PERCHÉ IL PROBLEMA DI GOLDBACH È DIFFICILE?

Alessandro Zaccagnini

Parma, 11 maggio 2000

In questa conferenza intendo spiegare perché la congettura di Goldbach è difficile, tanto da non essere stata ancora dimostrata, nonostante la sua apparente semplicità. Nella mia precedente conferenza dal titolo "Variazioni Goldbach: problemi con numeri primi" [19], ho cercato di spiegare perché questa congettura è naturale ed interessante, utilizzando un'argomentazione essenzialmente elementare che permette di dare una formulazione "quantitativa" alla congettura stessa, fornita dalla formula (6): ora ci occupiamo degli aspetti piú tecnici della questione e per questo motivo abbandoniamo l'esposizione divulgativa per entrare nel dettaglio delle idee matematiche.

§1. Problemi additivi: il metodo del cerchio

Nel corso degli ultimi secoli si sono presentati all'attenzione dei matematici molti problemi di natura additiva, come per esempio il problema di Waring (vedi Hardy & Wright [10], Capp. 20–21 per un'introduzione, e Vaughan [15] per uno studio piú approfondito) ed il problema di Goldbach. Posto in generale, il tipico problema additivo può essere visto cosí: sono dati s sottoinsiemi di $\mathbb{N}$, $\mathfrak{A}_1, \dots, \mathfrak{A}_s$, non necessariamente distinti, dove $s \in \mathbb{N}$ è almeno 2. Il problema consiste nel determinare il numero di soluzioni dell'equazione

$$n = a_1 + a_2 + \cdots + a_s \tag{1.1}$$

dove $n \in \mathbb{N}$ è dato, e $a_j \in \mathfrak{A}_j$ per $j = 1, \dots, s$, o per lo meno, dimostrare che per n sufficientemente grande questa equazione ha almeno una soluzione. Nel problema di Waring si prendono tutti gli insiemi $\mathfrak{A}_j$ uguali alle k-esime potenze e si cerca di determinare il minimo s per cui l'equazione (1.1) ha soluzione per ogni $n \in \mathbb{N}$, oppure il minimo s per cui l'equazione (1.1) ha soluzione per ogni $n \in \mathbb{N}$ sufficientemente grande. Nel problema binario di Goldbach si prendono $\mathfrak{A}_1 = \mathfrak{A}_2 = \mathfrak{P}$, l'insieme di tutti i numeri primi. Si osservi che in questo caso (ed in altri analoghi) ci sono motivi aritmetici che impongono delle restrizioni agli n per cui ci si chiede se la (1.1) abbia una soluzione.

Il metodo per affrontare i problemi additivi che esporrò qui ha la sua origine in un articolo del 1918 di Hardy & Ramanujan [9] sulle partizioni, ma dato il numero di problemi affrontati e risolti in questo modo da Hardy & Littlewood negli anni '20 (si vedano fra gli altri [7] e [8]) ormai ha preso il loro nome o quello di "metodo del cerchio." L'obiettivo di questa conferenza è una descrizione delle idee di Hardy, Littlewood & Ramanujan, con una certa dose di dettagli. Per semplicità, parleremo del caso in cui $s = 2$ ed $\mathfrak{A}_1 = \mathfrak{A}_2 = \mathfrak{A}$. Si parte ponendo

$$f(z) = f_{\mathfrak{A}}(z) := \sum_{n=0}^{\infty} a(n) z^n, \qquad \text{dove} \qquad a(n) = \begin{cases} 1 & \text{se } n \in \mathfrak{A}, \\ 0 & \text{altrimenti.} \end{cases}$$

Se $\mathfrak{A}$ è infinito (in caso contrario il problema non ha interesse) allora f è una serie di potenze con raggio di convergenza uguale ad 1. Ci interessa il numero delle "rappresentazioni" di n nella forma $a_1 + a_2$ con $a_j \in \mathfrak{A}$, $j = 1, 2$. Poniamo quindi

$$r_2(n) := \big|\{(a_1, a_2) \in \mathfrak{A} \times \mathfrak{A} : n = a_1 + a_2\}\big|,$$

Per le note proprietà delle serie di potenze (prodotto di Cauchy), per $|z| < 1$ si ha

$$f^2(z) = \sum_{n=0}^{\infty} c(n) z^n \qquad \text{dove} \qquad c(n) = \sum_{\substack{0 \le h,k \le n \\ h+k=n}} \sum a(h)a(k)$$

ed $a(h)a(k) \neq 0$ se e solo se h, $k \in \mathfrak{A}$; dunque $c(n) = r_2(n)$. Allo stesso modo si dimostra che $f^s(z) = \sum_{n=0}^{\infty} r_s(n) z^n$ dove $r_s(n) := \big|\{(a_1, \dots, a_s) \in \mathfrak{A}^s : n = a_1 + \cdots + a_s\}\big|$. Per il teorema di Cauchy, per $\varrho < 1$ si ha quindi

$$r_2(n) = \frac{1}{2\pi \mathrm{i}} \int_{\gamma(\varrho)} \frac{f^2(z)}{z^{n+1}} \, \mathrm{d}z, \tag{1.2}$$

dove $\gamma(\varrho)$ è la circonferenza di centro l'origine e raggio ϱ. Per certi insiemi $\mathfrak{A}$ è possibile determinare uno sviluppo asintotico per f in un intorno delle singolarità presenti sulla circonferenza $\gamma(1)$ e quindi si può stimare l'integrale nella (1.2) prendendo ϱ una funzione di n che ha limite 1. Per maggiori dettagli si veda Vaughan [15], Cap. 1.

Possiamo usare questo metodo per "risolvere" un problema piuttosto semplice: dato $k \in \mathbb{N}^*$, determinare in quanti modi è possibile scrivere $n \in \mathbb{N}$ come somma di esattamente k numeri naturali. In altre parole, vogliamo determinare $r_k(n) := \big|\{(a_1, \dots, a_k) \in \mathbb{N}^k : n = a_1 + \cdots + a_k\}\big|$. Naturalmente è possibile dimostrare direttamente che $r_k(n) = \binom{n+k-1}{k-1}$, ma qui ci interessa il funzionamento del metodo del cerchio. Evidentemente si ha $f(z) = \sum_{n=0}^{\infty} z^n = (1-z)^{-1}$. Quindi, per $\varrho < 1$,

$$r_k(n) = \frac{1}{2\pi \mathrm{i}} \int_{\gamma(\varrho)} \frac{\mathrm{d}z}{(1-z)^k z^{n+1}}. \tag{1.3}$$

