Block Notes Matematico

Il Metodo del cerchio

Problemi additivi – congettura di Goldbach

ing. Rosario Turco

Introduzione

Uno dei temi tipici della Teoria dei Numeri, che facilmente attira tutti gli appassionati di Matematica, anche per la sua facilità di comprensione della definizione del problema, è la congettura di Goldbach: eppure è un problema solo apparentemente semplice, come vedremo nel seguito.

Fin quando si rimane in ambito algebrico, geometrico, di matematica elementare e per bassi valori di interi (per alti intendiamo ad esempio valori come 10^10^10000), allora apparentemente sembra una congettura dimostrabile e vera. Se la congettura, invece, è affrontata in ambito analisi complessa, allora si scoprono ulteriori problematiche che possono mettere in crisi le dimostrazioni elementari trovate.

Per quanto riguarda l'utilizzo di metodi elementari, secondo "scuola Erdos", sono utilizzati attualmente solo a valle di una dimostrazione di una congettura, come tentativo di semplificazione del procedimento dimostrativo complesso.

Nel seguito viene descritto il "metodo del cerchio" introdotto negli anni '20 da Hardy, Littlewood e Ramanujan e semplificato, successivamente, da Vinogradov; il metodo fu introdotto perché fu individuato come adatto all'analisi complessa di *problemi additivi* (particolari *equazioni diofantee*), come la congettura di Goldbach ed il problema di Waring, su cui Hardy, Littlewood e Ramanujan hanno lasciato preziosi contributi.

Si mostreranno, infine, gli attuali dubbi esistenti sulla risoluzione della congettura di Goldbach, nati a seguito degli studi di Montgomery e Vaughan.

L'articolo, quindi, ha scopo divulgativo, sulla complessità dei problemi che sono dietro alla congettura di Goldbach.

Richiami di analisi complessa

Per comprendere meglio l'argomento facciamo un breve accenno all'analisi complessa necessaria, anche con qualche semplificazione non rigorosa, a vantaggio della comprensione; ovviamente approfondimenti maggiori sono consigliati al lettore su testi ulteriori, universitari e non.

Una serie di potenze in $\mathbb{C}$ è una serie del tipo:

$$f(z) = \sum_{k=0}^{\infty} a_k \cdot (z - z_0)^k$$

Per le serie di potenze in campo complesso valgono analoghi Teoremi esistenti nel campo reale. La regione di convergenza di una serie di potenza in $\mathbb{C}$ è un cerchio centrato su z0 , il cui raggio è il *raggio di convergenza* della serie. All'interno del cerchio la serie è uniformemente e assolutamente convergente; mentre sul cerchio dipende dalla situazione, cioè potrebbe essere non convergente o meno a causa della presenza o meno di punti di singolarità sulla curva stessa. All'esterno del cerchio, invece, la serie non convergerà mai.

Teorema di Weiestrass

Una serie di potenze, per ogni punto z interno alla circonferenza, è derivabile termine a termine *n* volte:

$$\frac{d^n f(z)}{dz^n} = \sum_{k=0}^{\infty} a_k \cdot \frac{d^n (z - z_0)^k}{dz^n}$$

Quindi la funzione è analitica in tutto il cerchio.

Teorema di Cauchy - Hadamard

Il raggio di convergenza ρ della serie di potenze

$$\sum_{k=0}^{\infty} a_k \cdot (z - z_0)^k$$

coincide con l'inverso del massimo trai punti di accumulazione della successione

$$\left\{ | a_k |^{1/k} \right\},$$

ovvero se esiste il limite è:

$$\rho = \left\{ \lim_{x \to \infty} | a_k |^{1/k} \right\}^{-1}$$

Serie di Taylor

Lo sviluppo in serie di Taylor conduce ad una serie di potenze di una funzione f(z) attorno ad un suo punto di analiticità (dove è analitica e non singolare). Poiché la funzione è analitica, è anche infinitamente derivabile[1] e, quindi, sviluppabile in serie di Taylor:

[1] In campo reale non è sufficiente l'infinita derivabilità di una funzione perché sia anche sviluppabile in serie di Taylor. In campo complesso è l'analiticità della funzione che lo permette.

$$f(z) = \sum_{k=0}^{\infty} a_k \cdot (z - z_0)^k$$

Dove:

$$a_k = \frac{1}{k!}\left[\frac{d^k f(z)}{dz^k}\right]_{z=z_0} = \frac{1}{2\pi i}\oint \frac{f(z)}{(z-z_0)^{k+1}}\,dz$$

Dove l'integrale di destra è lungo una curva γ(ρ) ed è la rappresentazione del Teorema di Cauchy (o anche del Teorema dei residui) della derivata di una funzione analitica. Ovviamente z_0 può anche essere z_0=0.

