Riv. Mat. Univ. Parma (4) 11 (1985), 229-236

EDMONDO BEDOCCHI (*)

Nota ad una congettura sui numeri primi (**)

1 – In un interessante lavoro del 1950, [3], Giuseppe Giuga, dopo aver osservato che a causa del (piccolo) teorema di Fermat risulta

(a) se n è un numero primo, allora

$$1^{n-1} + 2^{n-1} + \ldots + (n-1)^{n-1} \equiv -1 \pmod{n}, \tag{1.1}$$

dimostra

(b) se n è un numero intero positivo minore di 10^{1000} che verifica (1.1), allora n è un numero primo.

Questo risultato ha indotto Giuga a formulare la seguente

Congettura. Un numero intero positivo n è primo se e solo se è verificata (1.1).

Tale congettura ha un notevole interesse, come rilevato per esempio in [4] ed in [10], perchè se fosse vera sarebbe una delle poche, assieme al teorema di Wilson, proprietà caratteristiche dei numeri primi, note a tuttora.

Per dimostrare l'affermazione (b) di cui sopra, Giuga si serve di varie proposizioni, riportate in **2** della presente nota, che conducono ad introdurre una certa successione di interi $(i_n)_{n\geq 1}$ detta *successione dei ranghi* (Def. 2.8). Egli mostra che tale successione ha termini maggiori di 360 e da ciò trae la prova di (b), come richiamerò in **2**.

Giuga dimostra inoltre ([3], pag. 528) che la sua congettura è un teorema quando si provi che la successione $(i_n)_{n\geq 1}$ non è superiormente limitata.

(*) Indirizzo: Dipartimento di Matematica, Università, Piazza di Porta S. Donato 5, 40127 Bologna, Italy.

(**) Ricevuto: 10-X-1983.

Questa nota è una prosecuzione dello studio di questi problemi ed in particolare contiene i due seguenti risultati:

(b)$_1$ Se n è un numero intero positivo minore di 10^{1700} che verifica (1.1), allora n è un numero primo.

(c) La successione $(i_n)_{n\geqslant 1}$ è superiormente limitata.

Il risultato (c) è abbastanza significativo poichè mostra che la congettura di Giuga non può essere dimostrata (se è vera) usando il suo metodo. Tale metodo però può dare ancora buoni frutti; infatti se si riuscirà a conoscere completamente la successione $(i_n)_{n\geqslant 1}$, è probabile, come ho osservato alla fine di questa nota, che il risultato (b)$_1$ possa essere rimpiazzato dal più forte

(b)$_2$ se n è un numero intero positivo minore di 10^{29315} che verifica (1.1), allora n è un numero primo,

risultato che dovrebbe essere abbastanza prossimo al migliore possibile.

2 – In questo paragrafo richiamo le definizioni ed i risultati più importanti di [3].

Def. 2.1 ([3], pag. 516). Un numero intero positivo composto n, si dirà che è *normale* se: (i) n è dispari, (ii) n è libero da quadrati, (iii) per ogni p, q primi tali che $p, q \mid n$ risulta $p \not\equiv 1 \pmod{q}$.

Proposizione 2.2 ([3], pag. 517). *Sia n un numero intero positivo composto per cui valga* (1.1), *risulta allora*: (i) *n è normale*, (ii) $\sum_{p\mid n} 1/p > 1$, *dove p varia nei numeri primi.*

Def. 2.3 ([3], pag. 519). Un insieme finito, non vuoto, di numeri primi si dice *normale* se si riduce ad un singoletto oppure se il prodotto di tutti i suoi elementi è un numero composto normale.

Notazione 2.4 ([3], pag. 519). Sia $p_1, p_2, p_3, \ldots$ la successione dei numeri primi dispari; con il simbolo (p_h), $h\geqslant 1$, si intende la sottosuccessione $p_h, p_{h+1}, p_{h+2}, \ldots$.

Notazione 2.5 ([3], pag. 520). Sia $h\geqslant 2$, $\{q_1, q_2, \ldots, q_r\} \subseteq \{p_1, p_2, \ldots, p_{h-1}\}$ e $q_1 < q_2 < \ldots < q_r$. Con il simbolo $(q_1, q_2, \ldots, q_r, p_h)$ si intende la sottosuccessione di $p_1, p_2, \ldots$ che ha come primi r termini $q_1, q_2, \ldots, q_r$ e poi di seguito tutti i termini di (p_h) eccezion fatta per quelli che sono congrui ad 1 modulo qualcuno dei q_i, $i = 1, 2, \ldots, r$.

Per esempio $(3, 5, p_6)$ è la successione 3, 5, 17, 23, 29, 47, 53, ...

