

Indice

Introduzione	IV
1 Richiami di Teoria Analitica dei Numeri	1
1.1 Funzioni Aritmetiche	1
1.1.1 Funzioni Aritmetiche e Prodotto di Dirichlet	1
1.1.2 Identità fondamentali : funzioni μ, ϕ, Λ	3
1.1.3 Serie di Dirichlet.	5
1.1.4 Prodotti di Eulero.	9
1.2 Funzione ζ di Riemann	11
1.2.1 Funzione ζ di Riemann	11
1.2.2 Equazione Funzionale della ζ	13
1.2.3 Ipotesi di Riemann	15
1.2.4 Regioni Zero-free	16
1.2.5 Stime di Densità degli Zeri	17
1.3 Funzioni L di Dirichlet	19
1.3.1 Funzioni L di Dirichlet	19
1.3.2 Equazione Funzionale delle L	19
1.3.3 Ipotesi di Riemann Generalizzata e Teorema di Siegel	21
1.3.4 Regioni Zero-free	21
1.3.5 Stime di Densità degli Zeri	22
1.4 Formule Esplicite	23
1.4.1 Formula di Perron	23
1.4.2 Formula Esplicita di Riemann – von Mangoldt	23
1.4.3 Formula Esplicita Classica per $\psi(x, \chi)$	24
2 Problemi Moltiplicativi	27
2.1 Problemi Moltiplicativi	27
2.2 Teorema dei Numeri Primi	29
2.2.1 Funzione π e stime di Cebecev	29
2.2.2 Funzioni ψ e θ di Cebecev	30
2.2.3 Teorema dei Numeri Primi	32

2.3	Primi negli Intervalli Corti	36
2.4	Primi nelle Progressioni Aritmetiche	38
2.4.1	Progressioni aritmetiche e Caratteri Additivi	38
2.4.2	Caratteri Moltiplicativi e Teorema di Dirichlet	38
2.4.3	Teorema dei Numeri Primi nelle Progressioni	42
2.5	Teorema di Bombieri	43
3	Problemi Additivi	45
3.1	Problemi Additivi	45
3.2	Problemi di Goldbach	47
3.3	Metodo di Hardy-Littlewood	49
3.4	Metodo di Vinogradov	51
3.5	Teorema dei tre primi	52
3.6	Metodo del Cerchio e Problema di Goldbach	56
4	Crivello e Somme Esponenziali	59
4.1	Crivello e Somme Esponenziali	59
4.2	Crivello Piccolo	61
4.2.1	Crivello di Eratostene-Legendre	61
4.2.2	Crivello Combinatorio	67
4.2.3	Crivello di Selberg	70
4.3	Crivello Largo	73
4.4	Metodo della Dispersione	76
4.5	Somme Esponenziali	78
4.6	Forme Bilineari	79
4.7	Somme di Kloosterman	80
5	Problemi in Intervalli Corti	81
5.1	Problemi in Intervalli Corti	81
5.2	Primi in quasi tutti gli Intervalli Corti	83
5.2.1	Introduzione ed enunciato dei risultati	83
5.2.2	Enunciato e dimostrazione del Lemma 1	87
5.3	Problema di Goldbach con primi quasi uguali	90
5.3.1	Notazioni	92
5.3.2	Sketch del metodo di dimostrazione	93
5.3.3	Stime sugli archi maggiori	93
5.3.4	Stime sugli archi minori	95
5.4	Crivello Largo ed $n(n+2)$ in Intervalli Corti	98
5.4.1	Enunciato dei risultati	98
5.4.2	Dimostrazione del Teorema e dei Corollari	100
5.4.3	Una variante del Crivello Largo	103
5.5	Dispersione ed $n(n+2)$ in Intervalli Corti	106

5.5.1	Enunciato dei risultati	106
5.5.2	Dimostrazione del Teorema	107
5.6	Somme di Kloosterman ed $n(n + 2)$ in Intervalli Corti . . .	111
5.6.1	Enunciato dei risultati	111
5.6.2	Stime sulle parti frazionarie tramite somme di Kloosterman	112

Introduzione

La tesi introduce i principali risultati dell' Autore riguardo problemi moltiplicativi e additivi in intervalli corti, nell' ambito delle problematiche della Teoria Analitica dei Numeri.

Nel **Capitolo 1** si richiamano i principali **risultati “classici”** di Teoria Analitica dei Numeri (abbrev. **T.A.N.**), **riguardo** : le **funzioni aritmetiche**, le **serie di Dirichlet**, i **prodotti di Eulero**, la **funzione ζ di Riemann** e le **funzioni L di Dirichlet**.

Nel **Capitolo 2** viene data una breve rassegna dei **principali problemi moltiplicativi** (ovvero i problemi aritmetici che riguardano la struttura moltiplicativa degli interi) e in particolare il problema della **distribuzione dei numeri primi** (in particolare, anche nelle progressioni aritmetiche).

Nel **Capitolo 3** vengono esposti i **principali problemi additivi** (ovvero i problemi aritmetici che riguardano la struttura additiva degli interi) ed in particolare i **problemi di Goldbach** e una delle principali tecniche utilizzate per il trattamento di tali problemi, detta **Metodo del Cerchio**.

Nel **Capitolo 4** vengono presentati i **Metodi di Crivello**, le **Somme Esponenziali** e le **Forme Bilineari** che, fra le tecniche “moderne” (ovvero di questo secolo), sono fra le più avanzate in T.A.N.

Nel **Capitolo 5**, infine, vengono dati i **risultati originali ottenuti su particolari problemi moltiplicativi e additivi negli intervalli corti**, ovvero in cui il range dei valori considerati é di ordine di grandezza inferiore rispetto a tali valori. In particolare:

- **per i problemi moltiplicativi** si sono ottenuti risultati circa i **primi “in quasi tutti gli intervalli corti”** e la **distribuzione di $n(n+2)$ nelle progressioni aritmetiche negli intervalli corti**;

- **per i problemi additivi** si sono ottenuti risultati circa il **problema di Goldbach binario con primi “quasi uguali”**, ovvero con due primi in un intervallo corto.

Capitolo 1

Richiami di Teoria Analitica dei Numeri

1.1 Funzioni Aritmetiche

1.1.1 Funzioni Aritmetiche e Prodotto di Dirichlet

Si definisce **funzione aritmetica** una funzione $f : \mathbf{N} \rightarrow \mathbf{C}$; l'insieme \mathcal{A} delle funzioni aritmetiche, dotato delle operazioni:

$$+ : (f, g) \in \mathcal{A} \times \mathcal{A} \rightarrow f + g \in \mathcal{A}, \quad (f + g)(n) \stackrel{def}{=} f(n) + g(n) \quad \forall n \in \mathbf{N}$$

(somma)

$$\cdot : (\lambda, f) \in \mathbf{C} \times \mathcal{A} \rightarrow \lambda f \in \mathcal{A}, \quad (\lambda f)(n) \stackrel{def}{=} \lambda f(n) \quad \forall n \in \mathbf{N}$$

(prodotto per scalari)

$$* : (f, g) \in \mathcal{A} \times \mathcal{A} \rightarrow f * g \in \mathcal{A}, \quad (f * g)(n) \stackrel{def}{=} \sum_{d|n} f(d)g\left(\frac{n}{d}\right) \quad \forall n \in \mathbf{N}$$

(prodotto di Dirichlet)

é un' algebra commutativa su \mathbf{C} , il cui elemento neutro é dato dalla funzione $\mathbf{e} : \mathbf{N} \rightarrow \mathbf{C}$, definita da

$$\mathbf{e}(n) \stackrel{def}{=} \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } n > 1. \end{cases}$$

Si dice che $f \in \mathcal{A}$ é **multiplicativa** se:

$$f(mn) = f(m)f(n) \quad \forall m, n \in \mathbf{N} \quad \text{tali che} \quad (m, n) = 1,$$

mentre é detta **completamente moltiplicativa** quando:

$$f(mn) = f(m)f(n) \quad \forall m, n \in \mathbf{N}.$$

Segue dalle definizioni che le funzioni moltiplicative sono individuate dai loro valori sulle potenze dei primi, mentre per le f completamente moltiplicative basta conoscere $f(p)$, per ogni p primo.

Il prodotto di Dirichlet (detto anche **prodotto di convoluzione**), le funzioni moltiplicative e le completamente moltiplicative hanno un ruolo essenziale nella teoria delle serie di Dirichlet e dei prodotti di Eulero, come sar  chiaro in seguito.

Denotiamo con \mathcal{M} l'insieme delle funzioni moltiplicative e con \mathcal{U} l'insieme delle unit , ovvero degli **elementi invertibili** in \mathcal{A} **rispetto al prodotto di Dirichlet**.

Le $f \in \mathcal{U}$ sono caratterizzate dalla condizione: " $f(1)$ non si annulla" ed   facile dimostrare il:

TEOREMA 1.1. \mathcal{M}   un sottogruppo di \mathcal{U} (rispetto a $*$).

Da esso segue che il prodotto di Dirichlet di due funzioni moltiplicative   anch'esso moltiplicativo (mentre, in generale, $f * g$ **non   completamente moltiplicativa** quando f e g lo sono).

Un'altra notevole propriet  delle funzioni moltiplicative   data dal:

TEOREMA 1.2. Se f   moltiplicativa allora:

$$f \text{   completamente moltiplicativa} \Leftrightarrow f^{-1}(n) = \mu(n)f(n) \quad \forall n \in \mathbf{N}$$

(f^{-1} sta per l'inverso di f rispetto a $*$).

Una funzione $f \in \mathcal{A}$ si dice **additiva** quando:

$$f(mn) = f(m) + f(n) \quad \text{se} \quad (m, n) = 1,$$

mentre si dice **completamente additiva** quando:

$$f(mn) = f(m) + f(n) \quad \forall m, n \in \mathbf{N}.$$

In entrambi gli ultimi due casi f é una funzione aritmetica non invertibile, dato che $f(1) = 0$ (come si verifica immediatamente dalle definizioni).

Se definiamo il **prodotto ordinario** fra funzioni in \mathcal{A} :

$$(fg)(n) \stackrel{def}{=} f(n)g(n) \quad \forall n \in N$$

abbiamo che, per h completamente additiva, l' applicazione $f \rightarrow hf$ é una derivazione nell' algebra \mathcal{A} .

In particolare possiamo scegliere $h(n) = -\log(n)$ (ovvero $h = \mathbf{L}$, v. §1.1.3).