In generale il dominio di convergenza della serie è un cerchio con origine in z_0 e raggio pari alla distanza di z_0 al più vicino punto di singolarità.

Se consideriamo la serie geometrica

$$\sum_{k=0}^{\infty} z^k$$

Essa converge uniformemente a:

$$f(z) = \frac{1}{1-z}$$

nella regione |z|<1; mentre su z=1 c'è una singolarità.

Qui non facciamo richiami sui tipi di punti di singolarità, cioè zeri (semplici e molteplici), poli etc., demandando al lettore ulteriori approfondimenti.

Funzione di Partizionamento P(n)

Hardy, Littlewood e Ramanujan usarono le serie di potenze e, quindi l'analisi complessa per affrontare i problemi additivi come quello di Waring e quello di Goldbach. Il metodo è ricordato come "Metodo del cerchio", a causa del cerchio con raggio di convergenza della serie di potenze, oppure metodo di Hardy, Littlewood e Ramanujan.[2] Il metodo è nato durante la loro investigazione della funzione di partizionamento P(n).

Per comprendere il problema in maniera più elementare, introduciamo innanzitutto i partizionamenti sui numeri interi, in modo da capire come nascono le funzioni generatrici che ci portano, poi, alle serie di potenze.

[2] Probabilmente è meglio ricordarlo come "Metodo del cerchio" (The Circle Method), perché ci sono stati raffinamenti successivi anche di altri studiosi, primo tra tutti di Vinogradov e forse in futuro anche di altri.

Se nϵN allora chiameremo P(n) la *funzione di partizione*, che conta il numero di modi di scrivere n come somma di interi positivi scartando le soluzioni simmetriche (esempio: 3+1 e 1+3 se ne conta solo una).

Esempio n=4 P(4)=5 difatti:

4 = 4

4 = 3 + 1

4 = 2 + 2

4 = 2 + 1 + 1

4 = 1 + 1 + 1 + 1

Eulero e le funzioni generatrici

Eulero definì *identità formale della serie di potenze* la seguente identità:

$$f(x)=\frac{1}{(1-x)(1-x^2)(1-x^3)...}=1+\sum_{n=1}^{\infty}P(n)x^n$$

Per identità formale si intende che, senza preoccuparsi della convergenza, i due lati dell'identità hanno per ogni n gli stessi coefficienti di x^n.

La f(x) è definita *funzione generatrice* della funzione partizione P(n) (o della serie di potenza a destra dell'identità); per cui se a_n o a(n) è una funzione aritmetica, allora si può scrivere che :

$$f(x)=1+\sum_{n=1}^{\infty}a(n)x^n$$

Ecco che, quindi, sono di interesse le serie di potenze; ovviamente qui si intuisce subito che calcolare a(n) significa calcolare P(n).

Funzioni generatrici nel Metodo del cerchio

Se consideriamo una *funzione generatrice* di una serie di potenze con z_0=0 e ρ=1 allora avremo:

$$f(z)=\sum_{n=0}^{\infty}a_n\cdot z^n \quad \begin{cases} \mathrm{a_n}=1 \text{ se } \mathrm{a_n}\in N \\ 0 \text{ altrimenti} \end{cases}$$

Spesso interessano solo le rappresentazioni a k alla volta di numeri a_i, la cui somma restituisce un altro numero n; per cui le k-ple ottenibili, nell'ambito dell'insieme degli interi N, sono solo un sottoinsieme del prodotto cartesiano N^k (o di N x N se k=2).

Ad esempio per k=2 se *n* è il numero somma appartenente a N (insieme degli interi), e a1, a2 i numeri appartenenti a N, allora le rappresentazioni a coppie dei numeri a_i sono:

$$r_2(n) := \{(a_1, a_2) \in N \times N : n = a_1 + a_2\} \qquad (1)$$

In generale con la serie di Taylor o col Teorema dei residui si otterrebbe che:

$$r_2(n) = \frac{1}{2\pi i} \oint \frac{f(z)}{z^{n+1}} dz \qquad (2)$$

Ovvero $r_2(n)$ corrisponderebbe con a_n della serie.

Dovendo lavorare con un prodotto cartesiano, si potrebbe anche definire (per il *prodotto di Cauchy*):

$$f^2(z) = \sum_{n=0}^{\infty} c_n \cdot z^n \quad c_n = \sum_{h \geq 0} \sum_{\substack{k \leq n \\ h+k=n}}^{\infty} a_h \cdot a_k z^n \qquad (3)$$

Con $a_k a_h \neq 1$ se h e k appartengono a N, allora c_n corrisponde a $r_2(n)$; ovvero anche qui è:

$$r_2(n) = \frac{1}{2\pi i} \oint \frac{f^2(z)}{z^{n+1}} dz \qquad (4)$$

Dove l'integrale di destra è lungo un cerchio $\gamma(\rho)$, percorso in senso antiorario, di centro l'origine e raggio unitario.

