Dispense del corso
Teoria Analitica dei Numeri B

Riccardo Zanotto

7 ottobre 2019

Indice

Capitolo 1

Introduzione

In questo corso tratteremo prevalentemente la teoria analitica additiva; in particolare useremo il metodo del cerchio di Hardy-Littlewood per approcciarci ai seguenti problemi:

- problema di Waring
- problema di Goldbach
- problema di Erdos, Roth, Szemeredi

1.1 Il problema di Erdos

L'ultimo problema è stato proposto da Erdos nella seguente forma:

Congettura 1.1.1 (Erdos). *Sia $E \subset \mathbb{N}$ un insieme tale che $\overline{d}(E) = \limsup_{N\to\infty} \frac{\#E\cap[1,N]}{N} > 0$. Allora esistono tre elementi di E in progressione aritmetica.*

Il problema in questa forma venne risolto da Roth nel 1953; in seguito venne mostrato il seguente

Teorema 1.1.2 (Szemeredi, 1975). *Sia $E \subset \mathbb{N}$ un insieme tale che $\overline{d}(E) > 0$. Allora esistono segmenti di progressioni aritmetiche arbitrariamente lunghi.*

Negli ultimi anni si è arrivati anche al seguente risultato

Teorema 1.1.3 (Green e Tao, 2004). *L'insieme dei numeri primi contiene progressioni aritmetiche arbitrariamente lunghe*

1.2 Il problema di Waring

Un risultato molto importante nella teoria elementare dei numeri è il famoso "teorema dei quattro quadrati", ovvero

Teorema 1.2.1 (Lagrange, 1770)**.** *Ogni intero positivo si può scrivere come somma di al più quattro quadrati.*

Nello stesso anno, Waring propose la seguente generalizzazione:

Congettura 1.2.2 (Waring, 1770)**.** *Ogni intero positivo si scrive come somma di al più 9 cubi, 19 potenze quarte, e così via...*

Questa frase ci porta a definire il nostro oggetto di studio:

Definizione 1.2.3. Fissato k, sia $g(k)$ il minimo intero (eventualmente infinito) tale che ogni $n \in \mathbb{N}$ si può scrivere come somma di $g(k)$ potenze k-esime.

Uno dei primi risultati su $g(k)$ è un bound dal basso:

Proposizione 1.2.4 (Eulero)**.** $g(k) \geq 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2$

Dimostrazione. Sia $n_k = 2^k \cdot \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1$; si vede facilmente che $n_k < 3^k$. Quindi per scriverlo come somma di potenze k-esime possiamo usare solamente $1^k, 2^k$.
Tuttavia $2^k \cdot \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor > n_k$, perciò possiamo usare al più $\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1$ volte il 2^k.
Rimane poi $n_k - 2^k \cdot \left(\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 \right) = 2^k - 1$, per cui possiamo usare solo gli 1^k, e ce ne servono $2^k - 1$.
Sommando le due quantità otteniamo ul bound cercato. □

Osservazione. Sebbene questo sembri un bound banale, in realtà è molto forte: se calcoliamo il valore del bound per $2, 3, 4$ otteniamo $4, 9, 19$ che sono esattamente i valori congetturati da Waring.

Nell'ultimo secolo si è infatti dimostrato che

Teorema 1.2.5 (Mahler, 1957)**.** $g(k) = 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2$*, tranne al più un numero finito di k.*

Un importante risultato di inizio secolo è il seguente

Teorema 1.2.6 (Hilbert, 1909)**.** *Il numero $g(k)$ esiste finito per ogni intero k.*

Dato che lo studio di $g(k)$ è quasi completamente risolto, si è iniziata a studiare un'altra quantità

Definizione 1.2.7. Si indica con $G(k)$ il minimo intero s tale che ogni intero sufficientemente grande è scrivibile come somma di s potenze k-esime.

Osservazione. Vale ovviamente $G(k) \leq g(k)$ e quindi anche $G(k)$ è finito $\forall k$.