1.1.2 Identità fondamentali : funzioni μ, ϕ, Λ .

Definiamo $\mu \in \mathcal{A}$, la **funzione di Möbius**:

$$\mu(n) \stackrel{def}{=} \begin{cases} 1 & \text{se } n = 1 \\ (-1)^r & \text{se } n \text{ é il prodotto di } r \text{ primi distinti,} \\ 0 & \text{altrimenti,} \end{cases}$$

che é chiaramente moltiplicativa (ma non completamente moltiplicativa) e per la quale vale l' identità:

$$(1.1) \quad \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } n > 1, \end{cases}$$

che, definendo la **funzione costante uno**:

$$\mathbf{1}(n) \stackrel{def}{=} 1 \quad \forall n \in \mathbf{N},$$

può essere espressa dicendo che μ é l' inversa (rispetto a $*$) di $\mathbf{1}$:

$$(1.2) \quad \mu * \mathbf{1} = \mathbf{e}.$$

Grazie a quest' ultima possiamo ottenere la:

FORMULA DI INVERSIONE DI MÖBIUS. Se $f, g \in \mathcal{A}$ allora:

$$f(n) = \sum_{d|n} g(d) \quad \forall n \in \mathbf{N} \quad \Leftrightarrow \quad g(n) = \sum_{d|n} f(d) \mu\left(\frac{n}{d}\right) \quad \forall n \in \mathbf{N},$$

ovvero :

$$f = g * \mathbf{1} \quad \Leftrightarrow \quad g = f * \mu.$$

(La dimostrazione segue immediatamente dalla 1.2).

Definiamo, ora, la **funzione ϕ di Eulero**:

$$\phi(n) \stackrel{def}{=} \sum_{\substack{k \leq n \\ (k,n)=1}} 1$$

e la **funzione identica**:

$$\mathbf{I}(n) \stackrel{def}{=} n, \quad \forall n \in \mathbf{N},$$

che hanno la proprietà:

$$(1.3) \quad \phi = \mu * \mathbf{I};$$

infatti $\mu, I \in \mathcal{M}$ e per il teorema 1.1 ϕ é moltiplicativa; quindi sarà individuata da $\phi(p^\alpha)$, per $\alpha \geq 0$; $\phi(1) = 1$ e (**\mathbf{P} é l'insieme dei primi**):

$$(1.4) \quad \phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right) \quad \forall p \in \mathbf{P} \quad \forall \alpha \in \mathbf{N},$$

da cui si ha (il prodotto é su tutti i divisori primi di n):

$$(1.5) \quad \phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \quad \forall n \in \mathbf{N}.$$

Dalla 1.3, moltiplicando (tramite $*$) ambo i membri per $\mathbf{1}$, si ha anche :

$$(1.6) \quad \sum_{d|n} \phi(d) = n \quad \forall n \in \mathbf{N}.$$

Vale inoltre la seguente proprietà delle funzioni moltiplicative

PROPOSIZIONE 1.1. Sia $f \in \mathcal{M}$. Allora

$$\sum_{d|n} \mu(d)f(d) = \prod_{p|n} (1 - f(p)) \quad \forall n \in \mathbf{N}.$$

Una funzione aritmetica molto importante in T.A.N. é la **funzione Λ di von Mangoldt** :

$$\Lambda(n) \stackrel{def}{=} \begin{cases} \log p & \text{se } n = p^\alpha, \text{ per qualche } \alpha \in \mathbf{N}, \\ 0 & \text{altrimenti.} \end{cases}$$

che nel prossimo §2.2.2 si dimostrerà un' ottima sostituta della funzione caratteristica dei primi; essa ha inoltre la notevole proprietà:

$$(1.7) \quad \Lambda * \mathbf{1} = \mathbf{L},$$

dove "L" é l' usuale funzione logaritmo in base naturale, ma con dominio ristretto ad \mathbf{N} (così che $\mathbf{L} \in \mathcal{A}$); ovvero:

$$(1.8) \quad \sum_{d|n} \Lambda(d) = \log(n) \quad \forall n \in \mathbf{N}.$$

La 1.8 é l' anello di congiunzione fra la funzione Λ di von Mangoldt e la funzione ζ di Riemann; ovvero é il motivo per il quale si può indagare la distribuzione dei primi studiando le proprietà di tale funzione, in particolare la distribuzione dei suoi zeri.

1.1.3 Serie di Dirichlet.

Definiamo la **serie di Dirichlet** (abbrev. **s.d.D.**) di coefficienti $a(n)$, con $a \in \mathcal{A}$ (f sarà la sua funzione somma, quando la serie converge):

$$(1.9) \quad f(s) \stackrel{def}{=} \sum_{n=1}^{\infty} a(n)n^{-s}, \quad s \in \mathbf{C}.$$

Scriveremo, nel seguito, $s = \sigma + it$, con σ e t reali, usando una notazione che é divenuta standard dopo i contributi di Riemann alla T.A.N.

Occupiamoci dapprima dei problemi di convergenza della serie di cui alla 1.9.

Si può facilmente dimostrare il:

TEOREMA 1.3. Se $\sum_{n=1}^{\infty} a(n)n^{-s}$ converge per $s_0 = \sigma_0 + it_0$, allora:

i) $\sum_{n=1}^{\infty} a(n)n^{-s}$ converge $\forall s \in \mathbf{C}$ tale che $\sigma > \sigma_0$;

ii) $\sum_{n=1}^{\infty} a(n)n^{-s}$ converge uniformemente in ogni compatto del semipiano $\sigma > \sigma_0$.

Grazie al teorema 1.3 possiamo definire l' **ascissa di convergenza** di una serie di Dirichlet :

$$\sigma_c \left(\sum_{n=1}^{\infty} a(n)n^{-s} \right) \stackrel{def}{=} \inf \left\{ \sigma \in \mathbf{R} : s = \sigma + it, \sum_{n=1}^{\infty} a(n)n^{-s} \text{ converge} \right\}$$

e, considerando la serie $\sum_{n=1}^{\infty} |a(n)n^{-s}|$ nello stesso teorema, l' **ascissa di convergenza assoluta** di una s.d.D.:

$$\sigma_{ac} \left(\sum_{n=1}^{\infty} a(n)n^{-s} \right) \stackrel{def}{=} \inf \left\{ \sigma \in \mathbf{R} : s = \sigma + it, \sum_{n=1}^{\infty} |a(n)n^{-s}| \text{ converge} \right\}.$$

Dalle definizioni si ha immediatamente (per ogni s.d.D.):

$$(1.10) \quad \sigma_{ac} \geq \sigma_c \quad \text{e} \quad \sigma_c \geq \sigma_{ac} - 1.$$

Un esempio di serie di Dirichlet con ascisse di convergenza distinte é fornito da:

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s},$$

che converge per $\sigma > 0 = \sigma_c$, ma converge assolutamente solo per $\sigma > 1 = \sigma_{ac}$ (in questo caso la distanza fra σ_{ac} e σ_c é massima, cfr. 1.10).

Vediamo ora un risultato che ci sar  utile nel seguito:

TEOREMA 1.4 (DI UNICIT  PER LE SERIE DI DIRICHLET).

Se $f(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$, $g(s) = \sum_{n=1}^{\infty} b(n)n^{-s}$ (per entrambe $\sigma_{ac} < \infty$) ed esiste una successione di numeri complessi, $\{s_k\}$, tale che:

$$f(s_k) = g(s_k) \quad \forall k \in \mathbf{N} \quad e \quad \sigma_k \stackrel{def}{=} \operatorname{Re}(s_k) \rightarrow \infty \text{ quando } k \rightarrow \infty,$$

allora $a = b$.

Dal teorema segue immediatamente che ogni s.d.D. non identicamente nulla ammette un **semipiano zero-free**, ovvero un semipiano in cui non si annulla mai.

Veniamo al teorema più interessante riguardo le s. d. D.; esso collega immediatamente il prodotto di Dirichlet, $*$, (v. §1.1.1) con il prodotto fra s. d. D.:

TEOREMA 1.5. Se $f(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$, $g(s) = \sum_{n=1}^{\infty} \frac{b(n)}{n^s}$ e $\sigma_{ac} < \infty$ per entrambe, allora:

$$i) \sigma > \max(\sigma_{ac}(f), \sigma_{ac}(g)) \Rightarrow f(s)g(s) = \sum_{n=1}^{\infty} h(n)n^{-s}, \text{ con } h = a * b;$$

$$ii) \exists \{s_k\} \subseteq \mathbf{C} : f(s_k)g(s_k) = \sum_{n=1}^{\infty} c(n)n^{-s_k} \quad \forall k \in \mathbf{N} \text{ e } \sigma_k \rightarrow \infty \text{ per } k \rightarrow \infty \Rightarrow c = a * b.$$

Infatti i) afferma che il prodotto di due s.d.D. assolutamente convergenti è uguale alla s.d.D. del prodotto di convoluzione dei loro coefficienti; la ii) diventa, quindi, una semplice conseguenza del teorema 1.4.

Il seguente teorema ci dà una condizione sufficiente per la regolarità della funzione f di cui alla 1.9 e l'espressione esplicita di df/ds (scriveremo $f'(s)$):

TEOREMA 1.6. Se $\sigma > \sigma_c$ allora:

$$i) \text{ la funzione somma di } \sum_{n=1}^{\infty} a(n)n^{-s} = f(s) \text{ è analitica;}$$

$$ii) f'(s) = - \sum_{n=1}^{\infty} a(n) \log(n)n^{-s}.$$

Da ii) si vede immediatamente che la scelta $h(n) = -\log n$ fatta nel §1.1.1 è coerente con le regole di calcolo di $f'(s)$ (che si ottiene derivando termine a termine).