E' da aggiungere che nel caso della congettura di Goldbach dovremo sostituire a N l'*insieme dei primi P* e i termini a_i devono appartenere a P.

In generale potremmo avere a che fare con un *problema additivo* con k>2, come: il *problema di Waring* (k>2 qualsiasi e potenza s); il *Teorema di Vinogradov* (per k=3 e con gli a_i appartenenti all'insieme dei numeri primi P); il problema dei *numeri gemelli* per n=2, se –P=$\{$-2,-3,-5,-7,-11,…$\}$ e consideriamo P-P, studiando le coppie (p_1,p_2) con $p_1,p_2 \epsilon P$ tali che n=p1-p2.

Allora nel caso generale per k>2 ha interesse la risoluzione dell'equazione del tipo:

$$n = a_1 + a_2 + \ldots + a_k$$

$$r_k(n) := \{(a_1, a_2, \ldots, a_k) \in N^k : n = a_1 + a_2 + \ldots + a_k\}$$

In tal caso si deve scegliere una funzione

$$f^s(z) = \sum_{n=0}^{\infty} r_k(n) z^n$$

Per cui:

$$r_k(n) = \frac{1}{2\pi i} \oint \frac{f^s(z)dz}{z^{n+1}} \quad (4')$$

Se scegliessimo come funzione generatrice della serie, invece, la $f(z) = \sum_{n=0}^{\infty} z^n = \frac{1}{(1-z)^{-1}}$

Quindi, se la potenza della f è s=1, la (4') diventerebbe:

$$r_k(n) = \frac{1}{2\pi i} \oint \frac{dz}{(1-z)^k z^{n+1}} \quad (5)$$

La (5) del caso generale è interessante perché la funzione integranda ha una singolarità semplice su γ(1); per cui si può facilmente integrare. Difatti per $\rho<1$ possiamo sviluppare la potenza k-esima di un binomio:

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

Se sostituiamo nella (5) si ottiene:

$$r_k(n) = \frac{1}{2\pi i} \oint \frac{dz}{(1-z)^k z^{n+1}} = \frac{1}{2\pi i} \sum_{m=0}^{\infty}\binom{-k}{m}(-1)^m \oint z^{m-n-1}dz =$$

Per m = n l'integrale vale $2\pi i$, mentre 0 negli altri casi; per cui il risultato è:

$$= (-1)^n \binom{-k}{n} = \binom{n+k-1}{k-1} \quad (6)$$

La (6) rappresenta proprio il modo di scrivere n come somma di k elementi di potenza s=1. Se si usa la (6) si ritrova che P(4)=5 dell'esempio precedente.

Non sempre è possibile risolvere l'integrale; difatti la funzione integranda potrebbe avere più di una singolarità sulla curva.

Ad esempio se volessimo determinare in quanto modi possibili si possa scrivere nεN come somma di due dispari si deve considerare la funzione: $f(z) = \sum_{n=0}^{\infty} z^{2m+1} = \frac{z}{1-z^2}$ che ha singolarità in z=±1.

Questo richiederebbe uno sviluppo asintotico per la funzione integranda che sia valido nelle prossimità dei punti singolari.

L'idea iniziale del metodo

In generale l'obiettivo del metodo è di studiare il comportamento asintotico di una serie: questo si ottiene prendendo la funzione generatrice della serie e calcolando i residui (essenzialmente i coefficienti di Fourier).

La funzione generatrice della serie però è presa con raggio di convergenza unitaria, in modo da avere singolarità sul cerchio unitario. In sostanza il metodo del cerchio si occupa di come calcolare i residui con il *partizionamento* del cerchio in *archi maggiori* o principali (la maggior parte del cerchio) e *archi minori* o secondari (quelli contenenti le singolarità). Per archi si deve intendere che si farà lo spezzettamento dell'integrale almeno in due parti (archi maggiori e archi minori). La tecnica di scegliere gli archi dipende anche dal problema da risolvere (vedi [3][4]).

L'idea di base del metodo del cerchio, dovuto ad Hardy e Littlewood, è, quindi, di prendere una funzione fissata $f(z)^k$ e prendere ρ come funzione di n che ha limite 1; inoltre si devono trovare opportuni sviluppi asintotici di f nell'intorno delle singolarità (vedi [1][3]) che la funzione integranda presenta eventualmente su γ(1).