Def. 2.6 ([3], pag. 520). Sia $h \geqslant 2$ ed S_h sia l'insieme dei sottoinsiemi normali di $\{p_1, p_2, \ldots, p_{h-1}\}$. L'insieme di successioni I_h è così definito

$$I_h = \{(p_h)\} \cup \{(q_1, q_2, \ldots, q_r, p_h) \,|\, \{q_1, q_2, \ldots, q_r\} \in S_h\} .$$

Per completezza si pone $I_1 = \{(p_1)\}$.

Def. 2.7 ([3], pag. 521). Sia $(a_n)_{n \geqslant 1}$ una successione di numeri interi positivi. Si dirà che essa ha *rango* se $\sum_{n=1}^{\infty} 1/a_n > 1$ e l'intero positivo v per cui $\sum_{n=1}^{v} 1/a_n \leqslant 1$ e $\sum_{n=1}^{v+1} 1/a_n > 1$, sarà il suo rango.

Def. 2.8 ([3], pag. 522). Per ogni $h \geqslant 1$, si dirà *rango di* I_h e si indicherà con i_h il minimo dei ranghi delle successioni di I_h.

Osservazione ([3], pag. 522). La successione $i_1, i_2, \ldots$ è non decrescente.

Proposizione 2.9 ([3], pag. 522). *Per ogni* $h \geqslant 1$ *e per ogni numero composto normale* n, *esiste una successione di* I_h *che contiene tutti i fattori primi di* n.

Proposizione 2.10 ([3], pag. 522). *Per ogni* $h \geqslant 1$ *se* n *è un numero intero positivo composto che soddisfa la condizione* (1.1), *allora* n *ha più di* i_h *fattori primi.*

Corollario 2.11 ([3], pag. 522). *Per ogni* $h \geqslant 1$ *se* $p_1, p_2, p_3, \ldots$ *è la successione dei numeri primi dispari e* $N = \prod_{j=1}^{i_h+1} p_j$, *allora ogni numero intero positivo composto* n *minore di* N *non soddisfa la condizione* (1.1).

3 – A questo punto Giuga va a studiare la successione $(i_n)_{n \geqslant 1}$ e con un calcolo diretto ottiene: $i_1 = 8$, $i_2 = 26$, $i_3 = 65$ (1), $i_4 = 113$, $i_5 = 126$, $i_6 = 201$, $i_9 > 360$.

Con questi dati e con il Corollario 2.11 egli deduce allora che se n è un numero intero positivo composto che soddisfa la condizione (1.1) deve essere

$$n \geqslant \prod_{j=1}^{i_9+1} p_j > \prod_{j=1}^{361} p_j > 10^{1000}.$$

(1) Come già osservato in [1], $i_3 = 64$; l'errore è dovuto alla approssimazione delle tavole degli inversi dei numeri primi utilizzate dall'autore.

Questo risultato può essere migliorato senza grande fatica (visto che attualmente si dispone di calcolatori molto potenti) proseguendo nella determinazione dei termini della successione $(i_n)_{n\geqslant 1}$. Ho calcolato il valore esatto di i_9 (e per curiosità anche quelli di i_7 ed i_8) ottenendo $i_7 = 277$, $i_8 = 322$, $i_9 = 553$, da cui si ricava che se n è un numero intero positivo composto che soddisfa la condizione (1.1), allora

$$n \geqslant \prod_{j=1}^{i_9+1} p_j = \prod_{j=1}^{554} p_j > 10^{1700}.$$

4 – Si potrebbe continuare a calcolare valori di i_n (penso che i_{15} o i_{16} non dovrebbero richiedere tempi di calcolo eccessivi) ed ottenere limitazioni inferiori per n molto maggiori di 10^{1700}, ma credo che adesso occorra affrontare il problema dell'andamento all'infinito della successione $(i_n)_{n\geqslant 1}$.

Infatti se $\lim_{n\to\infty} i_n = +\infty$, per il Corollario 2.11, non esisterebbero numeri interi positivi composti n soddisfacenti (1.1) e quindi la congettura di Giuga sarebbe dimostrata.

Come si vedrà tra breve questa favorevole evenienza non ha luogo in quanto la successione $(i_n)_{n\geqslant 1}$ risulterà essere limitata (e perciò costante da un certo punto in poi).