Vediamo degli esempi di s. d. D.:

8 CAPITOLO 1. RICHIAMI DI TEORIA ANALITICA DEI NUMERI

$$\sum_{n=1}^{\infty} \mathbf{e}(n)n^{-s} = 1 \quad \forall s \in \mathbf{C} \text{ (s.d.D. assoc. ad } \mathbf{e})$$

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} \quad \forall s : \sigma > 1 \text{ (funzione zeta di Riemann, assoc. ad } \mathbf{1})$$

$$\sum_{n=1}^{\infty} nn^{-s} = \sum_{n=1}^{\infty} n^{-s+1} = \zeta(s-1) \quad \forall s : \sigma > 2 \text{ (s.d.D. assoc. ad } \mathbf{I})$$

$$\sum_{n=1}^{\infty} \mu(n)n^{-s} \quad \text{con } \sigma_{ac} = 1 \text{ (s.d.D. assoc. alla } \mu \text{ di Möbius)}$$

$$\sum_{n=1}^{\infty} \phi(n)n^{-s} \quad \text{con } \sigma_{ac} \leq 2 \text{ (s.d.D. assoc. alla } \phi \text{ di Eulero)}$$

$$\sum_{n=1}^{\infty} \Lambda(n)n^{-s} \quad \text{con } \sigma_{ac} = 1 \text{ (s.d.D. assoc. alla } \Lambda \text{ di von Mangoldt)}$$

Grazie alla relazione 1.6 ed ai teoremi 1.3 ed 1.5 si ha:

$$\sigma > 2 \Rightarrow \sum_{n=1}^{\infty} \phi(n)n^{-s} = \frac{\zeta(s-1)}{\zeta(s)}.$$

Applicando i teoremi 1.2, 1.3 e 1.5 si ottiene invece:

$$\sigma > 1 \Rightarrow \zeta(s) \sum_{n=1}^{\infty} \mu(n)n^{-s} = 1,$$

da cui:

$$(1.11) \quad |\zeta(s)| > 0 \quad e \quad \sum_{n=1}^{\infty} \mu(n)n^{-s} = \frac{1}{\zeta(s)} \quad \text{in } \sigma > 1.$$

Per gli stessi teoremi, se $f(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$:

$$(1.12) \quad a \text{ completam. moltiplicativa} \Leftrightarrow \sum_{n=1}^{\infty} \mu(n)a(n)n^{-s} = \frac{1}{f(s)},$$

nel semipiano $\sigma > \sigma_{ac}$.

Impieghiamo, ora, i teoremi 1.3, 1.5 e 1.6 per ottenere una relazione che ci sarà molto utile nel seguito (essendo il punto di partenza per la dimostrazione del Teorema dei Numeri Primi).

Se $\sigma > 1$ allora:

$$\zeta'(s) = (\text{per ii) del teor.1.6}) = - \sum_{n=1}^{\infty} \log(n)n^{-s} =$$

$$= (\text{per il Teor. 1.5 e la 1.7}) = -\zeta(s) \sum_{n=1}^{\infty} \Lambda(n)n^{-s},$$

da cui si ha:

$$(1.13) \quad \sum_{n=1}^{\infty} \Lambda(n)n^{-s} = -\frac{\zeta'(s)}{\zeta(s)}, \quad \forall \sigma > 1.$$

Diamo ora un risultato classico circa le singolarità delle funzioni definite da S.d.D. a termini positivi, il Teorema di Landau (v. [Te], p.110)

TEOREMA 1.7. (E. LANDAU)

Se $\sum_{n=1}^{\infty} a(n)n^{-s}$ ha $\sigma_c < \infty$ ed $\exists n_0$ tale che $a(n) \geq 0 \quad \forall n \geq n_0$, allora la funzione somma $f(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ ha una singolarità in σ_c .

Da questo teorema segue, in particolare, che la funzione ζ di Riemann ha una singolarità in $s = 1$, così come la funzione:

$$\sum_{n=1}^{\infty} \Lambda(n)n^{-s} = -\frac{\zeta'(s)}{\zeta(s)}.$$

(Per le dimostrazioni dei teoremi di questo paragrafo si veda [A], cap. XI; anche [Te], capitolo I.2, §2.3 e cap. II.1, §1.1, §1.2, §1.3.).

1.1.4 Prodotti di Eulero.

Consideriamo il **prodotto infinito** $\prod_{n=1}^{\infty} (1 + a(n))$, con $a \in \mathcal{A}$, che è definito da:

$$\prod_{n=1}^{\infty} (1 + a(n)) \stackrel{\text{def}}{=} \lim_{m \rightarrow \infty} \prod_{n=1}^m (1 + a(n));$$

quando tale limite esiste (se il limite è finito e non nullo si dice che il **prodotto è convergente**).

Inoltre $\prod_{n=1}^{\infty} (1 + a(n))$ **converge assolutamente**, per definizione, se $\sum_{n=1}^{\infty} a(n)$ è assolutamente convergente.

Nel seguito scriveremo \prod_p per indicare il prodotto infinito esteso a tutti i primi p (ovvero sottintenderemo $p \in \mathbf{P}$).

Abbiamo il seguente teorema :

TEOREMA 1.8 (IDENTITÀ DI EULERO).

Siano $f \in \mathcal{M}$ e $\sum_{n=1}^{\infty} |f(n)| < \infty$; allora:

i) $\sum_{n=1}^{\infty} f(n) = \prod_p (1 + f(p) + f(p^2) + f(p^3) + f(p^4) + \dots)$ e tale prodotto converge assolutamente;

ii) f completamente moltiplicativa $\Rightarrow \sum_{n=1}^{\infty} f(n) = \prod_p \left(\frac{1}{1-f(p)}\right)$.

Scegliendo $f(n) = a(n)n^{-s}$ nel precedente teorema abbiamo il notevole:

COROLLARIO 1.1. (PRODOTTI DI EULERO)

Se $a \in \mathcal{M}$ e $\sigma > \sigma_{ac}$ allora :

i) $\sum_{n=1}^{\infty} a(n)n^{-s} = \prod_p (1 + a(p)p^{-s} + a(p^2)p^{-2s} + a(p^3)p^{-3s} + \dots)$;

ii) a completamente moltiplicativa $\Rightarrow \sum_{n=1}^{\infty} a(n)n^{-s} = \prod_p \frac{1}{1-a(p)p^{-s}}$.

In particolare, per $a = \mathbf{1}$, abbiamo l'identità per la funzione ζ di Riemann

$$(1.14) \quad \zeta(s) \stackrel{def}{=} \sum_{n=1}^{\infty} n^{-s} = \prod_p \frac{1}{1-p^{-s}} \quad \forall s : \sigma > 1,$$

detta **Identità di Eulero**, che é la versione analitica del teorema fondamentale dell'aritmetica.

Inoltre, per $a(n) = \chi(n)$, con χ carattere di Dirichlet (mod q), non principale (v. §2.4.2)

$$(1.15) \quad L(s, \chi) \stackrel{def}{=} \sum_{n=1}^{\infty} \chi(n)n^{-s} = \prod_p \frac{1}{1-\chi(p)p^{-s}} \quad \forall \sigma > 1,$$

che, per il carattere principale, diventa (dato che $\chi_0(p) = 0 \Leftrightarrow p|q$, v. §2.4.2)

$$(1.16) \quad L(s, \chi_0) \stackrel{def}{=} \sum_{n=1}^{\infty} \chi_0(n)n^{-s} = \zeta(s) \prod_{p|q} (1-p^{-s}) \quad \forall \sigma > 1$$

e quindi $L(s, \chi_0)$ e la funzione ζ coincidono, a meno di un prodotto finito (che definisce una funzione olomorfa in $s \in \mathbf{C}$ e dipendente dal modulo q).

1.2 Funzione ζ di Riemann

1.2.1 Funzione ζ di Riemann

Come abbiamo già visto nel §1.1.3, la **funzione ζ di Riemann** é definita da:

$$(1.17) \quad \zeta(s) \stackrel{def}{=} \sum_{n=1}^{\infty} n^{-s} \quad \forall s \in \mathbf{C} : \sigma > 1.$$

Per ottenere un' estensione della ζ ad altri valori di $s \in \mathbf{C}$, diamo un' applicazione del lemma 1.1 di sommazione parziale alle s.d.D. con coefficienti $a(n)$, $a \in \mathcal{A}$ qualunque :

$$\sum_{n \leq x} a(n)n^{-s} = A(x)x^{-s} + s \int_1^x \frac{A(t)}{t^{s+1}} dt$$

da cui, nel limite $x \rightarrow \infty$, si ha:

$$(1.18) \quad \lim_{x \rightarrow \infty} \frac{A(x)}{x^s} = 0 \Rightarrow \sum_{n=1}^{\infty} a(n)n^{-s} = s \int_1^{\infty} \frac{A(x)}{x^{s+1}} dx.$$

Applichiamo tale formula per $a = \mathbf{1}$ e $\sigma > 1$ in modo da avere ($[x]$ sta per **parte intera** di x e $\{x\} \stackrel{def}{=} x - [x]$ é la **parte frazionaria**):

$$(1.19) \quad \zeta(s) = s \int_1^{\infty} \frac{[x]}{x^{s+1}} dx = \frac{s}{s-1} - s \int_1^{\infty} \frac{\{x\}}{x^{s+1}} dx,$$

che (poichè l' integrale converge $\forall \sigma > 0$ ed uniformemente per $\sigma \geq \delta > 0$, $\forall \delta > 0$), ci dà il **prolungamento analitico della funzione di Riemann al semipiano $\sigma > 0$ privato del punto 1**, nel quale la ζ ha un **polo semplice con residuo pari ad 1**.

Vedremo nel seguito come estendere ζ a tutto \mathbf{C} , tranne 1 (la sola 1.19 non ci assicura l' assenza di altre singolarità), attraverso i risultati enunciati da Riemann nel suo famoso memoriale del 1859 (v. §1.2.3).

Richiamiamo, prima, brevemente la definizione e le principali proprietà della **funzione Γ di Eulero** (per le dimostrazioni si veda [Gr], §1 del cap. XII):

$$(1.20) \quad \Gamma(s) \stackrel{def}{=} \int_0^{\infty} x^{s-1} e^{-x} dx \quad \forall s \in \mathbf{C} : \sigma > 0.$$

La funzione $1/\Gamma(s)$ ha il seguente prodotto di Weierstrass:

$$(1.21) \quad \frac{1}{\Gamma(s)} = s e^{\gamma s} \prod_{n=1}^{\infty} (1 + s/n) e^{-s/n} \quad \forall s \in \mathbf{C},$$

dove:

$$(1.22) \quad \gamma \stackrel{def}{=} \lim_{n \rightarrow \infty} \left(\sum_{k=1}^n \frac{1}{k} - \log n \right)$$

é la costante di Eulero.