Si osservi che la funzione integranda ha una sola singolarità sulla circonferenza $\gamma(1)$, e di un tipo piuttosto semplice. In questo caso particolare è possibile calcolare esattamente il valore dell'integrale a destra nella (1.3): infatti, poiché $\varrho < 1$ vale lo sviluppo

$$\frac{1}{(1-z)^k} = 1 + \binom{-k}{1}(-z) + \binom{-k}{2}(-z)^2 + \cdots = \sum_{m=0}^{\infty} \binom{-k}{m}(-z)^m.$$

La serie a destra converge totalmente in tutti i compatti contenuti in $\{z \in \mathbb{C} : |z| < 1\}$ e dunque possiamo sostituire nella (1.3) e scambiare l'integrale con la serie:

$$\begin{aligned} r_k(n) &= \frac{1}{2\pi \mathrm{i}} \sum_{m=0}^{\infty} \binom{-k}{m}(-1)^m \int_{\gamma(\varrho)} z^{m-n-1} \, \mathrm{d}z \\ &= \frac{1}{2\pi \mathrm{i}} \sum_{m=0}^{\infty} (-1)^m \binom{-k}{m} \begin{cases} 2\pi \mathrm{i} & \text{se } m = n, \\ 0 & \text{altrimenti,} \end{cases} = (-1)^n \binom{-k}{n}, \end{aligned}$$

e non è difficile vedere che $(-1)^n\binom{-k}{n} = \binom{n+k-1}{k-1}$. Si osservi infine che la funzione integranda è relativamente piccola su tutta la circonferenza $\gamma(\varrho)$ a parte un piccolo arco vicino al punto $z = \varrho$, il quale dà il contributo principale all'integrale nella (1.3).

In generale non sarà possibile valutare direttamente ed esattamente l'integrale, ed inoltre la funzione integranda avrà piú di una singolarità sulla circonferenza $\gamma(1)$. Per esempio, se si vuole determinare in quanti modi è possibile scrivere $n \in \mathbb{N}$ come somma di esattamente k interi dispari la funzione f dell'esempio di sopra deve essere sostituita da $g(z) = \sum_{m=0}^{\infty} z^{2m+1} = \dfrac{z}{1-z^2}$, che ha singolarità in $z = \pm 1$. In questi casi, come vedremo, si dovrà cercare uno sviluppo asintotico per la funzione integranda valido in prossimità di ciascuna singolarità.

Questo procedimento è stato utilizzato da Hardy & Littlewood negli anni '20 ([7] e [8]) per dimostrare molti risultati relativi al problema di Waring e per portare il primo vero attacco al problema di Goldbach. Negli anni '30 Vinogradov introdusse alcune semplificazioni che rendono la sua versione del metodo del cerchio piú semplice da esporre. L'idea di base di Hardy & Littlewood è quella di avere una funzione fissata, $f(z)^k$ nell'esempio precedente, e prendere ϱ come funzione di n che ha limite 1; inoltre si devono cercare opportuni sviluppi asintotici nei pressi delle singolarità che la funzione integranda presenta sulla circonferenza $\gamma(1)$. Vinogradov osserva che alla quantità $r_2(n)$ possono contribuire solo gli interi $m \le n$: dunque si può introdurre la funzione

$$f_N(z) := \sum_{m=0}^{N} z^m = \frac{1-z^{N+1}}{1-z} \tag{1.4}$$

(l'ultima uguaglianza è valida per $z \neq 1$). Per $n \le N$, il Teorema di Cauchy dà

$$r_k(n) = \frac{1}{2\pi\mathrm{i}} \int_{\gamma(1)} \frac{f_N^k(z)}{z^{n+1}}\,\mathrm{d}z. \tag{1.5}$$

In questo caso non ci sono singolarità della funzione integranda (si ricordi che f_N è una somma *finita*, e quindi non ci sono problemi di convergenza): per questo motivo possiamo fissare una volta per tutte la circonferenza su cui si integra. Poniamo $e(x) := e^{2\pi\mathrm{i}x}$ e facciamo il cambiamento di variabile $z = e(\alpha)$ nella (1.5):

$$r_k(n) = \int_0^1 f_N^k\big(e(\alpha)\big)\, e(-n\alpha)\,\mathrm{d}\alpha. \tag{1.6}$$

Questa è anche la formula che dà l'n-simo coefficiente di Fourier della funzione $f_N^k\big(e(\alpha)\big)$, per l'ortogonalità della funzione esponenziale complessa. Per futura comodità poniamo $T_N(\alpha) = T(\alpha) := f_N\big(e(\alpha)\big)$; per la (1.4) si ha quindi

$$T(\alpha) := \sum_{m=0}^{N} e(m\alpha) = \begin{cases} \dfrac{1-e\big((N+1)\alpha\big)}{1-e(\alpha)} = e\big(\tfrac{1}{2}N\alpha\big)\dfrac{\sin(\pi(N+1)\alpha)}{\sin(\pi\alpha)} & \text{se } \alpha \notin \mathbb{Z}; \\ N+1 & \text{se } \alpha \in \mathbb{Z}. \end{cases} \tag{1.7}$$

Si veda la Figura 2 per il grafico di $|T_{20}(\alpha)|$. La proprietà che ci serve per concludere la nostra analisi "elementare" riguarda la rapidità con cui la funzione T decade quando α si allontana dai valori interi: posto $\|\alpha\|$ la distanza di α dall'intero piú vicino, dalla (1.7) si ricava facilmente che

$$|T_N(\alpha)| \le \min\left(N+1, \frac{1}{|\sin(\pi\alpha)|}\right) \le \min\big(N+1, \|\alpha\|^{-1}\big) \tag{1.8}$$

poiché T è periodica di periodo 1 ed inoltre $\alpha \le \sin(\pi\alpha)$ per $\alpha \in \big(0, \frac12\big]$. Usando questa disuguaglianza, non è difficile vedere che se $\delta = \delta(N)$ non è troppo piccolo, l'intervallo $[\delta, 1-\delta]$ non dà un contributo apprezzabile all'integrale nella (1.6): infatti, se $\delta \ge \frac{1}{N}$ e $k \ge 2$ abbiamo

$$\left| \int_\delta^{1-\delta} T_N^k(\alpha) e(-n\alpha)\,\mathrm{d}\alpha \right| \le \int_\delta^{1-\delta} |T_N^k(\alpha)|\,\mathrm{d}\alpha \le \int_\delta^{1-\delta} \frac{\mathrm{d}\alpha}{\|\alpha\|^k} \le \frac{2}{k-1}\delta^{1-k} \tag{1.9}$$

e questo è $o\big(N^{k-1}\big)$ non appena $\delta^{-1} = o(N)$. In altre parole, è sufficiente che δ sia appena piú grande di N^{-1} affinché il contributo dell'intervallo $[\delta, 1-\delta]$ all'integrale nella (1.6) sia piú piccolo del termine principale che, ricordiamo, è dell'ordine di $N^{k-1}(k-1)!^{-1}$. In altre parole ancora, il termine principale è concentrato attorno ad $\alpha = 0$. Può essere interessante notare che, almeno nel caso $k = 2$, è possibile spingere la nostra analisi ancora piú avanti: prendendo $n = N$ e $\delta^{-1} = o(N)$, per le (1.6) ed (1.9) si ha