Il metodo, fin qui visto, dipende, in definitiva, dalla curva e dalla funzione scelta ed in ogni caso lo scopo iniziale non era il calcolo preciso, ma quello di affrontare in campo analitico e qualitativo tali problemi per trovare degli elementi che contraddicessero o affermassero la congettura o il problema che si affrontava.

Lo studio del metodo si dirama spesso nelle direzioni di tutti i problemi, a volte contemporaneamente, questo per capire se è possibile sfruttare i risultati di un problema anche in un altro. E' chiaro che Hardy, Littlewood e Ramanujan lo affrontarono in modo generale, così da poter avere risultati per la risoluzione di tutti i problemi additivi.

Nel seguito però ci sforzeremo di concentraci solo sul problema di Goldbach.

La semplificazione di Vinogradov

Vinogradov, invece, fece l'osservazione ulteriore che a $r_2(n)$ possono contribuire solo gli interi $m \leq n$; per cui si può introdurre una diversa funzione (rispetto a quella che ha portato alla (6)), più utile allo scopo:

$$f_N(z) := \sum_{m=0}^{N} z^m = \frac{1-z^{N+1}}{1-z} \quad \text{valida per } z \neq 1$$

Per $n \leq N$, il Teorema di Cauchy permette di scrivere:

$$r_k(n) = \frac{1}{2\pi i} \oint \frac{f_N(z)^k dz}{z^{n+1}} \qquad (7)$$

Il vantaggio adesso è che $f_N(z)$ è una somma finita e non ci sono problemi di convergenza, per cui la funzione integranda nella (7) non ha punti di singolarità e non ci sono i problemi precedenti; per cui adesso si può fissare definitivamente la curva su cui si integra. Si pone difatti come curva la funzione esponenziale complessa $e(x) := e^{2\pi i x}$ ([3]) ed effettuando un cambio di variabile z = e(α) la (7) diventa:

$$\int_0^1 V(\alpha)^2 e(-n\alpha) d\alpha = \sum_{p_1 \le N} \sum_{p_2 \le N} e((p_1 + p_2 - n)\alpha) d\alpha = r_2(n) \qquad (8)$$

La (8) è l'n-esimo coefficiente di Fourier di $f_N^k\ (e(\alpha))$. Se poniamo adesso $T(\alpha) = f_N\ (e(\alpha))$ ora è:

$$T(\alpha) = T_N(\alpha) = f_N\ (e(\alpha)) = \sum_{m=0}^{N} e(m\alpha) = \begin{cases} \dfrac{1 - e((N+1)\alpha)}{1 - e(\alpha)} = \dfrac{e(\frac{1}{2}N\alpha)\sin(\pi(N+1)\alpha)}{\sin(\pi\alpha)} & \alpha \notin Z \\ N+1 \quad \alpha \varepsilon Z \end{cases}$$

La funzione di sopra adesso è studiabile ed è uno strumento di analisi elementare sfruttabile.

Proprietà di $T_N(\alpha)$

La funzione T ha dei picchi sui valori interi e decresce molto su valori non interi. E' facile vedere, anche come calcolo numerico, (vedi [3]) che:

$$|T_N(\alpha)| \le \min(N+1, \frac{1}{|\sin(\pi\alpha)|}) \le \min(N+1, \frac{1}{||\alpha||}) \quad (9)$$

Dove $||\alpha||$ è la distanza tra due numeri, T è periodica di periodo 1 e $\alpha < \sin(\pi\alpha)$ per $\alpha \varepsilon (0,1/2]$. Se si usa la (9) e $\delta = \delta(N)$ è scelto non troppo piccolo, allora il contributo nell'intervallo $[\delta, 1-\delta]$ è trascurabile. Ad esempio se $\delta > 1/N$ allora:

$$\left| \int_\delta^{1-\delta} T_N^k(\alpha) e(-n\alpha) d\alpha \right| \le \int_\delta^{1-\delta} |T_N^k(\alpha)|\, d\alpha \le \int_\delta^{1-\delta} \frac{d\alpha}{||\alpha||^k} \le \frac{2}{k-1} \delta^{1-k} \quad (10)$$

Se si tiene conto della (8) e della (10) per n = N, k=2 e $\delta^{-1} = o(N)$ si ottiene che:

---

[3] Da notare che tale funzione è ortogonale nell'intervallo [0,1] difatti: $\int_1^0 \exp(az)\exp(-bz)dx = \begin{cases} 1 \ \ se\ a = b \\ 0\ \text{altrimenti} \end{cases}$ per cui è $r_k(n) = \int_1^0 f^k(\exp(z))\exp(-z)dz$

$$r_2(n) = \frac{1}{2\pi i}\int_0^1 \left(\frac{\sin(\pi(N+1)\alpha)}{\sin(\pi\alpha)}\right)^2 d\alpha = 2\int_\delta^{1-\delta} \left(\frac{\sin(\pi(N+1)\alpha)}{\sin(\pi\alpha)}\right)^2 d\alpha$$

In pratica la congettura di Goldbach attraverso il Metodo del cerchio

Ora disponiamo di molti elementi di impalcatura, per iniziare a comprendere come viene applicato il Metodo del cerchio alla congettura di Goldbach.