Valgono le seguenti relazioni funzionali:

$$(1.23) \quad \Gamma(s+1) = s\Gamma(s),$$

ovvero l' **Equazione Funzionale della funzione Γ di Eulero**, la

$$(1.24) \quad \Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)},$$

detta **Relazione dei Complementi**, e la cosiddetta **Formola di Duplicazione di Legendre**

$$(1.25) \quad \Gamma(s)\Gamma(s+1/2) = 2^{1-2s} \pi^{1/2} \Gamma(2s)$$

che, combinate, danno:

$$(1.26) \quad \Gamma(s/2)/\Gamma((1-s)/2) = \pi^{-1/2} 2^{1-s} \cos(\pi s/2) \Gamma(s).$$

Supponendo poi, $\forall \delta > 0$ fissato, che $-\pi + \delta < \arg(s) < \pi - \delta$ e $|s| \rightarrow \infty$, si ha la **Formola di Stirling**:

$$(1.27) \quad \log \Gamma(s) = \left(s - \frac{1}{2}\right) \log s - s + \frac{\log(2\pi)}{2} + \mathcal{O}(|s|^{-1});$$

da essa si ricava la relazione che esprime la **derivata logaritmica di Γ** :

$$(1.28) \quad \frac{\Gamma'(s)}{\Gamma(s)} = \log s + \mathcal{O}(|s|^{-1}).$$

1.2.2 Equazione Funzionale della ζ

Riemann dimostrò che (cfr. §1.2.3):

i) la funzione ζ definita dalla 1.17 può essere prolungata a **funzione analitica su tutto \mathbf{C} , tranne in 1, dove ha un polo semplice con residuo pari ad 1;**

ii) soddisfa l' **Equazione Funzionale** :

$$(F.E.) \quad \pi^{-s/2} \Gamma(s/2) \zeta(s) = \pi^{-(1-s)/2} \Gamma\left(\frac{1-s}{2}\right) \zeta(1-s)$$

(dalla terminologia inglese, Functional Equation).

Dalla *F.E.* e dalle proprietà della Γ si ottengono inoltre le proprietà :

iii) $\zeta(s) = 0, \sigma < 0 \Leftrightarrow s = -2, -4, -6, -8, \dots$ (**zeri banali**) (poichè $|\zeta(s)| > 0 \quad \forall \sigma > 1$ per la 1.11);

iv) gli zeri in $0 < \sigma < 1$, la **striscia critica**, sono simmetrici sia risp. l' asse reale che risp. la retta $\sigma = 1/2$, detta **retta critica** (ovvero c' è **simmetria degli zeri non banali rispetto ad $s = 1/2$**);

v) la funzione $\xi(s) \stackrel{def}{=} \frac{s(s-1)}{2} \pi^{-s/2} \Gamma(s/2) \zeta(s)$ **è intera e ha** la seguente **Equazione Funzionale**:

$$(1.29) \quad \xi(s) = \xi(1-s) \quad \forall s \in \mathbf{C}.$$

Occupiamoci ora della ξ ; una funzione intera f si dice **di ordine finito** se $\exists \alpha > 0$ tale che:

$$(1.30) \quad f(z) = \mathcal{O}(e^{|z|^\alpha}) \quad (|z| \rightarrow \infty),$$

e diremo **ordine** di f l' estremo inferiore degli $\alpha > 0$ per i quali vale la 1.30 (si noti che escludiamo il caso f costante).

Si può dimostrare che (cfr. [D], cap. 11 e [Gr], cap. X):

TEOREMA 1.9. Una funzione intera f di ordine 1 ha la forma:

$$f(z) = e^{A+Bz} \prod_{n=1}^{\infty} (1 - z/z_n) e^{z/z_n} \quad \forall z \in \mathbf{C} \quad (A, B \in \mathbf{C} \text{ costanti}),$$

(detto **prodotto di Weierstrass** di f); qui $\{z_n\}_{n \in \mathbf{N}}$ è la successione degli zeri di f ordinati secondo $r_n \stackrel{\text{def}}{=} |z_n|$ e ripetuti secondo molteplicità; inoltre :

$$i) \quad \forall \epsilon > 0 \quad \sum_{n=1}^{\infty} r_n^{-1-\epsilon} < \infty;$$

$$ii) \quad \sum_{n=1}^{\infty} r_n^{-1} < \infty \Leftrightarrow \exists C : |f(z)| = \mathcal{O}(e^{C|z|}), \quad |z| \rightarrow \infty.$$

Per il Teorema precedente, si può sviluppare ξ in prodotto infinito, perchè

TEOREMA 1.10. $\xi(s)$ è una funzione intera di ordine 1.

Inoltre, dalla Formula di Stirling 1.27 segue che $\xi(s)$ non soddisfa la maggiorazione di cui al punto *ii*) del Teorema 1.9, per cui ha infiniti zeri; essi sono tutti e soli gli **zeri non banali della ζ** , ovvero gli zeri compresi nella striscia critica (per la v)).

Tramite i teoremi 1.9 e 1.10 si può dimostrare (come fece per primo Hadamard nel 1893) il:

COROLLARIO 1.2. ξ ha infiniti zeri, $\rho_1, \rho_2, \dots, \rho_n, \dots$; inoltre

$$i) \quad \forall \epsilon > 0 \quad \sum_{n=1}^{\infty} |\rho_n|^{-1-\epsilon} \text{ converge};$$

$$ii) \quad \sum_{n=1}^{\infty} |\rho_n|^{-1} \text{ diverge};$$

iii) $\exists A, B \in \mathbf{C} : \xi(s) = e^{A+Bs} \prod_{\rho} (1 - s/\rho) e^{s/\rho}$ (il prodotto è sugli zeri ρ della ξ).

Le costanti A e B possono essere calcolate facilmente (v. [D], cap. 12):

$$A = -\log 2; \quad B = -\frac{\gamma}{2} - 1 + \frac{\log(4\pi)}{2}.$$

(Qui γ è la costante di Eulero 1.22).

Prendendo i logaritmi di ambo i membri della iii) e derivando (ovvero effettuando la **derivata logaritmica**) si ha:

$$\frac{\xi'(s)}{\xi(s)} = B + \sum_{\rho} \left(\frac{1}{s-\rho} + \frac{1}{\rho} \right);$$

per definizione di ξ si ha quindi:

$$\frac{\zeta'(s)}{\zeta(s)} = B - \frac{1}{s-1} + \frac{\log \pi}{2} - \frac{\Gamma'(s/2+1)}{2\Gamma(s/2+1)} + \sum_{\rho} \left(\frac{1}{s-\rho} + \frac{1}{\rho} \right),$$

che per comodità scriveremo (come per le altre derivate logaritmiche) :

$$(1.31) \frac{\zeta'}{\zeta}(s) = B - \frac{1}{s-1} + \frac{\log \pi}{2} - \frac{1}{2} \frac{\Gamma'}{\Gamma} \left(\frac{s}{2} + 1 \right) + \sum_{\rho} \left(\frac{1}{s-\rho} + \frac{1}{\rho} \right).$$

Per l'osservazione seguente il teorema 1.10, la somma é estesa agli zeri non banali della ζ , che verranno indicati d' ora in poi con $\rho = \beta + i\gamma$, $\beta \in [0, 1]$ e $\gamma \in \mathbf{R}$; si noti che la somma su $1/\rho$ converge nonostante diverga assolutamente : basta infatti raggruppare i termini ρ e $\bar{\rho}$ per avere

$$1/\rho + 1/\bar{\rho} = \frac{2\beta}{\beta^2 + \gamma^2} \leq \frac{2}{|\rho|^2}$$

e questo é il termine generale di una serie convergente (per la i) del cor.1.2).

1.2.3 Ipotesi di Riemann

Bernhard Riemann, nel memoriale del 1859 (l' unica sua pubblicazione di teoria dei numeri, di sole 8 pagine, dal titolo "*Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse*", cfr. [Ed]), oltre a dimostrare la i) e la ii) relative alla ζ (v. sezione precedente), fece le seguenti congetture:

- 1) la ζ ha infiniti zeri nella striscia critica (cfr. Cor.1.2);
- 2) vale la formula del Teorema 1.14;
- 3) ξ ammette la rappresentazione iii) del cor.1.2;

4) vale la Formula Esplicita per $\pi(x) - li(x)$, dimostrata da von Mangoldt nel 1895 (cfr. §1.4);

5) la ζ ha tutti gli zeri non banali sulla retta critica, ovvero:

$$(\mathbf{R.H.}) \quad \zeta(s) = 0, \operatorname{Re}(s) > 0 \Rightarrow \operatorname{Re}(s) = 1/2,$$

la famosa **Ipotesi di Riemann** (seguiamo l' acronimo inglese, che sta per "Riemann Hypothesis"), l' unica delle quali non ancora dimostrata.

Riguardo (*R.H.*), G. H. Hardy provò nel 1914 che infiniti zeri non banali si trovano sulla retta critica, mentre nel 1942 A. Selberg dimostrò che essa ne contiene una proporzione positiva, ovvero, detto

$$(1.32) \quad N(T) \stackrel{def}{=} |\{\rho = \beta + i\gamma : \zeta(\rho) = 0, 0 < \beta < 1, \gamma \in [0, T]\}|$$

il numero degli zeri della ζ nel rettangolo della striscia critica individuato dalle ordinate 0 e T ed indicato con

$$(1.33) \quad N_0(T) \stackrel{def}{=} |\{t \in [0, T] : \zeta(1/2 + it) = 0\}|$$

il numero degli zeri della ζ sul segmento della retta critica individuato dalle ordinate 0 e T , si ha che $\exists c > 0$ tale che

$$N_0(T) \geq cN(T), \quad \text{per } T \rightarrow \infty.$$

L' Ipotesi di Riemann é quindi equivalente a: $N(T) = N_0(T)$.

Essa ha notevoli conseguenze sulla distribuzione dei primi (cfr. §2.2.3).

1.2.4 Regioni Zero-free

Vediamo l' argomento euristico di Hadamard per dimostrare che :

$$\sigma = 1 \Rightarrow |\zeta(s)| > 0,$$

che é una premessa indispensabile per la dimostrazione del Teorema dei Numeri Primi.

Hadamard intuì che, poichè (v. Identità di Eulero 1.14):

$$\operatorname{Re}(\log \zeta(s)) = \sum_p \sum_{m=1}^{\infty} m^{-1} p^{-m\sigma} \cos(t \log(p^m)) \quad \forall \sigma > 1,$$

se $\zeta(s)$ avesse uno zero in $1 + it$, allora:

$$\operatorname{Re}(\log \zeta(\sigma + it)) \rightarrow -\infty, \quad \text{per } \sigma \rightarrow 1^+,$$

da cui $\cos(tm \log p)$ dovrebbe essere "quasi sempre" negativo; quindi $\cos(2tm \log p)$ sarebbe "quasi sempre" positivo, rendendo poco plausibile che $\operatorname{Re}(\log \zeta(\sigma + 2it))$ rimane limitato per $\sigma \rightarrow 1^+$ (cfr. [D], cap. 13).