$$r_2(N) = \int_0^1 \left(\frac{\sin\big(\pi(N+1)\alpha\big)}{\sin(\pi\alpha)} \right)^2 \mathrm{d}\alpha = 2\int_0^\delta \left(\frac{\sin\big(\pi(N+1)\alpha\big)}{\sin(\pi\alpha)} \right)^2 \mathrm{d}\alpha + o(N), \tag{1.10}$$

perché la funzione integranda è periodica di periodo 1 (se ne veda la definizione). Suddividiamo l'intervallo $[0, \delta]$ negli intervalli $\mathcal{I}_h := [\delta_h, \delta_{h+1}]$, per $h = 0, \dots$, dove abbiamo posto $\delta_h := \frac{h}{N+1}$. Stimando l'integrale su $\mathcal{I}_h$ con l'area del triangolo inscritto nel grafico si trova che quest'ultimo vale approssimativamente $4N^2(\pi h)^{-2}$ quando h è dispari. Facendo la somma su tutti i valori ammissibili di h si trova, coerentemente con quanto già sappiamo, che l'integrale a destra nella (1.10) vale $N + o(N)$.

§2. Il problema di Goldbach

Dopo questa lunga introduzione volta alla spiegazione del meccanismo del metodo del cerchio in un caso (relativamente) semplice, siamo pronti ad affrontare il ben piú complicato problema di Goldbach. Da qui in poi, le variabili p, p_1, p_2, $\dots$, indicano sempre numeri primi. Ci interessa il numero di rappresentazioni di n come somma di due primi

$$r_2(n) := \big|\{(p_1, p_2) \in \mathfrak{P} \times \mathfrak{P} : n = p_1 + p_2\}\big|,$$

dove p_1 e p_2 non sono necessariamente distinti, ma consideriamo distinte le rappresentazioni p_1+p_2 e p_2+p_1 se $p_1 \ne p_2$. Per il momento non facciamo l'ipotesi che n sia pari. Prendiamo un intero grande N e poniamo

$$V(\alpha) = V_N(\alpha) := \sum_{p \le N} e(p\alpha).$$

Per l'ortogonalità della funzione esponenziale complessa, per $n \le N$ si ha

$$\int_0^1 V(\alpha)^2 e(-n\alpha)\,\mathrm{d}\alpha = \sum_{p_1 \le N} \sum_{p_2 \le N} \int_0^1 e\big((p_1 + p_2 - n)\alpha\big)\,\mathrm{d}\alpha = r_2(n). \tag{2.1}$$

Di nuovo, questa è la formula che dà l'n-simo coefficiente di Fourier della funzione $V(\alpha)^2$ (cfr (1.6)), e permette di trasformare il problema di Goldbach in un problema che può essere affrontato con le tecniche dell'analisi reale e complessa.

Suddividiamo l'intervallo unitario $[0,1]$ (o il cerchio unitario che si ottiene mediante l'applicazione $x \mapsto e^{2\pi i x}$) in sotto-intervalli centrati approssimativamente sui numeri razionali con denominatore $q \le Q$, dove $Q = Q(N)$ è un parametro. Questa suddivisione si chiama dissezione di Farey di ordine Q (vedi Hardy & Wright [10] Cap. 3). Gli intervalli corrispondenti ai numeri razionali con denominatore $q \le P$ (dove $P = P(N)$ è un altro parametro, che di solito viene scelto in modo tale che PQ valga circa N) si chiamano *archi principali* e gli altri *archi secondari* (ma in italiano non è infrequente la dizione impropria di archi maggiori e minori). Hardy & Littlewood osservarono che la funzione V_N ha uno sviluppo asintotico su ciascuno degli archi principali che corrisponde ad un picco della funzione vicino ai punti razionali con denominatore "piccolo" (vedi Figura 1). Sfruttando il contributo di questi picchi, e trascurando i termini d'errore, Hardy & Littlewood ritrovarono le formule che nella mia conferenza precedente [19] hanno il numero (6), (8) e (10) ed anche l'ultima formula nella "Coda."

Per motivi tecnici che saranno piú chiari in seguito, invece di studiare la funzione $r_2(n)$ consideriamo piuttosto la versione "pesata"

$$R_2(n) := \sum_{p_1+p_2=n} \log p_1 \log p_2.$$

In altre parole, invece di contare ogni rappresentazione di n come $p_1 + p_2$ con peso 1, la facciamo pesare $\log p_1 \log p_2$. Naturalmente $r_2(n)$ è positiva se e solo se $R_2(n)$ lo è, e quindi se l'obiettivo è semplicemente quello di dimostrare la congettura di Goldbach nella sua forma originaria, possiamo tranquillamente formularla mediante $R_2(n)$. Con notazione ormai tradizionale scriviamo

$$S(\alpha) = S_N(\alpha) := \sum_{p\le N} \log p\, e(p\alpha) \qquad \text{e} \qquad \theta(N;q,a) := \sum_{\substack{p\le N \\ p\equiv a \mod q}} \log p.$$

Ricordiamo ora il Teorema dei Numeri Primi nelle progressioni aritmetiche: uniformemente per $q \le (\log N)^A$, dove $A > 0$ è una costante arbitraria ma fissata, si ha

$$\theta(N;q,a) = \frac{N}{\varphi(q)} + E_1(N;q,a) \quad \text{dove} \quad E_1(N;q,a) = \mathcal{O}_A\Big(N \exp\{-C(A)\sqrt{\log N}\}\Big) \tag{2.2}$$

purché $(a,q) = 1$ (vedi Davenport [2] Cap. 22), dove φ è la funzione di Eulero, che conta il numero degli interi h nell'intervallo $[1,q]$ tali che $(h,q) = 1$ e $C(A)$ è una costante positiva che dipende solo da A. In analogia con la (2.1), per $n \le N$ si ha

$$R_2(n) = \int_0^1 S(\alpha)^2 e(-n\alpha)\,\mathrm{d}\alpha. \tag{2.3}$$

Come operazione preliminare, calcoliamo i valori di $S(0)$, $S\big(\frac12\big)$, $S\big(\frac13\big)$, $S\big(\frac14\big)$ (vedi Figura 1). Tenendo presente il fatto che $e\big(\frac12\big) = -1$, $e\big(\frac13\big) + e\big(\frac23\big) = -1$, $e\big(\frac14\big) + e\big(\frac34\big) = 0$ e che per la (2.2) si ha $\theta(N;q,a) \approx \frac{1}{\varphi(q)}N$, abbiamo

$$\begin{aligned}
S(0) &= \theta(N;1,1) \approx N;\\
S\big(\tfrac12\big) &= -\theta(N;1,1) + 2\log 2 \approx -N;\\
S\big(\tfrac13\big) &= e\big(\tfrac13\big)\theta(N;3,1) + e\big(\tfrac23\big)\theta(N;3,2) + \log 3 \approx -\frac12 N;
\end{aligned}$$