La congettura di Goldbach, senza considerare la differenza tra la congettura debole e quella forte, dice che "Assegnato un numero pari maggiore di 4 esso è sempre somma di due numeri primi".

Per la congettura di Goldbach, quindi, ci interessano le rappresentazioni:

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

Dove p1, p2 sono numeri primi non necessariamente distinti, appartenenti all'insieme dei numeri primi P e per il momento non consideriamo n numero pari, ma qualsiasi (ad esempio accettiamo anche 2+3=5 in questa fase di investigazione). Ponendo:

$$V(\alpha) = V_N(\alpha) = \sum_{p \le N} e(p\alpha) \qquad (11)$$

Allora il problema di Goldbach, con le tecniche di analisi reale e complessa, si traduce per n $\leq$ N in:

$$\int_0^1 V(\alpha)^2 e(-n\alpha)d\alpha = \sum_{p_1 \le N}\sum_{p_2 \le N}\int_0^1 e((p_1 + p_2 - n)\alpha)d\alpha = r_2(n) \quad (12)([4])$$

Nel seguito anzicchè considerare direttamente la (12), si può considerare una versione pesata con peso diverso da 1 (anzicchè considerare p1+p2 consideriamo log(p1+p2)=logp1*logp2):

$$R_2(n) := \sum_{p_1+p_2=n} \log p_1 \log p_2 \quad (13)$$

E' chiaro che r2(n) è positiva se lo è anche R2(n); quindi è sufficiente studiare R2(n) per la congettura di Goldbach.

[4]Ricordiamo (vedi [2][3]) che comunque l'intervallo [0,1] (o il cerchio unitario quando si fa la trasformazione $x \to \exp(2\pi i x)$) nell'integrale della (12) andrebbe suddiviso in sotto-intervalli centrati su numeri razionali con denominatore q $\leq$Q dove Q = Q(N) è un parametro e la cosa viene detta *dissezione di Farey di ordine Q*. Ora gli intervalli corrispondenti ai numeri razionali con denominatore q$\leq$P, sono detti archi principali o maggiori mentre i rimanenti archi sono detti secondari o minori. In particolare P = P(N) è un altro parametro scelto in modo tale che il prodotto P*Q=N. Hardy e Littlewood osservarono in questo modo che V_N ha uno sviluppo asintotico su ogni arco principale che corrisponde ad un picco della funzione, per valori razionali con denominatore piccolo. Sfruttando il contributo di questi picchi e trascurando l'errore essi arrivarono anche alle formule per la costante dei numeri gemelli.

Una versione pesata della (11) adesso è:

$$S(\alpha) = S_N(\alpha) = \sum_{p \le N} \log p \; e(p\alpha) \qquad (14)$$

Tenendo presente il Teorema di Dirichlet sulle progressioni aritmetiche, scegliendo q, a tali che MCD(q,a)=1, scriviamo che

$$\theta(N;q,a) = \sum_{\substack{p \le N \\ p \equiv a \bmod q}} \log p \qquad (15)$$

Teorema di Siegel - Walfisz

Siano C,A>0 con q ed a relativamente primi tra loro, allora

$$\sum_{\substack{p \le N \\ p \equiv a \bmod q}} \log p = \frac{N}{\varphi(q)} + O(\frac{N}{\log^C N})$$

$$\text{per } q \le \log^A N$$

la costante precedente C non dipende da N, a, q (ma al più dipende da A: C(A)).

Quindi dal Teorema di Siegel – Walfisz (vedi [4]) ne consegue che:

$$\theta(N;q,a) = \frac{N}{\varphi(q)} + O(\frac{N}{\log^C N}) \qquad (16)$$

Dove possiamo chiamare $E(N;q,a) = O(\frac{N}{\log^C N}) = O(N \exp(-C(A)\sqrt{\log N}))$.