TEOREMA 1.11. *Sulla retta $\sigma = 1$ la ζ di Riemann non si annulla mai.*

Vediamo una generalizzazione che migliora questo teorema, fornendo una prima **regione zero-free** per ζ , ovvero un sottinsieme della striscia critica libero da zeri.

TEOREMA 1.12. *Esiste $c > 0$, esplicitabile, tale che $|\zeta(s)| > 0$ in:*

$$\sigma \geq 1 - \frac{c}{\log(|t| + 2)} \quad \forall t \in \mathbf{R}.$$

La regione zero-free più ampia fu trovata da Vinogradov e Korobov, indipendentemente, nel 1958 (tramite stime di somme esponenziali, cfr. le stime di Vinogradov al §3.5):

TEOREMA 1.13. *(I. M. VINOGRADOV - N. M. KOROBOV)*

Per ogni $\alpha > 2/3$ $\exists c = c(\alpha)$ tale che $|\zeta(\sigma + it)| > 0$ in :

$$\sigma \geq 1 - \frac{c(\alpha)}{(\log^\alpha t)}.$$

1.2.5 Stime di Densità degli Zeri

Sono detti **Teoremi di densità** tutti i risultati riguardanti stime sul numero degli zeri di ζ (o delle $L(s, \chi)$) in una data regione (di solito rettangolare) della striscia critica.

Vediamone il primo, congetturato da Riemann nel suo memoriale e dimostrato da von Mangoldt nel 1905 :

TEOREMA 1.14. Sia $N(T)$ il numero di zeri della ζ definito dalla 1.32; allora:

$$(1.34) \quad N(T) = \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + \mathcal{O}(\log T).$$

Nelle applicazioni i teoremi di densità più usati sono, però, quelli che danno il numero di zeri con parte reale maggiore di σ :

$$N(\sigma, T) \stackrel{def}{=} |\{\rho = \beta + i\gamma : \zeta(\rho) = 0, 0 < \sigma \leq \beta \leq 1, 0 < \gamma \leq T\}|, \quad \forall \sigma < 1$$

(per $\sigma \geq 1$ banalmente $N(\sigma, T) = 0$); ne diamo due esempi :

la **stima di densità di Ingham** (v. [In]):

TEOREMA 1.15. (A. E. INGHAM)

$$N(\sigma, T) \ll T^{\frac{3(1-\sigma)}{2-\sigma}} \log^5 T \quad \forall \sigma \in]0, 1[;$$

e la **stima di densità di Huxley** (v. [Hu(1)] e [Hu(2)]):

TEOREMA 1.16. (M. N. HUXLEY)

$$N(\sigma, T) \ll T^{\frac{3(1-\sigma)}{3\sigma-1}} \log^{12} T \quad \forall \sigma \in]0, 1[.$$

Combinando gli ultimi due Teoremi, otteniamo (v. [Hu(1)], cap. 28)

PROPOSIZIONE 1.2. (INGHAM - HUXLEY)

$$N(\sigma, T) \ll T^{\frac{12}{5}(1-\sigma)} \log^{12} T \quad \forall \sigma \in]0, 1[.$$

1.3 Funzioni L di Dirichlet

1.3.1 Funzioni L di Dirichlet

Fissati $q \in \mathbf{N}$ e $\chi(\bmod q)$, definiamo la **funzione $L(s, \chi)$ di Dirichlet** come funzione somma della s.d.D. associata alla funzione $\chi \in \mathcal{A}$:

$$(1.35) \quad L(s, \chi) \stackrel{def}{=} \sum_{n=1}^{\infty} \chi(n)n^{-s} \quad \forall \sigma > 1;$$

tramite la 1.16 otteniamo il prolungamento analitico della $L(s, \chi_0)$ grazie alla 1.19 in $\sigma > 0$, ma con un polo semplice in 1; inoltre, se χ non è principale, nella 1.18 il termine $A(x)$ è limitato, in virtù della 2.17, per cui abbiamo il prolungamento analitico in $\sigma > 0$.

1.3.2 Equazione Funzionale delle L

Per le funzioni $L(s, \chi)$ di Dirichlet, con χ primitivo vale una equazione funzionale analoga a quella per la funzione ζ di Riemann; stavolta, però, essa dipende dalla "parità" del carattere $\chi(\bmod q)$. Infatti, poichè $1 = \chi(1) = \chi(-1)^2$, abbiamo $\chi(-1) = 1$ oppure $\chi(-1) = -1$; per distinguere questi due casi, definiamo:

$$a = a(\chi) \stackrel{def}{=} \begin{cases} 1 & \text{se } \chi(-1) = -1, \\ 0 & \text{se } \chi(-1) = 1. \end{cases}$$

Vale il:

TEOREMA 1.17. (EQUAZIONE FUNZIONALE DELLE $L(s, \chi)$)

Sia $\chi(\bmod q)$ primitivo ($q \in \mathbf{N}$ fissato); se definiamo:

$$\xi(s, \chi) \stackrel{def}{=} \left(\frac{q}{\pi}\right)^{\frac{s+a}{2}} \Gamma\left(\frac{s+a}{2}\right) L(s, \chi),$$

allora :

$$(F.E.\chi) \quad \xi(1-s, \bar{\chi}) = \frac{i^a q^{1/2}}{\tau(\chi)} \xi(s, \chi)$$

(il fattore che moltiplica $\xi(s, \chi)$ ha modulo unitario per la 2.23).

La dimostrazione (v. [D], cap. 9) é condotta sulle stesse linee della dimostrazione della *F.E.*.

Come per la ζ , l'equazione funzionale delle $L(s, \chi)$ implica:

i) le $L(s, \chi)$ definite dalla 1.35 possono essere **prolungate a funzioni intere**;

ii) per $\chi(-1) = 1$ (ovvero $a(\chi) = 0$) si ha:

$$L(s, \chi) = 0, \sigma \leq 0 \Rightarrow s = 0, -2, -4, -6, \dots \text{ (zeri banali);}$$

per $\chi(-1) = -1$ (ovvero $a(\chi) = 1$) invece:

$$L(s, \chi) = 0, \sigma \leq 0 \Rightarrow s = -1, -3, -5, -7, \dots \text{ (zeri banali);}$$

iii) per $0 < \sigma \leq 1$ le $L(s, \chi)$ hanno **zeri** (detti **non banali**) simmetrici rispetto alla retta $\sigma = 1/2$, ma, in generale, per χ complesso, non rispetto all'asse reale.

La funzione $\xi(s, \chi)$ é di ordine finito, anzi:

TEOREMA 1.18. $\xi(s, \chi)$ é una funzione intera di ordine 1.

Discende immediatamente dai teoremi 1.9 e 1.18 il :

COROLLARIO 1.3. $\xi(s, \chi)$ ha infiniti zeri, ρ_1, ρ_2, \dots , tali che :

$$\text{i) } \sum_{n=1}^{\infty} |\rho_n|^{-1-\epsilon} \text{ converge } \forall \epsilon > 0 ;$$

$$\text{ii) } \sum_{n=1}^{\infty} |\rho_n|^{-1} \text{ diverge;}$$

iii) $\exists A, B \in \mathbf{C} : \xi(s) = e^{A+Bs} \prod_{\rho} (1 - s/\rho) e^{s/\rho}$ (il prodotto é sugli zeri ρ della $\xi(s, \chi)$).

Questa volta, a differenza del prodotto per ξ , le costanti A e B dipendono dal carattere $\chi \pmod{q}$; grazie a iii) ed alla definizione di $\xi(s, \chi)$ abbiamo, analogamente alla 1.31:

$$(1.36) \frac{L'}{L}(s, \chi) = -\frac{1}{2} \log \frac{q}{\pi} - \frac{1}{2} \frac{\Gamma'}{\Gamma} \left(\frac{s+a}{2} \right) + B(\chi) + \sum_{\rho} \left(\frac{1}{s-\rho} + \frac{1}{\rho} \right)$$

dove la somma é estesa agli zeri della $\xi(s, \chi)$; questi ultimi sono gli zeri non banali della $L(s, \chi)$ corrispondente.

1.3.3 Ipotesi di Riemann Generalizzata e Teorema di Siegel

Analogamente alla funzione ζ , esiste una congettura riguardo la disposizione degli zeri non banali delle $L(s, \chi)$, detta **Ipotesi di Riemann Generalizzata** (che sembra essere stata formulata per la prima volta da Piltz, nel 1884):

$$\text{(G.R.H.)} \quad L(s, \chi) = 0, \operatorname{Re}(s) > 0 \Rightarrow \operatorname{Re}(s) = 1/2.$$

(di nuovo, l' acronimo é inglese e sta per "Generalized Riemann Hypothesis").

Per le L di Dirichlet si presenta un problema nuovo (rispetto alla teoria della ζ): se χ é reale e non principale, $L(s, \chi)$ ammette al più uno zero reale (semplice), detto **zero eccezionale** (o **zero di Siegel**).

Purtroppo, non si sa ancora se tale zero esiste; comunque, a tale proposito, si può fare l' ipotesi che esiste e, come per la (R.H.) o la (G.R.H.), ottenere una serie di risultati "condizionali", ovvero che assumono la verità (o, anche, la falsità) di tale ipotesi.

Il seguente **Teorema di Siegel** fornisce la regione zero-free più ampia nota per le funzioni L (per una dim. v. [D], cap.21):

TEOREMA 1.19. (C. L. SIEGEL) $\forall \epsilon > 0 \exists C(\epsilon) > 0$ tale che : χ non principale $\Rightarrow |L(s, \chi)| > 0$ in :

$$s > 1 - C(\epsilon)q^{-\epsilon}.$$

1.3.4 Regioni Zero-free

Per le regioni zero-free delle $L(s, \chi)$ valgono i teoremi :

TEOREMA 1.20. Esiste una costante $c > 0$ (esplicitabile) tale che, se $\chi(\bmod q)$ é complesso, $L(s, \chi)$ non ha zeri nella regione:

$$\sigma \geq \begin{cases} 1 - \frac{c}{\log(q|t|)} & \text{se } |t| \geq 1 \\ 1 - \frac{c}{\log q} & \text{se } |t| \leq 1 \end{cases}$$

Inoltre, se χ é reale e non principale, $L(s, \chi)$ ammette al più uno zero reale (semplice) in tale regione, lo **zero eccezionale** (o **zero di Siegel**, v. §1.3.3).