Lo studio di questa funzione è molto più difficile di quello di $g(k)$. Alcuni dei risultati che si hanno sono

Teorema 1.2.8 (Davenport, 1939)**.** $G(4) = 16$

Teorema 1.2.9 (Vaughan e Wooley)**.** $G(k) \leq k \log k + k \log\log k + Ck$

1.3 Il problema di Goldbach

Questo è uno dei problemi più famosi della matematica, data la semplicità dell'enunciato:

Congettura 1.3.1 (Goldbach, 1742)**.**

- *Forma forte: Ogni intero pari è esprimibile come somma di due primi.*
- *Forma debole: Ogni intero è scrivibile come somma di al più tre primi.*

Un risultato parziale è il seguente

Teorema 1.3.2 (Helfgott, 2013)**.** *Ogni intero dispari $n \geq 7$ si scrive come somma di tre primi dispari.*

Ci sono metodi "probabilistici" per vedere che asintoticamente molti numeri soddisfano la congettura.
Ad esempio, Hardy e Littlewood dimostrarono che il numero di rappresentazioni come somma di k primi è asintotico a $c_k \frac{n^2}{\log^3 n}$; tuttavia $c_2 = 0$, quindi la parte principale è un'altra. Abbiamo poi il seguente

Teorema 1.3.3. *Ogni intero positivo, tranne al più un insieme E, è somma di 2 primi; con $E \cap [1, N] = O\left(\frac{N}{\log^\alpha N}\right)$ per ogni α.*

Un'altra strada è attraverso metodi di crivello, giungendo a risultati del tipo

Teorema 1.3.4 (Chen, 1973)**.** *Ogni intero positivo sufficientemente grande è somma di un primo e di un semiprimo (ovvero di un prodotto di al più due primi).*

1.4 Il metodo di Hardy-Littlewood

Sia a_m una successione crescente di interi; siamo interessati a studiare il comportamento della quantità $R_s(n)$ che è il numero di rappresentazioni di n come somma di s termini della successione.
Introduciamo allora la serie di potenze $F(z) = \sum_{m \geq 0} z^{a_m}$. Vale allora

$$F^s(z) = \sum_{n \geq 0} z^n \cdot R_s(n)$$

Dato che F è olomorfa in $|z| < 1$, possiamo usare il teorema di Cauchy per ottenere

$$R_s(n) = \oint_{|z|=\rho} \frac{F^s(z)}{z^{n+1}} dz$$

Notazione. Definiamo $e(\alpha) = e^{2\pi i \alpha}$. Diciamo che $f \ll g$ se $f = O(g)$.

Una variante del metodo, che permette di integrare sul cerchio unitario, si ottiene considerando somme parziali del tipo $S(\alpha) = \sum_{m \leq N} e(\alpha a_m)$ in modo da ottenere

$$S^s(\alpha) = \sum_{m \leq N \cdot s} R_s(m, N) e(\alpha m)$$

dove $R_s(m, n)$ indica il numero di modi di scrivere m come somma di s elementi della successione, ognuno $\leq N$.
Usando allora l'ortogonalità delle funzioni $e(\alpha k)$, possiamo ricavare che

$$R_s(m, N) = \int_0^1 S^s(\alpha) e(-\alpha m) d\alpha$$

Capitolo 2

Il problema di Goldbach

Approcciamo ora le congetture di Goldbach, dimostrandone una forma debole.

2.1 Richiami sui numeri primi

Ci serviranno alcuni risultati classici, stile PNT.

Definizione 2.1.1. La funzione Λ di von Mangoldt è data da

$$\Lambda(n) = \begin{cases} \log p & \text{se } n = p^a \\ 0 & \text{altrimenti} \end{cases}$$

Sia poi $\psi(x) = \sum_{n \leq x} \Lambda(n)$ la funzione ψ di Chebycheff.
Infine definiamo la θ di Chebycheff: $\theta(x) = \sum_{p \leq x} \log p$ dove la somma è fatta sui primi.