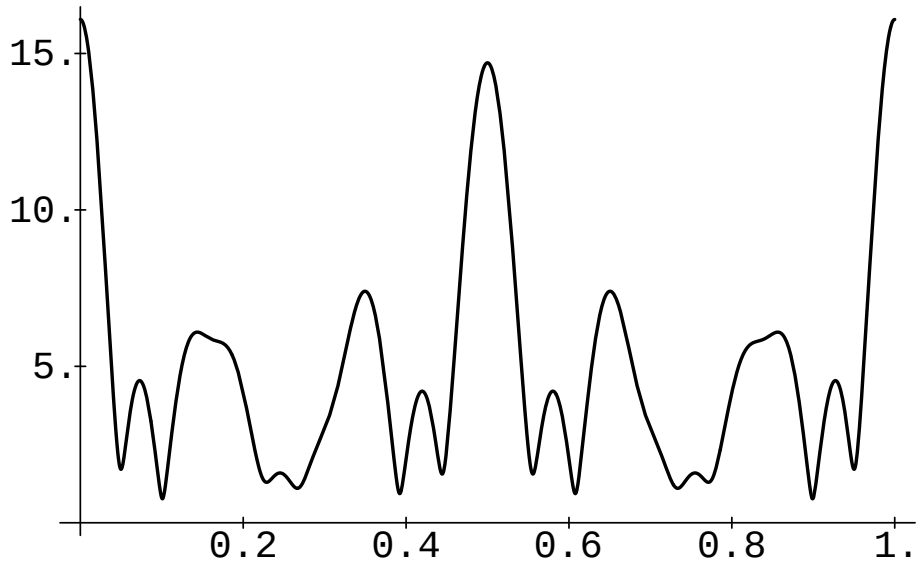

Figura 1. *Il grafico della funzione $|S_{20}(\alpha)|$ nel quale si notano molto bene i picchi in prossimità dei valori razionali di $\alpha = 0$, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, $\frac{1}{6}$, $\frac{5}{6}$, mentre in $\alpha = \frac{1}{4}$, $\frac{3}{4}$ non c'è picco poiché $\mu(4) = 0$.*

$$S\big(\tfrac14\big) = e\big(\tfrac14\big)\theta(N;4,1) + e\big(\tfrac34\big)\theta(N;4,3) + \log 2 \approx 0;$$

Piú in generale, ora calcoliamo S su un razionale $\frac{a}{q}$, quando $1 \le a \le q$ ed $(a,q) = 1$:

$$\begin{aligned} S\left(\frac{a}{q}\right) &= \sum_{h=1}^{q} \sum_{\substack{p\le N\\ p\equiv h \bmod q}} \log p\, e\big(p\tfrac{a}{q}\big) = \sum_{h=1}^{q} e\big(h\tfrac{a}{q}\big) \sum_{\substack{p\le N\\ p\equiv h \bmod q}} \log p \\ &= \sum_{h=1}^{q} e\big(h\tfrac{a}{q}\big)\theta(N;q,h) = \sum_{h=1}^{q}{}^{*} e\big(h\tfrac{a}{q}\big)\theta(N;q,h) + \mathcal{O}(\log q \log N), \end{aligned} \tag{2.4}$$

dove * significa che alla somma abbiamo aggiunto la condizione supplementare $(h,q) = 1$. Per il Teorema 272 di [10] e per la (2.4) abbiamo dunque

$$\begin{aligned} S\left(\frac{a}{q}\right) &= \frac{N}{\varphi(q)} \sum_{h=1}^{q}{}^{*} e\big(h\tfrac{a}{q}\big) + \sum_{h=1}^{q}{}^{*} e\big(h\tfrac{a}{q}\big) E_1(N;q,h) + \mathcal{O}(\log q \log N) \\ &= \frac{\mu(q)}{\varphi(q)} N + \sum_{h=1}^{q}{}^{*} e\big(h\tfrac{a}{q}\big) E_1(N;q,h) + \mathcal{O}(\log q \log N), \end{aligned} \tag{2.5}$$

dove μ è la funzione di Möbius (vedi [10] §16.3): qui è sufficiente ricordare che $\mu(q) = 0$ se q è divisibile per il quadrato di qualche numero primo, mentre $\mu(q) = (-1)^k$ se q è prodotto di k numeri primi *distinti*. È questo il senso preciso in cui si deve intendere l'affermazione precedente che $|S(\alpha)|$ è grande quando α è un numero razionale: si noti che la grandezza di $\big|S\big(\frac{a}{q}\big)\big|$ decresce essenzialmente come $\frac{1}{q}$.

Poiché S è una funzione continua, ci si aspetta che $|S|$ sia grande in un intorno di $\frac{a}{q}$, e cercheremo di sfruttare questo fatto per trovare una formula approssimata per $R_2(n)$. Per cominciare, estendiamo l'influenza del picco vicino ad $\frac{a}{q}$ per quanto ci è possibile: lo strumento piú semplice da usare a questo proposito è la formula di sommazione parziale (vedi Hardy & Wright [10], §22.5, Teorema 421, oppure Vaughan [15], Lemma 2.6, o anche

[18], §A.1). Si tratta di una formula simile a quella di integrazione per parti. È essenziale sottolineare il fatto che il numero e la larghezza degli archi principali dipendono in modo cruciale dalla possibilità di ottenere una buona stima per il termine d'errore che compare nel passaggio da $S\big(\frac{a}{q}\big)$ ad $S(\alpha)$, dove α appartiene all'arco che contiene $\frac{a}{q}$: si può dimostrare che questo errore è dell'ordine di $q\big(1+N\big|\alpha-\frac{a}{q}\big|\big)E_1(N;q,a)$ (Vaughan [15], Lemma 3.1). Poniamo $\alpha := \frac{a}{q}+\eta$. Ci si può dunque aspettare che per $|\eta|$ "piccolo" si abbia

$$S\left(\frac{a}{q}+\eta\right) = \frac{\mu(q)}{\varphi(q)}\sum_{m\le N} e(m\eta) + E_2(N;q,a,\eta) = \frac{\mu(q)}{\varphi(q)}T(\eta) + E_2(N;q,a,\eta) \tag{2.6}$$

dove, per la formula di sommazione parziale, per la (2.2) e per la (2.5), si ha

$$E_2(N;q,a,\eta) = \mathcal{O}_A\Big(q\big(1+N|\eta|\big)N\exp\{-C(A)\sqrt{\log N}\}\Big).$$

Queste formule mostrano piuttosto chiaramente che non possiamo prendere i nostri archi principali troppo numerosi o troppo ampi oppure q troppo grande se vogliamo ancora avere un termine d'errore sufficientemente piccolo.