Dove φ è la funzione totiente di Eulero[5] e C non deve essere scelto molto grande. Il teorema è efficace quando q è molto piccolo rispetto ad N. A questo punto analogamente alla (12) possiamo scrivere che per n$\leq$N:

$$\int_0^1 S(\alpha)^2 e(-n\alpha) d\alpha \qquad (17)$$

Come operazione preliminare vediamo qualche valore di S (per l'esponenziale ricordate la trasformazione $x \to \exp(2\pi i x)$ quindi ad esempio a ½ si tratta di exp(2πi*1/2)=-1):

[5] la funzione totiente di Eulero φ(q) conta il numero degli interi h nell'intervallo [1,q] minori uguali ad q e tali che MCD(h,q)=1. Ad esempio φ(8)=4, perché se scriviamo 1,2,3,4,5,6,7,8 solo 1,3,5,7 sono tali che MCD(h,q)=1.

S(0) = $\theta(N,1,1)\approx N$

S(1/2) = $-\theta(N,1,1)+2\log 2\approx -N$

S(1/3) = $\exp(1/3)\,\theta(N,3,1) + \exp(2/3)\,\theta(N,3,2) + \log 3 \approx -\tfrac{1}{2} N$

S(1/4) = $\exp(1/4)\,\theta(N,4,1) + \exp(3/4)\,\theta(N,4,3) + \log 2 \approx 0$

Adesso vediamo S anche per qualche valore razionale a/q, quando $0 \le a \le q$ e MCD(a,q)=1. In tal caso la (14) diventa:

$$S(a/q) = \sum_{h=1}^{q} \sum_{\substack{p\le N \\ p\equiv h \bmod q}} \log p \; e(p\cdot a/q) =$$

$$= \sum_{h=1}^{q} e(h\cdot a/q) \sum_{\substack{p\le N \\ p\equiv h \bmod q}} \log p = \sum_{h=1}^{q} e(h\cdot a/q)\cdot\theta(N;q,a) = \sum_{h=1}^{q}{}^{*} e(h\cdot a/q)\cdot\theta(N;q,a) + O(\log q \log N) \quad (18)$$

L'asterisco nell'ultima sommatoria indica l'ulteriore condizione che MCD(h,q)=1.

Dalla (18) tenendo conto della (16) si ottiene:

$$S(a/q) = \frac{N}{\varphi(q)} \sum_{h=1}^{q}{}^{*} e(h\cdot a/q) + \sum_{h=1}^{q}{}^{*} e(h\cdot a/q)\cdot E(N;q,a) + O(\log q \log N)$$

$$= \frac{\mu(q)}{\varphi(q)} + \sum_{h=1}^{q}{}^{*} e(h\cdot a/q)\cdot E(N;q,a) + O(\log q \log N) \qquad (19)$$

Dove μ è la *funzione di Moebius*[6]. A causa della funzione di Moebius, $|S(\alpha)|$ è grande quando α è un numero razionale, in un intorno di a/q, e dagli esempi precedenti si è visto anche che S(a/q) decresce come 1/q.

Avendo capito come si comporta S, possiamo adesso tentare di trovare una espressione per $R_2(n)$ e lo strumento di solito usato è la "somma parziale sugli archi". L'obiettivo è di ottenere un errore piccolo, per cui occorre scegliere un numero di archi adatto a questo scopo. Vaughan dimostrò che l'errore dipende da $q(1+N|\alpha-a/q|)E(N;q,a)$.

Poniamo: $\alpha = \frac{a}{q} + \eta$, per $|\eta|$ piccolo si ottiene:

[6] $\mu(q)=0$ se q è divisibile per il quadrato di qualche numero primo, è $(-1)^k$ se $q=p_1p_2...p_k$ dove i p_i sono k numeri primi distinti.

$$S(a/q+\eta)=\frac{\mu(q)}{\varphi(q)}\sum_{m\le N}e(m\eta)\cdot E(N;q,a,\eta)=\frac{\mu(q)}{\varphi(q)}T(\eta)+E(N;q,a,\eta)$$

Dalla (16) e dalla (19) risulta:

$$E(N;q,a,\eta)=O_A(q(1+N\,|\,\eta\,|)N\exp(-C(A)\sqrt{\log N}))$$

Questo ci fa comprendere che non possiamo prendere troppi archi principali o archi troppo ampi o q molto grandi altrimenti l'errore non è piccolo. L'errore e gli archi dipendono, quindi, dalla scelta di q ed a.