Proposizione 2.1.2. *Si verificano facilmente le seguenti proprietà:*

- $e^{\psi(N)} = mcm(1, 2, \ldots, N)$.
- $\psi(x) = \sum_{i=1}^{\lfloor \log_2(x) \rfloor} \theta(x^{1/i})$.

Un teorema classico è il seguente

Teorema 2.1.3. $x \ll \psi(x), \theta(x) \ll x$.

che raffinato diventa il teorema dei numeri primi

Teorema 2.1.4 (PNT). $\psi(x) \sim \theta(x) \sim x$.

2.2 Il teorema di Vinogradov

L'oggetto di studio di questa sezione è la seguente funzione

Definizione 2.2.1. Dato $N \geq 2$, sia $r(N) = \displaystyle\sum_{k_1+k_2+k_3=N} \Lambda(k_1) \cdot \Lambda(k_2) \cdot \Lambda(k_3)$

L'obiettivo finale sarà dimostrare il

Teorema 2.2.2 (Vinogradov, 1930). *Per ogni $A > 0$ vale*

$$r(N) = \frac{1}{2}\sigma(N) \cdot N^2 + O\left(\frac{N^2}{(\log N)^A}\right)$$

dove $\sigma(N) = \displaystyle\prod_{p|N} \left(1 - \frac{1}{(p-1)^2}\right) \cdot \prod_{p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right)$

Osservazione. Se N è pari, allora $\sigma(N) = 0$, quindi la parte principale svanisce e occorre studiare meglio il resto.

Vediamo intanto come il teorema risolve la congettura di Goldbach sui dispari.
Detta $r^*(N) = \sum_{p_1+p_2+p_3=N} \log(p_1)\log(p_2)\log(p_3)$, si può vedere che è molto vicina lla $r(N)$ che stiamo studiando.
Infatti, consideriamo i termini di $r(N)$ in cui almeno un k_i (diciamo k_1) è una potenza di un primo con esponente almeno 2; ma allora deve essere $k_1 \leq \sqrt{N}$ e quindi si ricava $r(N) - r^*(N) \leq \sum_{k_1 \leq \sqrt{N}} \Lambda(k_1) \cdot \sum_{k_2+k_3 \leq N} \Lambda(k_2)\Lambda(k_3)$.
Il primo fattore è esattamente $\psi(\sqrt{N})$, che per il PNT è $\ll \sqrt{N}$; il secondo fattore può essere maggiorato con $\sum_{k_2 \leq N} \Lambda(k_2) \cdot \log N$, ovvero $\psi(N) \log N$ che di nuovo è $\ll N \log N$.
Concludiamo cioè che $r(N) = r^*(N) + O(N^{3/2} \log N)$.
Abbiamo allora il

Corollario 2.2.3. *Ogni intero dispari N sufficientemente grande è somma di 3 primi in almeno $c\dfrac{N^2}{\log^3 N}$ modi, con $c > 0$.*

Dimostrazione. Per il teorema di Vinogradov e la stima appena vista, la parte principale di $r^*(N)$ è cN^2.
Inoltre $r^*(N) = \displaystyle\sum_{p_1+p_2+p_3=N} \log(p_1)\log(p_2)\log(p_3) \leq \sum_{p_1+p_2+p_3=N} \log^3(N)$, cioè il numero di modi di scrivere N come somma di 3 primi è almeno $\frac{r^*(N)}{\log^3(N)}$. □

Per la dimostrazione del teorema di Vinogradov ci serviranno un po' di lemmi.

L'idea comunque è di considerare la funzione $S(\alpha, N) = \sum_{k \leq N} \Lambda(k) e(\alpha k)$, da cui $S^3(\alpha, N) = \sum_{l \leq 3N} e(\alpha l) r(l, N)$.
Quindi per inversione di Fourier possiamo scrivere

$$r(N) = \int_0^1 S^3(\alpha, N) e(-\alpha N) d\alpha$$

Dividiamo in archi principali e secondari...