Indichiamo con $\mathfrak{M}(q,a) := \big(\frac{a}{q}-\xi(q,a), \frac{a}{q}+\xi'(q,a)\big)$ l'arco di Farey relativo al numero razionale $\frac{a}{q}$ (osservando che si prendono $\xi(q,a)$ e $\xi'(q,a)$ dell'ordine di $(qQ)^{-1}$), e scriviamo

$$\mathfrak{M} := \bigcup_{q\le P}\ \bigcup_{a=1}^{q}{}^{*}\ \mathfrak{M}(q,a) \qquad \text{e} \qquad \mathfrak{m} := [\xi(1,1), 1+\xi(1,1)] \setminus \mathfrak{M},$$

dove di nuovo * indica che abbiamo aggiunto la condizione supplementare $(a,q)=1$. $\mathfrak{M}$ è dunque l'insieme degli archi principali, ed il suo complementare $\mathfrak{m}$ è l'insieme degli archi secondari. Abbiamo traslato l'intervallo di integrazione da $[0,1]$ a $\big[\xi(1,1), 1+\xi(1,1)\big]$ per evitare di avere due "semi-archi" in 0 ed in 1, ma questo è legittimo perché tutte le funzioni di cui ci stiamo occupando hanno periodo 1. Per $n \le N$ dalla (2.3) abbiamo

$$\begin{aligned} R_2(n) &= \int_0^1 S(\alpha)^2 e(-n\alpha)\,\mathrm{d}\alpha = \left(\int_{\mathfrak{M}} + \int_{\mathfrak{m}}\right) S(\alpha)^2 e(-n\alpha)\,\mathrm{d}\alpha \\ &= \sum_{q\le P}\ \sum_{a=1}^{q}{}^{*} \int_{-\xi(q,a)}^{\xi'(q,a)} S\left(\frac{a}{q}+\eta\right)^2 e\Big(-n\big(\tfrac{a}{q}+\eta\big)\Big)\,\mathrm{d}\eta + \int_{\mathfrak{m}} S(\alpha)^2 e(-n\alpha)\,\mathrm{d}\alpha \\ &= R_{\mathfrak{M}}(n) + R_{\mathfrak{m}}(n), \end{aligned}$$

diciamo. D'ora in avanti scriveremo $\approx$ per indicare un'uguaglianza asintotica attesa (ma non ancora dimostrata). Se per il momento trascuriamo il contributo degli archi secondari $R_{\mathfrak{m}}(n)$ e tutti i termini d'errore trovati fin qui, per la (2.6) abbiamo

$$\begin{aligned} R_{\mathfrak{M}}(n) &\approx \sum_{q\le P}\ \sum_{a=1}^{q}{}^{*} \int_{-\xi(q,a)}^{\xi'(q,a)} \frac{\mu(q)^2}{\varphi(q)^2} T(\eta)^2 e\big(-n\big(\tfrac{a}{q}+\eta\big)\big)\,\mathrm{d}\eta \\ &= \sum_{q\le P} \frac{\mu(q)^2}{\varphi(q)^2} \sum_{a=1}^{q}{}^{*} e\big(-n\tfrac{a}{q}\big) \int_{-\xi(q,a)}^{\xi'(q,a)} T(\eta)^2 e(-n\eta)\,\mathrm{d}\eta. \end{aligned} \tag{2.7}$$

Se estendiamo l'integrale a tutto l'intervallo $[0,1]$ troviamo

$$\int_0^1 T(\eta)^2 e(-n\eta)\,\mathrm{d}\eta = \sum_{m_1+m_2=n} 1 = n-1 \approx n. \tag{2.8}$$

Dunque, si può pensare che $R_2(n)$ sia ben approssimato da

$$R_{\mathfrak{M}}(n) \approx n \sum_{q\le P} \frac{\mu(q)^2}{\varphi(q)^2} \sideset{}{^*}\sum_{a=1}^{q} e\big(-n\tfrac{a}{q}\big). \tag{2.9}$$

La somma interna si chiama "somma di Ramanujan" ed è possibile calcolarne il valore in termini delle funzioni μ e φ (vedi [10], §16.6, Teorema 272; nella (2.5) abbiamo usato la stessa formula nel caso $n=1$) e quindi la (2.9) diventa

$$R_{\mathfrak{M}}(n) \approx n \sum_{q\le P} \frac{\mu(q)^2}{\varphi(q)^2} \mu\left(\frac{q}{(q,n)}\right) \frac{\varphi(q)}{\varphi\left(\frac{q}{(q,n)}\right)} = n \sum_{q\le P} \frac{\mu(q)^2}{\varphi(q)} \frac{\mu\left(\frac{q}{(q,n)}\right)}{\varphi\left(\frac{q}{(q,n)}\right)}.$$

Ora estendiamo la somma a tutti gli interi $q\ge 1$ (commettendo un errore stimabile in modo preciso): osserviamo che l'addendo della somma è una "funzione moltiplicativa" di q (vedi [18], Cap. 2), e quindi per il Teorema 285 di [10] abbiamo

$$R_2(n) \approx n \sum_{q\le P} \frac{\mu(q)^2}{\varphi(q)} \frac{\mu\left(\frac{q}{(q,n)}\right)}{\varphi\left(\frac{q}{(q,n)}\right)} \approx n \sum_{q\ge 1} \frac{\mu(q)^2}{\varphi(q)} \frac{\mu\left(\frac{q}{(q,n)}\right)}{\varphi\left(\frac{q}{(q,n)}\right)} = n \prod_p \big(1+f_n(p)\big) \tag{2.10}$$

dove il prodotto è esteso a tutti i numeri primi ed

$$f_n(p) := \frac{\mu(p)^2}{\varphi(p)} \frac{\mu\left(\frac{p}{(p,n)}\right)}{\varphi\left(\frac{p}{(p,n)}\right)} = \begin{cases} \dfrac{1}{p-1} & \text{se } p \mid n, \\ -\dfrac{1}{(p-1)^2} & \text{se } p \nmid n. \end{cases}$$

