$$

Ora, da quanto precede si ottiene un'espressione analitica della P dato che la (7), quando si tenga conto della (16), assume la forma

$$\frac{(n-2)!}{n} - \left[\frac{(n-2)!}{n}\right] = \frac{1}{n} \tag{20}$$

epperò può porsi

$$\begin{cases} \mathcal{S}(n) = 0 & \text{per } n = 1, 4 \\ \mathcal{S}(n) = (n-2)! - n \left[\dfrac{(n-2)!}{n}\right] & \text{per ogni altro naturale.} \end{cases} \tag{21}$$

5. Dalla (7) segue che i naturali $p \in N_5$, $p - 2 \in N_3$ saranno entrambi primi se e solo se $p \in N_5$ è radice delle due equazioni

$$\frac{(p-1)!}{p} - \left[\frac{(p-1)!}{p}\right] = \frac{p-1}{p} \tag{22}$$

$$\frac{(p-3)!}{p-2} - \left[\frac{(p-3)!}{p-2}\right] = \frac{p-3}{p-2}. \tag{23}$$

Ricavando da ognuna di queste equazioni $\frac{(p-3)!}{p}$, e uguagliando le espressioni ottenute, se ne deduce che: se $p, p-2 \in \mathcal{S}$ ed è $p \geq 5$, il numero $p$ verifica necessariamente l'equazione

$$(24) \qquad \frac{1}{p(p-2)} + \frac{1}{(p-1)(p-2)}\left[\frac{(p-1)!}{p}\right] = \frac{p-3}{p} + \frac{p-2}{p}\left[\frac{(p-3)!}{p-1}\right].$$

Viceversa, come ora proveremo, si ha che: se $p \in N_5$ verifica la (24) risulta $p, p-2 \in \mathcal{S}$.

È subito visto in primo luogo che un naturale $p \geq 5$, non primo, non può soddisfare la (24). Da questa infatti, tenendo conto che nelle nostre ipotesi $\frac{(p-1)!}{n}$ è intero, si avrebbe l'assurdo

$$\frac{1}{p-2} = \left\{(p-2)\left[\frac{(p-3)!}{p-2}\right] + p - 3 - (p-3)!\right\} \in \pm N_0.$$

Se dunque $p \in N_5$ verifica la (24) dev'essere $p \in \mathcal{S}$. Supponiamo allora che il numero primo $p \in N_5$ verifichi la (24) e sia $p-2 \notin \mathcal{S}$. L'ipotesi $p \in \mathcal{S}$ porta allora, tenuta presente la (7), a sostituire nella (24) al posto di $\left[\frac{(p-1)!}{n}\right]$ l'espressione $\frac{(p-1)!}{p} - \frac{p-1}{p}$, e poiché è $p \in N_2$, epperò $p-2 \neq 4$, l'altra ipotesi $p-2 \notin \mathcal{S}$ implica che $\frac{(p-3)!}{p-2}$ è intero. Con facili calcoli si vede allora che la (24) darebbe l'assurdo

$$\frac{(p-3)!}{p} = \frac{(p-3)!}{p} + \frac{p-3}{p} \qquad (p \in N_5).$$

Rimane dunque così provato che: *Condizione necessaria e sufficiente perché i naturali* $p \in N_5$ *e* $p-2$ *siano entrambi primi è che* $p$ *verifichi la* (24).

6. Vogliamo ora dare alla (24) una forma più espressiva. Tenuto presente la (16), la (24) diventa intanto

$$1 + p\left[\frac{(p-2)!}{p}\right] = (p-2)^2\left[\frac{(p-3)!}{p-2}\right] + (p-2)(p-3)$$

ovvero

$$p\left\{\left[\frac{(p-2)!}{p}\right] + (4-p)\left[\frac{(p-3)!}{p-2}\right] - p + 5\right\} - 5 = 4\left[\frac{(p-3)!}{p-2}\right]$$

e quindi può dirsi che: se $p \in N_5$ verifica la (24), ovvero: se i naturali $p \in N_5$ e $p-2$ sono primi risulta

$$(25) \qquad 4\left[\frac{(p-3)!}{p-2}\right] \equiv -5 \pmod{p}.$$

Dimostreremo ora che se $p \in N_5$ verifica la (25) si ha $p, p-2 \in P$. Si prova direttamente in primo luogo che $p = 6$ non soddisfa la (25). Supponiamo ora che $p \in N_5$ verifichi la (25) e sia $p-2 \notin \mathcal{S}$, con il che è $p \in N_8$. Essendo $p-2 \neq 4$, il numero $\frac{(p-3)!}{p-2}$ è intero e quindi dalla (25) segue

$$4(p-3)! \equiv -5(p-2) \equiv 10 \pmod{p}$$

e quindi ancora

$$4\,(p-1)\,! \equiv 10\,(p-2)\,(p-1) \equiv 20 \pmod{p} \qquad (p \in N_2)$$

e cioè

$$\frac{4\,(p-1)\,! - 20}{p} \in N_1 . \tag{26}$$

Tale relazione è però nelle nostre ipotesi impossibile. Se infatti $p \in N_8$ non è primo, il numero $\frac{(p-1)\,!}{p}$ è intero, e quindi per la (26) si avrebbe che $p \mid 20$ epperò: o $p = 10$, o $p = 20$. Ma per $p = 10$ la (25) non è verificata, come si vede direttamente, e per $p = 20$ si arriva alla stessa conclusione osservando che il numero $2 \cdot \frac{17\,!}{9} + 5$ non può essere divisibile per 20 in quanto non è divisibile per 4. Si ha infatti

$$\frac{2.17\,!}{9} + 5 = 4\,(3 \times 4 \times \cdots \times 8 \times 10 \times \cdots \times 17 + 1) + 1.$$

Supposto poi che $p \in N_8$ sia primo, e quindi $p \in N_{11}$, per la (7) la (26) si scrive

$$4 \left\{ 1 + \left[ \frac{(p-1)\,!}{p} \right] \right\} - \frac{24}{p} \in N_1 \qquad (p \in N_{11})$$

relazione evidentemente assurda.

Se dunque $p \in N_5$ verifica la (25) dev'essere $p - 2 \in \mathcal{S}$ e in questa ipotesi dobbiamo ancora provare che dev'essere $p \in \mathcal{S}$. Per questo osserviamo che per la (7) la (25) si scrive ora

$$\frac{4\,(p-3)\,!}{p-2} - 4\,\frac{p-3}{p-2} \equiv -5 \pmod{p}$$

ovvero

$$4\,\{(p-3)\,! - (p-3)\} \equiv -5\,(p-2) \equiv 10 \pmod{p}$$

e quindi ancora

$$4\,(p-3)\,! \equiv -2 \pmod{p}$$

da cui

$$4\,(p-1)\,! \equiv -4 \pmod{p}$$

Essendo $(p\,,\,4) = 1$ (che se così non fosse sarebbe $p - 2 \notin \mathcal{S}$, per essere $p - 2$ pari, e maggiore di 2 per l'ipotesi $p \in N_5$), la precedente ci dà

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

e quindi

$$p \in \mathcal{S}.$$

Possiamo dunque concludere che: *condizione necessaria e sufficiente perché i naturali* $p \in N_5$ *e* $p - 2$ *siano entrambi primi è che* $p$ *verifichi la* (24) *o la* (25).