In questo caso, per tale $\chi(\bmod q)$ esiste comunque una costante positiva $c > 0$ (che non denota, però, sempre la stessa costante) per la quale ogni zero di $L(s, \chi)$ per il quale $|\gamma| \geq \frac{c}{\log q}$ soddisfa $\beta < 1 - \frac{c}{5(\log q + \log(|\gamma| + 2))}$.

Per una regione zero-free più ampia, ma con una costante non esplicitabile, v. il *Teorema di Siegel* (sez. prec.). Per le dim. di questa sez., v. [D], cap.14.

1.3.5 Stime di Densità degli Zeri

Poichè gli zeri non banali delle $L(s, \chi)$ non sono, in generale, disposti in maniera simmetrica rispetto all'asse reale, definiamo:

$$(1.37) \quad N(T, \chi) \stackrel{def}{=} |\{\rho = \beta + i\gamma : L(\rho, \chi) = 0, 0 < \beta < 1, |t| \leq T\}|$$

e :

$$(1.38) \quad N(\sigma, T, \chi) \stackrel{def}{=} |\{\rho = \beta + i\gamma : L(\rho, \chi) = 0, \sigma < \beta < 1, |t| \leq T\}|.$$

Generalizzando il teorema 1.18 alle $L(s, \chi)$, poichè $N(T, \chi) = 2N(T) \forall \chi(\bmod 1)$, (dalla 1.37), si ha (v. [D], cap. 16) il:

TEOREMA 1.21. *Sia $q \in \mathbf{N}$, $\chi = \chi(\bmod q)$ e $N(T, \chi)$ definito dalla 1.37; allora :*

$$\frac{1}{2}N(T, \chi) = \frac{T}{2\pi} \log \frac{qT}{2\pi} - \frac{T}{2\pi} + \mathcal{O}(\log(qT)).$$

Per quanto riguarda il numero di zeri nella 1.38, abbiamo (cfr. anche [M(1)]), ad esempio, la stima di Bombieri (v. Cor. in [B(2)])

PROPOSIZIONE 1.3. *Uniformemente per $\frac{1}{2} \leq \alpha \leq 1$ e $2 \leq T \leq X^{1/2}$ si ha*

$$\sum_{q \leq X} \sum_{\chi} N(\sigma, T, \chi) \ll X^{1+2(1-\alpha)+\varepsilon} T^{1+\varepsilon};$$

inoltre, uniformemente per $\frac{5}{6} \leq \alpha \leq 1$ e $2 \leq T \leq X^2$, si ha

$$\sum_{q \leq X} \sum_{\chi} N(\sigma, T, \chi) \ll X^{1+\varepsilon} T^{2+\varepsilon}.$$

1.4 Formule Esplicite

1.4.1 Formula di Perron

Le formule di Perron sono uno strumento essenziale della T.A.N., in quanto permettono di ottenere una stima "esplicita" di $\psi(x)$ (e quindi, per somministrazione parziale, di $\pi(x)$).

Esse, infatti, collegano le somme parziali di una s.d.D. alla somma della serie stessa (quando questa converge assolutamente).

Vediamo il risultato classico di Perron, che ha dato il nome alle altre formule simili:

TEOREMA 1.22 (FORMULA DI PERRON). *Siano $c > 0$, $x > 0$, $f(s) \stackrel{def}{=} \sum_{n=1}^{\infty} a(n)n^{-s}$, $w = u + iv$ ed $u > \sigma_{ac} - c$. Allora:*

$$(1.39) \quad \sum'_{n \leq x} a(n)n^{-w} = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} f(s+w) \frac{x^s}{s} ds.$$

Qui (e nel seguito) **la somma con apice indica**, per def., *che il termine relativo ad x , $a(x)x^{-w}$, se presente, ovvero se $x \in \mathbf{N}$, va dimezzato.*

La dimostrazione si può fare, ad esempio, utilizzando il Teorema dei Residui (di Cauchy).

Impiegando in modo analogo il Teorema dei Residui si possono dimostrare formule analoghe (per la dim. del Teorema ed approfondimenti si veda il [Te], pp. 130-134).

1.4.2 Formula Esplicita di Riemann – von Mangoldt

Diamo ora *la formula esplicita per ψ* provata nel 1905 da von Mangoldt sulle linee indicate da Riemann nel memoriale del 1859; per tale motivo essa é detta **Formula Esplicita Classica di Riemann-von Mangoldt**.

Definendo (v. sopra per la def. dell' apice):

$$\psi_0(x) \stackrel{def}{=} \sum'_{n \leq x} \Lambda(n),$$

vale la seguente formula.

TEOREMA 1.23 (FORMULA ESPLICITA CLASSICA). Se $x > 1$ valgono le:

$$\psi_0(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{\zeta'}{\zeta}(0) - \frac{1}{2} \log(1 - x^{-2}),$$

con

$$\sum_{\rho} \frac{x^{\rho}}{\rho} \stackrel{def}{=} \lim_{T \rightarrow \infty} \sum_{\rho: |\gamma| \leq T} \frac{x^{\rho}}{\rho}$$

e:

$$(1.40) \quad \psi_0(x) = x - \sum_{|\gamma| \leq T} \frac{x^{\rho}}{\rho} - \frac{\zeta'}{\zeta}(0) - \frac{1}{2} \log(1 - x^{-2}) + E(x, T),$$

dove

$$E(x, T) \ll \frac{x \log^2(xT)}{T} + (\log x) \min\left(1, \frac{x}{T < x >}\right)$$

essendo $< x > \stackrel{def}{=} \min_{\{q \in \mathbf{N}: q = p^{\alpha}\}} |x - q|$.

In particolare, se $T \leq x$, si ha:

$$(1.41) \quad \psi(x) = x - \sum_{|\gamma| \leq T} \frac{x^{\rho}}{\rho} + E(x, T),$$

dove

$$(1.42) \quad E(x, T) \ll \frac{x \log^2 x}{T}.$$

Per provare 1.40 si utilizza la formula di Perron (di cui alla sez. prec.) e stime per la funzione ζ di Riemann (che derivano dall'espressione della sua derivata logaritmica, v. 1.31).

1.4.3 Formula Esplicita Classica per $\psi(x, \chi)$

Definiamo $\psi(x, \chi) \stackrel{def}{=} \sum_{n \leq x} \Lambda(n) \chi(n)$ e $\psi_0(x, \chi) \stackrel{def}{=} \sum'_{n \leq x} \Lambda(n) \chi(n)$.

Vale allora la seguente (v. [D], cap.19)

TEOREMA 1.24 (FORMULA ESPLICITA PER $\psi(x, \chi)$). Siano $q \geq 1$ ed $x > 1$; allora $\forall \chi = \chi \pmod{q}$ primitivo si ha :

$$(1.43) \quad \psi_0(x, \chi) = \epsilon(\chi)x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \epsilon_1(\chi)(\log x) - \epsilon_2(\chi) - \sum_{m=1}^{\infty} \frac{x^{a-2m}}{2m-a}$$

dove la prima serie é estesa agli zeri ρ non banali della funzione $L(s, \chi)$ e

$$\epsilon(\chi) \stackrel{def}{=} \begin{cases} 1 & \text{se } \chi = \chi_0 \\ 0 & \text{altrimenti} \end{cases}, \quad \epsilon_1(\chi) \stackrel{def}{=} 1 - a,$$

con $a = a(\chi)$ definita in §1.3.2 e

$$\epsilon_2(\chi) \stackrel{def}{=} \lim_{s \rightarrow 0} \left(\frac{L'}{L}(s, \chi) - \frac{\epsilon_1(\chi)}{s} \right);$$

inoltre :

$$(1.44) \quad \psi_0(x, \chi) = \epsilon(\chi)x - \sum_{|\gamma| \leq T} \frac{x^{\rho}}{\rho} - \epsilon_1(\chi)(\log x) - \epsilon_2(\chi) + E(x, T, \chi)$$

dove

$$E(x, T, \chi) \ll \frac{x \log^2(qxT)}{T} + (\log x) \min\left(1, \frac{x}{T < x >}\right).$$

In particolare, se $T \leq x$, vale:

$$(1.45) \quad \psi(x, \chi) = \epsilon(\chi)x - \sum_{|\gamma| \leq T} \frac{x^{\rho}}{\rho} + E(x, T, \chi),$$

dove

$$(1.46) \quad E(x, T, \chi) \ll \frac{x \log^2(qx)}{T}.$$

Capitolo 2

Problemi Moltiplicativi

2.1 Problemi Moltiplicativi

I problemi moltiplicativi, in Teoria Analitica dei Numeri, sono tutti i problemi connessi con la fattorizzazione degli interi (positivi).

In particolare, i principali riguardano :

- la distribuzione dei numeri primi (sia in intervalli "lunghi" che in intervalli corti) e quindi tutti gli strumenti analitici ad essa collegati (formule esplicite, stime sugli zeri della funzione ζ , identità combinatorie per approssimare la funzione caratteristica dei numeri primi, metodi di Crivello, stime di forme bilineari, stime sui polinomi di Dirichlet, ecc.);
- la distribuzione dei numeri primi nelle progressioni aritmetiche (di nuovo, sia in intervalli lunghi che in intervalli corti) e quindi tutti gli strumenti analitici ad essa collegati (che, oltre ai precedenti, comprendono anche stime sulle somme di Gauss, sulle somme di Ramanujan, sulle somme di caratteri di Dirichlet, ecc.);
- la distribuzione dei numeri primi in successioni polinomiali (ancora, sia in intervalli lunghi che corti), vale a dire la stima del numero di primi rappresentabili come valori di un polinomio (fissato); tramite i metodi di Crivello tale problema é spesso ricondotto al seguente:
- la distribuzione dei valori di un polinomio nelle progressioni aritmetiche (di solito, per i crivelli, al variare del solo modulo, con classe di resto 0; ma, anche, con classe di resto variabile, per altre applicazioni);

- il valore medio della funzione divisori (anche, di funzioni simili, come il numero di divisori primi, la funzione somma dei divisori, ecc.)
- più in generale, la rappresentabilità di tutti gli interi (positivi) come prodotto di un numero fissato (da stimare) di interi in un sottinsieme (fissato) di \mathbf{N} .