Cominciamo subito con l'osservare che se n è dispari il fattore $1+f_n(2)$ vale 0, e quindi, correttamente, la nostra formula (2.10) predice che non ci dobbiamo aspettare rappresentazioni di n come somma di due numeri primi. In effetti, se n è dispari allora $R_2(n)=0$ se $n-2$ non è primo, ed $R_2(n)=2\log(n-2)$ se $n-2$ è primo: il risultato della formula (2.10) deve essere inteso nel senso che $R_2(n)$ ha ordine di grandezza piú piccolo di n, e questo è certamente vero. Viceversa, se n è pari possiamo trasformare la (2.10) con qualche calcolo:

$$\begin{aligned} R_2(n) &\approx n \prod_{p\mid n} \left(1+\frac{1}{p-1}\right) \prod_{p\nmid n} \left(1-\frac{1}{(p-1)^2}\right) \\ &= 2n \prod_{\substack{p\mid n \\ p>2}} \left(\frac{p}{p-1}\cdot\frac{(p-1)^2}{p(p-2)}\right) \prod_{p>2} \left(1-\frac{1}{(p-1)^2}\right) = C_0 n \prod_{\substack{p\mid n \\ p>2}} \frac{p-1}{p-2}, \end{aligned}$$

dove C_0 è la costante dei primi gemelli (vedi [19], "Coda"). Questa è dunque la formula asintotica per $R_2(n)$ data dall'euristica basata sul Teorema dei Numeri Primi nelle progressioni aritmetiche. È piú grande della formula originale per $r_2(n)$ (vedi (6) in [19]) di un fattore $(\log n)^2$ a causa dei "pesi" $\log p_1 \log p_2$ che abbiamo dato alle rappresentazioni. Nel prossimo paragrafo indicheremo brevemente quali dei punti lasciati in sospeso qui sopra rappresentano davvero un problema.

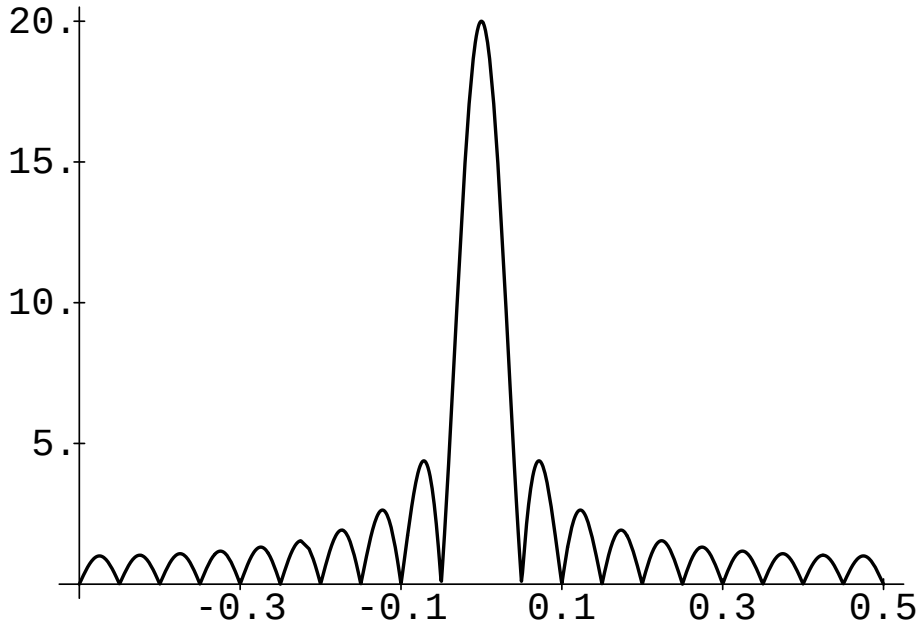

Figura 2. *Il grafico della funzione $|T_{20}(\alpha)|$ nel quale si nota molto bene che questa funzione ha un grosso picco in prossimità dei valori interi di α, ed è altrimenti molto piccola.*

§3. Dove sono le difficoltà?

Per brevità parleremo soltanto delle due piú importanti questioni che rimangono da risolvere. Infatti, l'approssimazione che facciamo nel passare dalla (2.7) alla (2.8) può essere giustificata ricordando che per la (1.8) si ha $|T(\alpha)| \le \min\bigl(N+1, \|\alpha\|^{-1}\bigr)$: la Figura 2 mostra che $T(\alpha)$ decade molto rapidamente allontanandosi dai valori interi di α. L'errore commesso nella (2.10) può essere messo in una forma quantitativa sfruttando il fatto che la serie è assolutamente convergente e che la funzione f_n è moltiplicativa. Rivolgiamo dunque la nostra attenzione all'approssimazione di $\theta(N;q,a)$ ed al contributo degli archi secondari.

L'approssimazione di θ. L'approssimazione di θ fornita dal Teorema dei Numeri Primi nelle progressioni aritmetiche (2.2) è piuttosto debole per due motivi: come abbiamo già osservato, questa è valida in un intervallo di valori di q ristretto e siamo quindi costretti a prendere il parametro P (che serve per distinguere gli archi principali da quelli secondari) piuttosto piccolo come funzione di N.

In secondo luogo la maggiorazione oggi nota per l'errore è troppo grande: come osservato nella "Coda" della conferenza [19], si congettura che questo errore sia in realtà molto piú piccolo. È noto (vedi Davenport [2], Capp. 21–22) che la differenza $\theta(N;q,a) - \frac{N}{\varphi(q)}$ dipende essenzialmente da una somma infinita i cui addendi sono del tipo $\frac{N^\varrho}{\varphi(q)\varrho}$, dove ϱ indica il generico zero complesso di certe funzioni (dette funzioni L di Dirichlet). Nel caso piú semplice, quando $q = a = 1$, c'è una sola funzione di questo tipo, detta funzione zeta di Riemann: si può dimostrare (vedi Davenport [2], (11) del Cap. 17) che per $T \le N$ si ha

$$\theta(N;1,1) = N - \sum_{\substack{\varrho\in\mathbb{C}\ \text{t. c. } \zeta(\varrho)=0\\ \varrho=\beta+\mathrm{i}\gamma\\ |\gamma|\le T}} \frac{N^\varrho}{\varrho} + \mathcal{O}\left(\frac{N}{T}(\log N)^2 + \sqrt{N}\log N\right) \tag{3.1}$$

dove $\varrho = \beta + \mathrm{i}\gamma$ è il generico zero della funzione zeta di Riemann con $\beta \in (0,1)$. Non esiste una formula analoga a questa (ed altrettanto semplice) valida per $\pi(N)$, ed è per

questo che si preferisce formulare il problema di Goldbach in termini di $R_2(n)$ piuttosto che $r_2(n)$. Questa formula mostra che al posto della funzione $T(\eta)$ definita dalla (1.7), conviene prendere come approssimazione di $S\big(\frac{a}{q}+\eta\big)$ la funzione

$$K(\eta) := \sum_{n\le N}\Big(1 - \sum_{|\gamma|\le T} n^{\varrho-1}\Big)e(n\eta) \tag{3.2}$$

dove il coefficiente di $e(n\eta)$ nella (3.2) è la derivata rispetto ad N dei primi due termini nella (3.1), calcolata in n (poiché se f è regolare $\sum f(n) \sim \int f(t)\,\mathrm{d}t$). L'approssimazione di S cosí ottenuta è valida solo vicino a 0, ma introducendo le funzioni L di Dirichlet si possono trovare approssimazioni simili, valide su ciascun arco principale.