Sia $\{q_1, q_2, \ldots, q_r\}$, $q_1 < q_2 < \ldots < q_r$, un insieme normale di numeri primi e $(c_n(q_1, q_2, \ldots, q_r))_{n\geqslant 1}$ sia la successione così definita

$$\text{(4.1)}\qquad \begin{aligned} &c_n(q_1, q_2, \ldots, q_r) = q_n \quad \text{se } n = 1, 2, \ldots, r \\ &c_n(q_1, q_2, \ldots, q_r) = \min\{p \mid p \text{ primo e } p > c_{n-1}(q_1, q_2, \ldots, q_r) \text{ e } p \not\equiv 1 \\ &\pmod{c_i(q_1, q_2, \ldots, q_r)} \text{ per } i = 1, 2, \ldots, n-1\} \quad \text{se } n > r. \end{aligned}$$

È evidente che per ogni intero positivo t, l'insieme $\{c_1(q_1, q_2, \ldots, q_r), c_2(q_1, q_2, \ldots, q_r), \ldots, c_t(q_1, q_2, \ldots, q_r)\}$ risulta essere normale.

Per semplicità, d'ora in poi, quando il discorso prescinderà dalla natura dei numeri primi $q_1, q_2, \ldots, q_r$, una successione definita secondo (4.1) verrà indicata brevemente con $(c_n)_{n\geqslant 1}$.

Ora per giungere alla prova della limitatezza di $(i_n)_{n\geqslant 1}$ basterà trovare, se è possibile, una successione $(c_n)_{n\geqslant 1}$ che abbia rango.

Prima di far partire il calcolatore alla ricerca di una tale successione è opportuno farsi un'idea, anche approssimativa, della probabilità che la ricerca abbia successo e della direzione nella quale dirigerlo.

Sia $(c_n)_{n\geqslant 1}$ una successione definita secondo (4.1), m sia un intero positivo e $\{c_1, c_2, \ldots, c_k\}$ sia l'insieme dei c_n non maggiori di m. Voglio valutare il nu-

mero dei c_n per cui $m < c_n \leqslant 2m$; seguendo la terminologia di [**6**], sia $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ la famiglia di proprietà così definita: $\alpha_i = \text{« } x \equiv 1 \pmod{c_i}\text{ »}$ per $i = 1, 2, \ldots, k$ ed $S = \{p \mid p \text{ primo } e \ m < p \leqslant 2m\}$.

Si vede facilmente che il numero cercato è esattamente $N_{1,2,\ldots,k}$ che si calcola ([**6**], pag. 2) con la formula

$$N_{1,2,\ldots,k} = \sum_{(j_1, j_2, \ldots, j_s)} (-1)^s N(j_1, j_2, \ldots, j_s) ,$$

dove $(j_1, j_2, \ldots, j_s)$ varia nell'insieme dei sottoinsiemi di $\{1, 2, \ldots, k\}$ ed $N(j_1, j_2, \ldots, j_s)$ è il numero degli elementi di S per cui sono vere $\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_s}$ contemporaneamente.

Ora, essendo $c_{j_1}, c_{j_2}, \ldots, c_{j_s}$ numeri primi distinti, risulta

$$N(j_1, j_2, \ldots, j_s) = \pi(2m, c_{j_1} \cdot c_{j_2} \cdot \ldots \cdot c_{j_s}, 1) - \pi(m, c_{j_1} \cdot c_{j_2} \cdot \ldots \cdot c_{j_s}, 1) ,$$

dove $\pi(x, b, a)$ è il numero dei numeri primi p tali che $p \leqslant x$ e $p \equiv a \pmod{b}$. Ricordato che se $(a, b) = 1$, allora $\pi(x, b, a) = (1/\varphi(b)) \cdot \pi(x) + o(\pi(x))$ ([**8**], pag. 139) si ha

$$N(j_1, j_2, \ldots, j_s) = \frac{1}{\varphi(c_{j_1} \cdot c_{j_2} \cdot \ldots \cdot c_{j_s})} \cdot (\pi(2m) - \pi(m)) + E(m) ,$$

dove $E(m) = o(\pi(2m) - \pi(m))$. Tenuto conto di $\varphi(c_{j_1} \cdot c_{j_2} \cdot \ldots \cdot c_{j_s}) = (c_{j_1} - 1) \cdot (c_{j_2} - 1) \ldots (c_{j_s} - 1)$ e sostituendo nella formula di $N_{1,2,\ldots,k}$ si ottiene

$$\begin{aligned} & N_{1,2,\ldots,k} \\ &= (\pi(2m) - \pi(m)) \cdot \sum_{(j_1, j_2, \ldots, j_s)} (-1)^s \frac{1}{(c_{j_1} - 1)(c_{j_2} - 1) \ldots (c_{j_s} - 1)} + E_1(m) \\ &= (\pi(2m) - \pi(m)) \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{c_i - 1}\right) + E_1(m) \\ &= (\pi(2m) - \pi(m)) \cdot \prod_{i=1}^{k} \frac{c_i - 2}{c_i - 1} + E_1(m) , \end{aligned}$$

dove $E_1(m) = o(\pi(2m) - \pi(m))$ se si tiene fisso k.