Se come in [3] indichiamo con $\mathfrak{M}(\mathrm{q,a}):=(\frac{a}{q}-\xi(q,a),\frac{a}{q}+\xi'(q,a))$ l'arco di Farey relativo al numero razionale a/q, con $\xi(q,a)$ e $\xi'(q,a)$ di ordine $(qQ)^{-1}$, allora definiamo l'insieme o l'unione degli *archi maggiori* e *minori* nel seguente modo:

$$\mathfrak{M}:=\bigcup_{q\le P}\bigcup_{a=1}^{q}{}^{*}\mathfrak{M}(q,a)\qquad \mathrm{m}:=\left[\xi(1,1),1+\xi(1,1)\right]\setminus\mathfrak{M}\quad(20)$$

Anche qui l'asterisco indica la condizione aggiuntiva che il MCD(q,a)=1. Per l'intervallo dell'arco minore anzicchè considerare [0,1] si è traslato a $\left[\xi(1,1),1+\xi(1,1)\right]$, cosa possibile vista la periodicità 1.

E' chiaro che, ripartendo dalla (17), adesso $R_2(n)$ è somma di due integrali, uno sull'arco maggiore e l'altro sull'arco minore (come abbiamo detto quando abbiamo esaminato la (12)) e per $n\le N$ è:

$$R_2(n)=\int_0^1 S(\alpha)^2e(-n\alpha)d\alpha=(\int_{\mathfrak{M}}+\int_{\mathfrak{m}})S(\alpha)^2e(-n\alpha)d\alpha=$$

Da come abbiamo definito gli archi maggiori nella (20) è quindi

$$R_2(n)=\sum_{q\le P}\sum_{a=1}^{q}{}^{*}\int_{-\xi(q,a)}^{\xi'(q,a)}S(\frac{a}{q}+\eta)^2e(-n(\frac{a}{q}+\eta))d\eta+\int_{\mathfrak{m}}S(\alpha)^2e(-n\alpha)d\alpha=R_{\mathfrak{M}}(n)+R_m(n)\quad(21)$$

Nel seguito col simbolo $\approx$ intenderemo come in [3] una uguaglianza asintotica (all'infinito) che, attualmente, per il problema di cui discutiamo nella pratica è riscontrata ma matematicamente non è stata ancora dimostrata rigorosamente.

La (21) si può riscrivere ancora nel seguente modo:

$$R_{\mathfrak{M}}(n)\approx\sum_{q\le P}\sum_{a=1}^{q}{}^{*}\int_{-\xi(q,a)}^{\xi'(q,a)}\frac{\mu(q)^2}{\varphi(q)^2}T(\eta)^2e(-n(\frac{a}{q}+\eta))d\eta=$$

$$= \sum_{q \le P} \frac{\mu(q)^2}{\varphi(q)^2} \sum_{a=1}^{q}{}^{*} e(-n\frac{a}{q}) \int_{-\xi(q,a)}^{\xi'(q,a)} T(\eta)^2 e(-n\eta) d\eta \quad (22)$$

Se l'integrale che contiene T lo estendiamo in tutto l'intervallo [0,1]

$$\int_0^1 T(\eta)^2 e(-n\eta) d\eta = \sum_{m1+m2=n} 1 = n-1 \approx n \quad (23)$$

Per cui otteniamo:

$$R_{\mathfrak{M}}(n) \approx n \sum_{q \le P} \frac{\mu(q)^2}{\varphi(q)^2} \sum_{a=1}^{q}{}^{*} e(-n\frac{a}{q}) \qquad (24)$$

Dove la somma interna è detta la *somma di Ramanujan* e si dimostra con un Teorema che è esprimibile in funzione di μ e di φ:

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

Se estende la somma a $q \geq 1$ e tenendo conto di un altro Teorema (vedi [3]) si arriva a:

$$R_2(n) \approx n \sum_{q \ge 1} \frac{\mu(q)^2}{\varphi(q)} \frac{\mu(\frac{q}{(q,n)})}{\varphi(\frac{q}{(q,n)})} = n \prod_p (1 + f_n(p)) \quad (25)$$

Il produttorio è su tutti i numeri primi; inoltre è:

$$f_n(p) = \frac{\mu(q)^2}{\varphi(q)} \frac{\mu(\frac{q}{(q,n)})}{\varphi(\frac{q}{(q,n)})} = \begin{cases} \frac{1}{p-1} & \text{se p|n} \\ -\frac{1}{(p-1)^2} & \text{altrimenti} \end{cases}$$

Se n è dispari allora $1 + f_n(2) = 0$ per cui la (23) afferma che non ci sono coppie di Goldbach per n.