È anche noto che il caso ottimale per la distribuzione dei numeri primi è quello in cui *tutte* le parti reali β di tutti gli zeri $\varrho = \beta + \mathrm{i}\gamma$ della funzione ζ con $\gamma \neq 0$ sono uguali ad $\frac12$ (Congettura di Riemann): se cosí è, allora si hanno le buone approssimazioni equivalenti

$$\theta(N;1,1) = N + \mathcal{O}\Big(N^{1/2}(\log N)^2\Big) \qquad \text{e} \qquad \pi(N) = \int_2^N \frac{\mathrm{d}t}{\log t} + \mathcal{O}\Big(N^{1/2}\log N\Big). \tag{3.3}$$

Analogamente, se si riuscisse a dimostrare che *tutti* gli zeri di tutte le funzioni L di Dirichlet hanno parte reale uguale ad $\frac12$ (Congettura di Riemann Generalizzata), per $q \le x$ si avrebbe anche la stima (Davenport [2], Cap. 20)

$$\theta(N;q,a) = \frac{N}{\varphi(q)} + \mathcal{O}\Big(N^{1/2}(\log N)^2\Big). \tag{3.4}$$

Si osservi che le stime (3.3) e (3.4) sono ottimali, e cioè l'esponente di N nel termine d'errore non può essere ulteriormente abbassato. Questo significa che, anche se si riuscisse a dimostrarle (e non c'è alcun motivo di credere che una tale dimostrazione sia imminente), neppure in questo caso si riuscirebbe a dimostrare la congettura di Goldbach. Al momento attuale, la situazione nel caso generale $q > 1$ è piú complicata di quella nel caso $q = 1$: infatti non è ancora possibile escludere che qualcuna delle funzioni L di Dirichlet abbia uno zero reale $\beta \in (0,1)$, con β molto prossimo ad 1, e questo è essenzialmente il motivo per cui siamo costretti ad imporre una severa limitazione per q come detto a proposito della formula (2.2). L'eventuale contributo di questo zero sarebbe $\pm\frac{N^\beta}{\varphi(q)\beta}$, e cioè molto prossimo al "termine principale" $\frac{N}{\varphi(q)}$, cosí da vanificare la possibilità di avere un errore sufficientemente piccolo nella formula asintotica per $\theta(N;q,a)$ per questo particolare valore di q, e di conseguenza per $R_2(n)$.

Il contributo degli archi secondari. Il problema principale presentato dagli archi secondari è costituito dal fatto che non si riesce a dare una buona stima individuale del loro contributo: in altre parole, vedremo fra un istante che è relativamente semplice dimostrare che "in media" su tutti gli interi $n \in [1,N]$ gli archi secondari non danno un grande contributo ad $R_2(n)$, ma non è possibile trovare una maggiorazione altrettanto buona per ogni singolo valore di n. Per la formula che dà il coefficiente di Fourier n-simo, la disuguaglianza di Bessel ed il Teorema dei Numeri Primi (2.2) nel caso $q = 1$, si ha

$$\sum_{n\le N}\Big|\int_{\mathfrak{m}} S(\alpha)^2 e(-n\alpha)\,\mathrm{d}\alpha\Big|^2 \le \int_{\mathfrak{m}} |S(\alpha)|^4\,\mathrm{d}\alpha \le \sup_{\alpha\in\mathfrak{m}}|S(\alpha)|^2 \int_0^1 |S(\alpha)|^2\,\mathrm{d}\alpha$$

$$= \mathcal{O}\Big(N \log N \sup_{\alpha\in\mathfrak{m}} |S(\alpha)|^2\Big).$$

Dalla (2.5) possiamo aspettarci (e questo può essere dimostrato rigorosamente in una forma piú debole ma sufficiente ai nostri scopi: vedi Davenport [2], Cap. 25) che l'estremo superiore qui sopra valga essenzialmente N^2P^{-2} dato che se $\alpha \in \mathfrak{m}$ allora è "vicino" ad un razionale con denominatore $> P$. In effetti si riesce a dimostrare che

$$\sum_{n\le N} |R_{\mathfrak{m}}(n)|^2 = \sum_{n\le N} \Big|\int_{\mathfrak{m}} S(\alpha)^2 e(-n\alpha)\,\mathrm{d}\alpha\Big|^2 = \mathcal{O}\big(N^3(\log N)^4 P^{-1}\big)$$

e questo dice che, per la "maggioranza" degli interi $n \in [1, N]$ si ha $|R_{\mathfrak{m}}(n)| = \mathcal{O}\big(NP^{-1/3}\big)$, che ha ordine di grandezza minore del contributo degli archi principali dato dalla (2.10).

§4. Varianti: il Teorema dei tre primi ed i Primi gemelli

Il metodo di Hardy & Littlewood è estremamente flessibile e si può applicare ad una grande quantità di problemi diversi. Per esempio, con notazione analoga a quella di sopra abbiamo

$$R_3(n) := \sum_{p_1+p_2+p_3=n} \log p_1 \log p_2 \log p_3 = \int_0^1 S(\alpha)^3 e(-n\alpha)\,\mathrm{d}\alpha$$

se $n \le N$. Un'argomentazione simile a quella qui sopra mostra che $R_3(n)$ può essere bene approssimata dal solo contributo degli archi principali e questo dà la relazione (8) della [19] moltiplicata per $(\log n)^3$, sempre a causa della presenza dei pesi nella somma che definisce $R_3(n)$. Il fatto di avere 3 addendi invece di 2 fa mutare completamente la natura del problema: ci limitiamo ad osservare che in questo caso è piuttosto semplice trovare una buona maggiorazione individuale per il contributo degli archi secondari, cioè per ogni $n \le N$. Infatti abbiamo essenzialmente (vedi Davenport [2], Cap. 26)

$$\Big|\int_{\mathfrak{m}} S(\alpha)^3 e(-n\alpha)\,\mathrm{d}\alpha\Big| \le \sup_{\alpha\in\mathfrak{m}} |S(\alpha)| \int_0^1 |S(\alpha)|^2\,\mathrm{d}\alpha = \mathcal{O}\Big(N^2(\log N)^4 P^{-1/2}\Big).$$

Deshouillers, Effinger, te Riele & D. Zinoviev [3] hanno dimostrato che se è vera la Congettura di Riemann Generalizzata allora *tutti* gli interi dispari $n \ge 7$ si possono scrivere come somma di tre numeri primi. Una semplice osservazione mostra anche come il problema dei primi gemelli sia naturalmente legato al problema di Goldbach: in analogia con la notazione di [19] poniamo

$$\theta_N(n) := \sum_{\substack{p_2\le N\\ p_2-p_1=n}} \log p_1 \log p_2 = \int_0^1 |S(\alpha)|^2 e(-n\alpha)\,\mathrm{d}\alpha,$$

come si vede con un breve calcolo. Questo mostra che i due problemi sono strettamente legati e della stessa difficoltà.