Per poter proseguire occorre una valutazione del prodotto $\prod_{i=1}^{k} (c_i - 2)/(c_i - 1)$; utilizzando il teorema di Mertens ([**5**], pag. 351) si ottiene

$$\prod_{\substack{3 \leqslant p \leqslant x \\ p \text{ primo}}} \frac{p - 2}{p - 1} \sim \frac{2C_2}{\exp(\gamma) \log x} , \tag{4.2}$$

dove C_2 è la costante dei numeri primi gemelli ([5], pag. 371) e γ è la costante di Eulero.

Ora per ogni $(c_n)_{n\geqslant 1}$ definisco i numeri P_j, Q_j, R_j, $j = 0, 1, \ldots$, come segue

$$P_0 = \#\{c_n \mid 3 \leqslant c_n \leqslant 2500\}\,, \qquad P_j = \#\{c_n \mid 2^{j-1}\cdot 2500 < c_n \leqslant 2^j \cdot 2500\} \quad \text{se } j \geqslant 1$$

$$Q_j = \prod_{3 \leqslant c_n \leqslant 2^j \cdot 2500} \frac{c_n - 2}{c_n - 1}\,,$$

$$R_0 = \frac{P_0}{\pi(2500)}\,, \qquad R_j = \frac{P_j}{\pi(2^j \cdot 2500) - \pi(2^{j-1}\cdot 2500)} \qquad \text{se } j \geqslant 1\,.$$

Tenuto conto del valore di $N_{1,2,\ldots,k}$ e di (4.2), trascurando i relativi termini errore, si hanno le seguenti valutazioni approssimative di P_{j+1}, Q_{j+1} e R_{j+1} a partire da P_j, Q_j e R_j:

$$\begin{aligned} P_{j+1} &= \Big[(\pi(2^{j+1}\cdot 2500) - \pi(2^j \cdot 2500)) \cdot \prod_{3 \leqslant c_n \leqslant 2^j \cdot 2500} \frac{c_n - 2}{c_n - 1}\Big] \\ &= \big[(\pi(2^{j+1}\cdot 2500) - \pi(2^j \cdot 2500))Q_j\big], \\ R_{j+1} &= \frac{P_{j+1}}{\pi(2^{j+1}\cdot 2500) - \pi(2^j \cdot 2500)} \\ Q_{j+1} &= Q_j \cdot \prod_{2^j \cdot 2500 < c_n \leqslant 2^{j+1}\cdot 2500} \frac{c_n - 2}{c_n - 1} \\ &= Q_j \cdot \Big(\frac{\log 2^j \cdot 2500}{\log 2^{j+1}\cdot 2500}\Big)^{R_{j+1}}, \end{aligned}$$

dove quest'ultima uguaglianza è ottenuta con la ulteriore supposizione che i c_n compresi tra $2^j \cdot 2500$ e $2^{j+1}\cdot 2500$ si distribuiscano uniformemente sulla successione dei numeri primi e $[\cdot]$ è la funzione parte intera.

Supponiamo che una data $(c_n)_{n\geqslant 1}$ goda delle seguenti proprietà

$$P_0 = 125\,, \qquad Q_0 = 0.350\,000\,. \tag{4.3}$$

Con le formule appena ottenute determino i successivi valori di P_j, Q_j ed R_j per $j = 1, 2, \ldots, 7$.

I risultati ottenuti sono riportati nella seguente tabella

j	P_j	Q_j	$\pi(2^j \cdot 2500)$	R_j
0	125	0.350 000	367	0.340 599
1	105	0.339 821	669	0.347 682
2	190	0.330 919	1 229	0.339 286
3	341	0.323 087	2 262	0.330 106
4	627	0.316 103	4 203	0.323 029
5	1 148	0.309 839	7 837	0.315 905
6	2 121	0.304 172	14683	0.309 816
7	3 931	0.299 014	27608	0.304 139

Ricordato che $\sum_{p\leqslant x} 1/p \sim \log\log x$ ([5], pag. 351) e supponendo al solito che i c_n maggiori di 2500 si distribuiscano uniformemente sulla successione dei numeri primi, si può affermare che una approssimazione di $\sum_{2500<c_n\leqslant 320000} 1/c_n$ è data da

$$\sum_{j=1}^{7} R_j \log\frac{\log 2^j\cdot 2500}{\log 2^{j-1}\cdot 2500} = \sum_{j=1}^{7} \log\frac{Q_{j-1}}{Q_j} = \log\frac{Q_0}{Q_7} = 0.157443\,.$$

Ora, se oltre alle (4.3) la successione $(c_n)_{n\geqslant 1}$ soddisfa anche

$$\sum_{3\leqslant c_n\leqslant 2500} 1/c_n \geqslant 0.842\,557\,, \tag{4.4}$$

essa avrà rango e nel caso che in (4.4) valga l'uguaglianza tale rango varrà approssimativamente $P_0 + P_1 + \ldots + P_7 = 8588$.