Per lo studio dei problemi moltiplicativi si impiegano le serie di Dirichlet, a causa della proprietà

$$(mn)^s = m^s n^s \quad \forall m, n \in \mathbf{N},$$

con $s \in \mathbf{C}$ fissato.

Notiamo che già Eulero, nel 1742, aveva ben chiara tale proprietà e la usava, ma con $s \in \mathbf{R}$.

In seguito, con Dirichlet e Riemann fu chiaro che i metodi dell' Analisi complessa avrebbero consentito una maggiore comprensione delle proprietà aritmetiche, insieme ad una maggiore flessibilità delle tecniche (dovuta sostanzialmente al teorema dei residui e alla possibilità di "classificare gli infiniti", grazie alla classificazione delle singolarità isolate delle funzioni analitiche).

Ovviamente, tutto ciò che si può studiare con metodi di Analisi complessa si può riportare nell' ambito dell' Analisi reale, ma a costo di una minore sinteticità e, talora, anche di una minore efficienza delle stime (si confronti la dimostrazione, cit. in §2.2.1, "elementare" del teorema dei numeri primi; oltre ad una minore trasparenza dell' argomento c'è anche la mancanza di una stima precisa del termine di resto, che si dimostra solo essere $o(x/\log x)$, cfr. §2.2.3).

2.2 Teorema dei Numeri Primi

2.2.1 Funzione π e stime di Cebicev

Definiamo la **funzione** π , che conta i primi fino ad x ($x > 0$):

$$\pi(x) \stackrel{def}{=} \sum_{\substack{p \leq x \\ p \text{ primo}}} 1.$$

(é da notare che π non é una funzione aritmetica; inoltre é una funzione a gradino, essendo costante negli intervalli $[p, p'$], dove p' é il primo successivo a p , e discontinua per x primo).

Il primo risultato sulla π è, ovviamente, il **Teorema di Euclide** : esistono infiniti primi, ovvero $\pi(x) \rightarrow \infty$, per $x \rightarrow \infty$.

Il primo studio sistematico della π comincia, però, con il matematico russo Cebicev, che, nel 1852, dimostra il "postulato di Bertrand", ovvero : ogni intervallo $]n, 2n]$, con $n \geq 1$ intero, contiene almeno un primo.

Tale risultato seguiva dalle stime inferiori e superiori

$$(2.1) \quad (c_1 + o(1)) \frac{x}{\log x} \leq \pi(x) \leq (c_2 + o(1)) \frac{x}{\log x}$$

($c_1 = \log(2^{1/2} 3^{1/3} 5^{1/5} 30^{-1/30})$ e $c_2 = \frac{6}{5}c_1$) e, come al solito in Analisi, $f = o(g)$ indica che $f(x)/g(x) \rightarrow 0$, quando $x \rightarrow \infty$. Nel seguito indicheremo come **stime di Cebicev** le seguenti

$$(2.2) \quad \frac{x}{\log x} \ll \pi(x) \ll \frac{x}{\log x},$$

dove abbiamo usato la **notazione di Vinogradov** $f \ll g$, che indica, per $g > 0$, che $\exists X > 0, \exists C > 0$ (eventualmente $C = C(X)$) tali che $|f(x)| \leq Cg(x) \quad \forall x > X$.

Dall' esame di tavole numeriche K. F. Gauss (nel 1792) e A. M. Legendre (nel 1798) ipotizzarono che:

$$(2.3) \quad \pi(x) \sim \frac{x}{\log x} \quad \text{per } x \rightarrow \infty$$

ovvero:

$$\lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1.$$

(Come al solito in Analisi, $f(x) \sim g(x)$, f e g sono **asintotiche**, se $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$, con x tendente al limite specificato: in questo caso $x \rightarrow \infty$).

La formula 2.3 prende il nome di **Teorema dei numeri primi**, ed è stata dimostrata per la prima volta, ed indipendentemente, nel 1896 da J. Hadamard e C. de la Vallée Poussin con metodi di analisi complessa, a partire dalle proprietà della funzione ζ di Riemann. In particolare, la proprietà richiesta è il non annullarsi sulla retta $\sigma = 1$.

La condizione $|\zeta(1 + it)| > 0$ è stata utilizzata anche in altre due dimostrazioni. Una, nel 1935, fu data da Ingham con tecniche di analisi di Fourier. L'altra, è stata data nel 1980, da J.D. Newman, che ha utilizzato tecniche di integrazione nel campo complesso.

Nel 1949, Paul Erdős ed Atle Selberg, indipendentemente, diedero una dimostrazione "elementare" della 2.3, ovvero non fecero uso di metodi dell'analisi complessa, né della ζ di Riemann. (Si veda, ad esempio, [H-W], cap. XXII.). Recentemente, è stata data un'altra dimostrazione elementare, da Daboussi (1984) (v. [Te]).

2.2.2 Funzioni ψ e θ di Cebicev

Definiamo, ora, le **funzioni di Cebicev**, ψ e θ ($x > 0$):

$$\psi(x) \stackrel{def}{=} \sum_{n \leq x} \Lambda(n), \quad \theta(x) \stackrel{def}{=} \sum_{p \leq x} \log p.$$

è immediato verificare che:

$$(2.4) \quad \psi(x) = \theta(x) + \mathcal{O}(x^{1/2} \log^2(x)),$$

dove $f(x) = \mathcal{O}(g(x))$ è una notazione usuale dell'Analisi, equivalente a $f(x) \ll g(x)$ (anche qui $x \rightarrow \infty$ e $g(x) > 0$), anche se quest'ultima è più usata in Teoria dei Numeri. Inoltre scriveremo $f(x) = \mathcal{O}_{\varepsilon, \vartheta, A, \dots}(g(x))$

oppure $f(x) \ll_{\varepsilon, \vartheta, A, \dots}(g(x))$ per indicare che la costante C dipende dalle variabili $\varepsilon, \vartheta, A, \dots$ (oltre che, eventualmente, da X , cfr. dopo la 2.2).

La notazione \mathcal{O} è dovuta a E. Landau, che la usò sistematicamente proprio per la Teoria Analitica dei Numeri (da allora è una notazione standard dell'Analisi). Inoltre, è molto usata anche la notazione di Vinogradov (v. sopra), $f \ll g$, che si incontra più frequentemente in Teoria dei Numeri, anche a causa della maggiore praticità.

Per mostrare le connessioni fra θ e π utilizzeremo una semplice conseguenza del Teorema Fondamentale del Calcolo Integrale :

LEMMA 2.1. (SOMMAZIONE PARZIALE)

Se $a \in \mathcal{A}$ ed $A(x) \stackrel{def}{=} \sum_{n \leq x} a(n)$ ($A(x) = 0 \quad \forall x < 1$), $f \in C^1([1, x])$ allora :

$$(2.5) \quad \sum_{n \leq x} a(n)f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt.$$

Applichiamo il lemma con $a(n) = \chi_{\mathbf{P}}(n) \log(n)$, (con $\chi_{\mathbf{P}}$ funzione caratteristica dei primi), ed $f(t) = 1/\log(t)$, $t \in [2, x]$, per avere:

$$\pi(x) = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t \log^2 t} dt.$$

Da quest' ultima, la 2.4 e la definizione della funzione "li", "logaritmo integrale" :

$$(2.6) \quad \text{li}(x) \stackrel{def}{=} \int_2^x \frac{dt}{\log t} = \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{dt}{\log^2 t},$$

si ha il

LEMMA 2.2. Se $\psi(x) = x + \mathcal{O}(R(x))$ allora

$$(2.7) \quad \pi(x) = \text{li}(x) + \mathcal{O}\left(\frac{R(x)}{\log x} + x^{1/2} \log x\right).$$

Poichè nella 2.6 si ha $\text{li}(x) \sim x/\log(x)$, dalla 2.7 segue, per $R(x) = o(\text{li}(x) \log x)$,

$$(2.8) \quad \pi(x) \sim \text{li}(x) \sim \frac{x}{\log x},$$

ovvero il Teorema dei Numeri Primi.

Nella prossima sezione vedremo come ottenere $R(x) = o(x)$, in modo da ottenere la 2.8 e quindi il Teorema dei Numeri Primi a partire dal Lemma 2.2.

2.2.3 Teorema dei Numeri Primi

Come abbiamo visto nel §1.3, la funzione ψ è un ottimo sostituto per π , la funzione che conta i primi fino ad x ; una formula nella quale compaia π può quindi essere rimpiazzata da una analoga relazione per ψ ; così la formula per $\pi(x) - li(x)$ data da Riemann nel suo famoso memoriale del 1860 e dimostrata da von Mangoldt nel 1895 è equivalente alla relazione per $\psi(x) - x$ data dalla *formula esplicita classica* (v. §1.4.2):

$$\psi(x) = x - \sum_{|\gamma| \leq T} \frac{x^\rho}{\rho} + E(x, T),$$

dove la somma è estesa agli zeri ρ non banali della ζ per i quali $|Im(\rho)| = |\gamma| \leq T$; se supponiamo $T \leq x$, il resto $E(x, T)$ è :

$$E(x, T) \ll \frac{x \log^2(x)}{T}.$$

Grazie a tale formula possiamo dimostrare il Teorema dei Numeri Primi utilizzando la regione zero-free del Teorema 1.12:

TEOREMA 2.1 (DE LA VALLEE POUSSIN). $\exists c > 0$ *esplicitabile tale che:*

$$\psi(x) = x + \mathcal{O}(x \exp(-c(\log x)^{1/2})).$$

DIM.: Si deve dimostrare che:

$$\psi(x) - x = - \sum_{|\gamma| \leq T} \frac{x^\rho}{\rho} + E(x, T) \ll x \exp(-c(\log x)^{1/2})$$

e scegliamo $T \leq x$ in modo che valga la 1.42; quindi per la simmetria dei ρ risp. l'asse reale resta da provare che:

$$\sum_{0 < |\gamma| < T} \frac{x^\rho}{\rho} \ll x \exp(-c(\log x)^{1/2}).$$

Per il Teorema 1.12 abbiamo che (c non é sempre la stessa):

$$(2.9) \quad |x^\rho| = x^\beta < x \exp(-c(\log x)/(\log T))$$

per $|\gamma| < T$ e T abbastanza grande (come possiamo supporre).