§5. Riferimenti Bibliografici

Il riferimento classico per il metodo del cerchio è la monografia di Vaughan [15]. Si vedano anche Hardy [6], Cap. 8 (in particolare i §§8.1–8.7) e James [11], §5. La genesi dell'idea di

studiare il comportamento della funzione generatrice in prossimità di diverse singolarità è esposta molto chiaramente in Hardy & Ramanujan [9] (in particolare i §§1.2–1.5) ed in Hardy [6], Cap. 8 (in particolare i §§8.6–8.7). Per il problema ternario di Goldbach si veda il §3.1 di Vaughan [15]. Nel §3.2 si dimostra che, detto $\mathcal{E}(x) := \{2n \le x : r_2(2n) = 0\}$, per ogni $A > 0$ si ha $|\mathcal{E}(x)| = \mathcal{O}_A\big(x(\log x)^{-A}\big)$. Montgomery & Vaughan [13] hanno dimostrato il risultato piú forte che esiste $\delta > 0$ tale che $|\mathcal{E}(x)| = \mathcal{O}\big(x^{1-\delta}\big)$, calcolando con precisione il contributo del possibile zero reale β di cui si parla sopra. Un'applicazione del metodo del cerchio a diversi problemi legati alla congettura di Goldbach si può trovare in Languasco [12], mentre in [16–17] sono trattati problemi additivi "misti" ed in [17] si può trovare anche una breve introduzione al metodo del cerchio simile alla presente. Nelle dispense [18] si può trovare un'introduzione ad alcuni dei problemi citati in questa conferenza. Un'altra argomentazione euristica per il numero dei primi gemelli si trova in Hardy & Wright [10], §22.20. Le congetture di cui si parla in questa conferenza e nella [19] sono inquadrate nel contesto generale della congettura di Schinzel & Sierpiński nell'introduzione di Halberstam & Richert [5]; si vedano le Note relative per la versione quantitativa di Bateman & Horn (vedi [19], "Coda" per il caso delle "costellazioni" di primi). Una maggiorazione per $r_2(n)$ del giusto ordine di grandezza è contenuta nel Teorema 3.11 di Halberstam & Richert [5]. La dimostrazione completa del Teorema dei tre primi di Vinogradov si trova nel Cap. 26 di Davenport [2]. Per altre strategie per la dimostrazione della congettura di Goldbach si veda anche Ribenboim [14], §4.VI, e per ulteriori riferimenti Guy [4], §C.1. Chen ha dimostrato che ogni numero pari sufficientemente grande può essere scritto come somma di un primo e di un intero che ha al massimo 2 fattori primi (Halberstam & Richert [5], Cap. 10). Una dimostrazione relativamente semplice di questo fatto (ma con 4 al posto di 2) si trova nel §9 di Bombieri [1].

[1] E. Bombieri, *Le Grand Crible dans la Théorie Analytique des Nombres*, Astérisque n. 18, Societé Mathématique de France, Paris, 1974.

[2] H. Davenport, *Multiplicative Number Theory*, 2ª ed., Springer, Berlin, 1980.

[3] J.-M. Deshouillers, G. Effinger, H. te Riele & D. Zinoviev, *A complete Vinogradov 3-primes theorem under the Riemann Hypothesis*, Electr. Res. Announcements Amer. Math. Soc. **3** (1997), 99–104.

[4] R. K. Guy, *Unsolved Problems in Number Theory*, 2ª ed., Springer, Berlino, 1994.

[5] H. Halberstam & H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[6] G. H. Hardy, *Ramanujan. Twelve Lectures on Subjects Suggested by His Life and Work*, 3ª ed., Chelsea, New York, 1999.

[7] G. H. Hardy & J. E. Littlewood, *Some problems of "Partitio Numerorum"; III: On the expression of a number as a sum of primes*, Acta Math. **44** (1923), 1–70.

[8] ———, *Some problems of "Partitio Numerorum"; V. A further contribution to the study of Goldbach's problem*, Proc. London Math. Soc. (2) **22** (1923), 46–56.

[9] G. H. Hardy & S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. (2) **17** (1918), 75–115, = S. Ramanujan, "Collected papers," edited by G. H. Hardy, P. V. Seshu Aiyar & B. M. Wilson, 3ª ed., AMS–Chelsea, 1999; n. 36, 276–309.

[10] G. H. Hardy & E. M. Wright, *An Introduction to the Theory of Numbers*, 5ª ed., Oxford U. P., 1979.

[11] R. D. James, *Recent progress in the Goldbach problem*, Bull. Amer. Math. Soc. **55** (1955), 246–260.

[12] A. Languasco, *Some results on Goldbach's problem*, Rend. Sem. Mat. Univ. Pol. Torino **53 (4)** (1995), 325–337.

[13] H. L. Montgomery & R. C. Vaughan, *On the exceptional set in Goldbach's problem*, Acta Arith. **27** (1975), 353–370.

[14] P. Ribenboim, *The New Book of Prime Number Records*, Springer, Berlino, 1996.

[15] R. C. Vaughan, *The Hardy–Littlewood Method*, 2ª ed., Cambridge U. P., Cambridge, 1997.

[16] A. Zaccagnini, *Somme di primi e k-esime potenze*, Tesi di dottorato, 1994.

[17] ———, *Additive problems with prime numbers*, Rend. Sem. Mat. Univ. Pol. Torino **53 (4)** (1995), 471–486.

[18] ———, *Metodi elementari in teoria analitica dei numeri*, Dispense del corso di "Teoria dei Numeri," A. A. 1999–2000, Università di Parma.

[19] _____, *Variazioni Goldbach: problemi con numeri primi*, L'Educazione Matematica, Anno XXI, Serie VI, **2** (2000), 47–57.

N. B.: I testi [18] e [19] sono disponibili su rete rispettivamente agli indirizzi
`http://www.math.unipr.it/∼zaccagni/psfiles/DispenseTdN.ps`
`http://www.math.unipr.it/∼zaccagni/psfiles/Goldbach_I.ps`

Dipartimento di Matematica, Università di Parma, via Massimo d'Azeglio 85/A, 43100, Parma
E-mail address: `zaccagnini@prmat.math.unipr.it`
URL: `http://www.math.unipr.it/∼zaccagni/home.html`