È chiaro che quella appena terminata non è la dimostrazione dell'esistenza di una successione di tipo (4.1) dotata di rango; è semplicemente una stima orientativa per la ricerca che intendo fare con il calcolatore.

Guidato dalle indicazioni ottenute ho preso in esame la successione $(c_n(5))_{n\geqslant 1}$ che ha caratteristiche abbastanza vicine a (4.3) e (4.4); infatti risulta

$$P_0 = 129\,, \quad Q_0 = 0.366\,118\,, \quad \sum_{3\leqslant c_n(5)\leqslant 2500} 1/c_n(5) = 0.850\,677\,.$$

Utilizzando il calcolatore CDC 7600 del CINECA ho trovato che essa ha rango e che questi vale 8134 (e che, a conforto dell'analisi precedentemente condotta, $c_{8135}(5) = 321\,053$).

Questo fatto assieme alla Proposizione 2.9 assicura che la successione $(i_n)_{n\geqslant 1}$, dei ranghi degli insiemi I_n, è costante da un certo n_0 in poi ed inoltre risulta $i_{n_0}\leqslant 8134$.

5 – Come conclusione vorrei aggiungere una considerazione su questo i_{n_0}; da valutazioni approssimate e da esperimenti fatti sulle successioni $(c_n)_{n\geqslant 1}$ ho tratto la convinzione che i_{n_0} non sia minore di 7000. Se ciò, come penso, risponde a verità, il Corollario 2.11 può essere riformulato in questi termini:

Corollario 2.11. *Se $p_1, p_2, p_3, \ldots$ è la successione dei numeri primi dispari e $N = \prod_{j=1}^{7001} p_j$, allora ogni numero intero positivo composto n minore di N non soddisfa la condizione* (1.1).

Tenuto conto di $\sum_{p \leqslant x} \log p = \vartheta(x)$ e $\vartheta(x) > x(1 - 1/(2 \log x))$ se $x \geqslant 563$ ([9], pag. 70), risulta

$$\log N = \sum_{j=1}^{7001} \log p_j = \left(\sum_{p \leqslant 70667} \log p \right) - \log 2 > 67\,501 ,$$

da cui $N > 10^{29315}$, che è un numero veramente ragguardevole.

Bibliografia

[1] A. CHICCA, *Proprietà caratteristiche dei numeri primi*, Tesi di Laurea, Università di Bologna, (Relatore Prof. L. Muracchini, A.A. 1973-74.)

[2] A. CUNNINGHAM, *Quadratic partitions*, Francis Hodgson, London 1904.

[3] G. GIUGA, *Su una presumibile proprietà caratteristica dei numeri primi*, Ist. Lombardo Sci. Lett. Rend. A **83** (1950), 511-528.

[4] R. H. GUY, *Unsolved problems in number theory*, Springer, Berlin 1981.

[5] G. H. HARDY and E. M. WRIGHT, *An introduction to the theory of numbers*, V Edizione, Oxford University Press, Oxford 1979.

[6] C. HOOLEY, *Applications of sieve methods to the theory of numbers*, Cambridge University Press, Cambridge 1976.

[7] L. POLETTI, *Tavole dei numeri primi*, Hoepli, Milano 1920.

[8] K. PRACHAR, *Primzahlverteilung*, Reprint, Springer, Berlin 1978.

[9] B. J. ROSSER and L. SCHOENFELD, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64-94.

[10] W. SIERPIŃSKI, *Elementary theory of numbers*, Państwowe Widawnictwo Naukowe, Warszawa 1964.

Summary

The paper is concerned with the method employed by G. Giuga in order to prove that the positive integers $n < 10^{1000}$, *satisfying* (1.1) *above, are prime numbers. We prove that this method cannot lead to Giuga's conjecture* (i.e. *every integer satisfying* (1.1) *is a prime number*). *Furthermore we prove that Giuga's bound*, i.e. $n < 10^{1000}$, *can be improved to* $n < 10^{1700}$.

* * *