Infatti R2(n)=0 se n-2 non è primo, R2(n)=2log(n-2) se n-2 è un numero primo. Se, invece n è pari possiamo ottenere una espressione

$$R_2(n) \approx n\prod_{p|n}(1+\frac{1}{p-1})\prod_{p\nmid n}(1-\frac{1}{(p-1)^2})$$

$$R_2(n) \approx 2n\prod_{\substack{p|n\\ p>2}}(\frac{p}{p-1}\cdot\frac{(p-1)^2}{p(p-2)})\prod_{p>2}(1-\frac{1}{(p-1)^2}) = C_o n\prod_{\substack{p|n\\ p>2}}(\frac{p-1}{p-2}) \quad (26)$$

Dove C_0 è la costante dei numeri gemelli. La (26) è la formula asintotica per $R_2(n)$ basata sulla Teoria dei numeri e fornisce un valore maggiore di $r_2(n)$ di una quantità $(\log n)^2$, a causa dei pesi logp1logp2.

I problemi ancora in gioco del Metodo del cerchio

Tutto il procedimento del metodo del cerchio non assicura che il numero di coppie di Goldbach non può essere mai nullo, ma dà una stima del numero di coppie asintotiche, abbastanza buono.

Nelle formule precedenti (22)(23) si sono fatte delle approssimazioni tenendo conto che T decade rapidamente dai valori interi a quelli razionali. Anche l'approssimazione di θ per le progressioni aritmetiche non è abbastanza efficace, ma anche se si trovasse un procedimento più convincente, riducendo l'errore e migliorando la scelta degli archi non sembra che si riesca lo stesso a dimostrare la congettura di Goldbach. Nel procedimento precedente inoltre non si riesce ancora a stimare bene il contributo degli archi inferiori.

I dubbi sulla congettura di Goldbach

Sappiamo che i numeri primi si rarefanno quando si prosegue verso l'infinito. Si dice che esistono "intervalli rarefatti", intervalli cioè abbastanza ampi dove non si trova un numero primo.

Sappiamo anche che la funzione che rappresenta il numero di coppie di Goldbach (corrispondente a $r_2(n)$) oscilla parecchio, cioè non è una funzione monotona crescente.

Qualsiasi metodo finora preso in considerazione dagli studiosi non è stato in grado di escludere che la funzione di conteggio delle coppie di Goldbach non si annulla mai.

Adesso supponiamo che i1 sia un intero dispari, ad esempio dell'ordine di grandezza di 100^100^10000, ovvero qualcosa come un 1 seguito da cento milioni di zeri. Attualmente anche un computer è in difficoltà con numeri del genere, figuriamoci se devono cercare i contro-esempi alla congettura.

Supponiamo che n sia un numero pari tale che n=i1+3, ma essendo i1 dispari e non numero primo, se n è ottenibile come somma dalla sola coppia di numeri i1+3, allora la congettura di Goldbach

sarebbe falsa; o per lo meno sarebbe vera solo fino ad un limite superiore di N o fino ad un numero minore di X = n.

Questo dubbio fa parte anche del lavoro di *Montgomery* e Vaughan (Vedi [5]). Se viene indicato con E(X) l'insieme dei numeri pari minori di X che non possono essere scritti come somma di due numeri primi, Vaughan ha prima mostrato prima che:

$$E(X) < X \exp(-c \log^{1/2} X)$$

Poi ulteriormente Montgomery e Vaughan hanno dimostrato un Teorema ([5]), per cui "esiste un δ positivo e piccolo tale che per grandi valori di X è:

$$E(X) < X^{1-\delta}"$$

Conclusioni

La dimostrazione di Montgomery e Vaughan è basata anch'essa sulla tecnica del Metodo del cerchio ([5]). Il Teorema di sopra è l'unico grande risultato, espresso qualitativamente dal punto di vista teorico, da tale metodo e che attualmente mette in dubbio la congettura di Goldbach. Si suppone però un X molto grande. Attualmente è impossibile per i computer quantificare un valore di numero pari, con X molto grande, per cui non sia vera la congettura di Goldbach (e probabilmente nemmeno un uomo sarebbe capace di leggere un numero del genere), né credo sia possibile inventare ulteriori metodi analitici, di solito qualitativi, che possono quantificare un numero pari per cui non sia vera la congettura di Goldbach (è la stessa differenza che esiste tra il concetto di misura e di forma chiusa).

Riferimenti

[1] R.C. Vaughan The Hardy{Littlewood Method, 2a ed., Cambridge U. P., Cambridge, 1997.

[2] A. Zaccagnini –Variazioni Goldbach: Problemi con Numeri primi

[3] A. Zaccagnini – Perché il problema di Goldbach è difficile

[4] Steven J. Miller, Ramin Takloo-Bighash – The Circle Method

[5] The exceptional set in Goldbach's problema – H.L.Montgomery, R.C.Vaughan

I Riferimenti [2][3][4][5] sono reperibili su INTERNET.

Letture divulgative

[6] A. Doxiadis, *Zio Petros e la congettura di Goldbach*, Bompiani, 2001