Notiamo che $\gamma > 0 \Rightarrow |\rho| \geq \gamma$ e quindi:

$$\sum_{0 < |\gamma| < T} \frac{1}{\rho} \ll \sum_{0 < \gamma < T} \frac{1}{\gamma};$$

quest' ultima somma può essere espressa come integrale di Riemann – Stieltjes:

$$(2.10) \quad \sum_{0 < \gamma < T} \frac{1}{\gamma} = \int_0^T t^{-1} dN(t) = \frac{1}{T} N(T) + \int_0^T t^{-2} N(t) dt,$$

dove abbiamo integrato per parti ($N(T)$ def. nella 1.32); dalla 2.10 e dalla 1.34 si ha quindi:

$$\sum_{0 < |\gamma| < T} \frac{1}{\rho} \ll \log^2(T).$$

Combinando quest' ultima e la 2.9 abbiamo:

$$\sum_{0 < |\gamma| < T} \frac{x^\rho}{\rho} \ll x \exp(-c(\log x)/(\log T)) \log^2(T),$$

da cui la tesi, scegliendo T tale che $\log^2(T) = \log(x)$.

Il Teorema dei Numeri Primi segue facilmente dal lemma 2.2; basta infatti scegliere in quest' ultimo il termine di resto dato dal Teorema precedente:

$$R(x) = \mathcal{O}(x \exp(-c(\log x)^{1/2})).$$

É evidente l' importanza di una buona stima del resto $R(x)$, ovvero di disporre di formule esplicite con un buon termine $E(x, T)$ (cfr. 1.42).

Come abbiamo visto nell' ultimo teorema, basta stimare la somma sugli zeri della ζ ed $E(x, T)$ nella formula esplicita classica per ottenere il Teorema dei Numeri Primi (a patto di scegliere opportunamente T); grazie all' Ipotesi di Riemann, *R.H.* (cfr. §1.2.3), la stima 2.9 diventa:

$$|x^\rho| = x^{1/2},$$

da cui (applichiamo la 1.42 con $T \leq x$):

$$|\psi(x) - x| \ll x^{1/2} \log^2(T) + \frac{x \log^2(x)}{T},$$

ovvero, prendendo $T = x^{1/2}$:

$$|\psi(x) - x| \ll x^{1/2} \log^2(x);$$

sotto *R.H.* abbiamo quindi:

$$\psi(x) = x + \mathcal{O}(x^{1/2} \log^2(x)),$$

ovvero il resto "migliore possibile" nel Lemma 2.2 e nella:

$$\pi(x) = li(x) + \mathcal{O}(x^{1/2} \log^2(x)).$$

Notiamo che la bontà del resto dipende ovviamente dalla disposizione degli zeri, e precisamente dall' ampiezza delle regioni zero-free della ζ .

Infatti, vale il seguente risultato:

PROPOSIZIONE 2.1. *Sia $1/2 \leq \theta < 1$ fissato. Allora*

$$|\psi(x) - x| \ll x^\theta \log^2 x \quad \Leftrightarrow \quad |\zeta(s)| > 0 \text{ per } \sigma > \theta.$$

DIM.: Supponiamo dapprima che

$$\psi(x) = x + \mathcal{O}(x^\theta \log^2 x);$$

dalla 1.18, con $a = \Lambda$, ovvero $A(x) = \psi(x)$, abbiamo quindi, grazie alla 1.13:

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \Lambda(n)n^{-s} = \frac{s}{s-1} + s \int_1^{\infty} \frac{R(x)}{x^{s+1}} dx \quad \forall \sigma > 1,$$

con $R(x) \ll x^{\theta} \log^2 x$, da cui l' integrale é definito e regolare per $\sigma > \theta$, in cui ζ non si annulla (altrimenti la derivata logaritmica avrebbe ivi una singolarità).

Ragionando come nel Teorema precedente si dimostra l' implicazione inversa.

Allo stesso modo, impiegando la più ampia regione zero-free di Vinogradov e Korobov (v. §1.2.4) otteniamo il Teorema più potente (del precedente, che utilizzava una regione zero-free meno estesa):

TEOREMA 2.2. $\forall \beta \in]0, 3/5[\exists c = c(\beta) > 0$ tale che:

$$\psi(x) = x + \mathcal{O}(x \exp(-c(\beta)(\log x)^{\beta})).$$

Infatti, può essere dimostrato come il precedente Teorema, scegliendo:

$$\log T = (\log x)^{\beta},$$

con $\beta = \frac{1}{\alpha+1}$, dove α é la costante della regione zero-free di Vinogradov – Korobov (cit., §1.2.4).

2.3 Primi negli Intervalli Corti

Diciamo che $[x, x + H]$ é un intervallo corto se $H = H(x)$ é una funzione positiva e crescente di x tale che H/x é decrescente, $H \rightarrow \infty$ e $H = o(x)$ per $x \rightarrow \infty$.

Nel 1972 M. N. Huxley [Hu(2)] ha dimostrato che, quando $H \geq x^{7/12+\epsilon}$, con $\epsilon > 0$, l' intervallo corto $[x, x + H]$ contiene sempre un primo, per x abbastanza grande; anzi, il numero di primi in quest' intervallo é pari al valore atteso (ovvero $H/\log x$).

Inoltre, usando il suo risultato sui teoremi di densità (cit.), si puo' vedere, con tecniche analitiche standard, che la richiesta sull' ordine di grandezza di H si puo' indebolire fino ad $H \geq x^{1/6+\epsilon}$ per ottenere che, per "quasi tutti" gli $x \in [N, 2N]$, $[x, x + H]$ contiene sempre un primo (per N abbastanza grande); con cio' si intende che l' insieme degli x in $[N, 2N]$ per i quali $[x, x + H]$ non contiene un primo ha misura al massimo $o(N)$ (in generale, diciamo che una relazione vale per quasi tutti gli $x \in I$ se e' vera $\forall x \in I \setminus S$, dove $|S| = o(|I|)$).

Più in generale, vale la seguente relazione fra teoremi di densità e primi in intervalli corti (rispettivamente, tutti o quasi tutti).

Diciamo che vale il **Teorema dei Numeri Primi nell' intervallo corto** $[x, x + h]$ se vale

$$(2.11) \quad \psi(x + h) - \psi(x) = (1 + o(1))h \quad (h = o(x) \text{ per } x \rightarrow \infty).$$

Il seguente risultato collega le stime di densità al Teorema dei Numeri Primi negli Intervalli Corti:

TEOREMA 2.3 (STIME DI DENSITÀ PER PRIMI IN INTERVALLI CORTI). *Sia*

$$N(\sigma, T) \ll T^{A(\sigma)(1-\sigma)} \log^D T \quad \text{unif. } \forall \sigma \in [1/2, 1],$$

per qualche $D \geq 1$ e $A(\sigma)(1 - \sigma) \leq 0$, dove per qualche $\frac{1}{2} < u < 1$ abbiamo $A(\sigma) \leq 2$ per $\sigma \geq u$ e, per $\frac{1}{2} \geq \sigma \geq u$ abbiamo $A(\sigma) \leq C$, per qualche $C > 1$. Allora vale la 2.11 con $h \geq x^{1-1/C} \log^M x$, per ogni $M > \frac{D+2}{C(1-u)}$.

Per quanto riguarda, invece, il Teorema dei Numeri Primi in quasi tutti gli Intervalli Corti (ovvero 2.11 per quasi tutti gli intervalli corti $[x, x + h]$), si ha il

TEOREMA 2.4 (STIME DI DENSITÀ PER PRIMI IN QUASI TUTTI GLI INTERVALLI CORTI). *Sia*

$$N(\sigma, T) \ll T^{C(1-\sigma)} \log^D T \quad \text{unif. } \forall \sigma \in [1/2, 1],$$

per qualche $C \geq 2$ e $D \geq 1$. Allora per quasi tutti gli x abbiamo la 2.11, sotto l'ipotesi che

$$h \geq x^{1-2/C} \log^B x, \quad (h = o(x), B \geq 0),$$

con $B = B(C, D)$ esplicitabile.

Per quanto riguarda la dimostrazione dei due Teoremi di cui sopra, si veda l' [Iv] (§12.5).

2.4 Primi nelle Progressioni Aritmetiche

2.4.1 Progressioni aritmetiche e Caratteri Additivi

Si definisce **progressione aritmetica** di modulo q un qualunque sottinsieme degli interi del tipo $\{qn + a : n \in \mathbf{N}\}$, con $q \in \mathbf{N}$ ed $a \in \mathbf{Z}$.

Si definisce **carattere additivo** una qualunque delle radici q -sime dell'unità nel campo complesso, diciamo $e_q(a) \stackrel{def}{=} e^{2\pi ia/q}$.

Per esprimere la condizione $n \equiv a \pmod{q}$ (e cioè che n sta nella progressione aritmetica $(\text{mod } q)$ relativa ad a) si può usare la relazione detta **ortogonalità dei caratteri additivi** (cfr. il paragrafo successivo per l'ortogonalità dei caratteri moltiplicativi)

$$(2.12) \quad \frac{1}{q} \sum_{j \leq q} e_q((n-a)j) = \begin{cases} 1 & \text{se } n \equiv a \pmod{q} \\ 0 & \text{altrimenti.} \end{cases}$$

A partire da tale relazione (che si dimostra facilmente) possiamo valutare le **somme di Ramanujan**

$$(2.13) \quad c_q(n) \stackrel{def}{=} \sum_{\substack{j \leq n \\ (j,q)=1}} e_q(jn);$$

infatti

$$c_q(n) = \sum_{d|q} \sum_{\substack{j \leq n \\ (j,q)=d}} e_q(jn)$$

e tramite la formula di inversione di Möbius otteniamo dalla 2.12

$$c_q(n) = \sum_{\substack{d|n \\ d|q}} d \mu\left(\frac{q}{d}\right)$$

dalla quale segue, in particolare, che $c_q(n)$ é una funzione moltiplicativa rispetto a q per ogni n fissato; valutandola sulle potenze dei primi otteniamo infine

$$(2.14) \quad c_q(n) = \frac{\mu(q/(n,q))\phi(q)}{\phi(q/(n,q))}.$$

2.4.2 Caratteri Moltiplicativi e Teorema di Dirichlet

Si può dimostrare il teorema di Euclide tramite l'Identità di Eulero 1.14, come fece lo stesso matematico svizzero Leonhard Euler nel 1737, facendo tendere $s \rightarrow 1^+$ e sfruttando la divergenza della serie armonica.

Tale argomento fu ripreso da Peter Gustav Lejeune Dirichlet per dimostrare il suo famoso Teorema sull'infinità dei primi nelle progressioni aritmetiche non banali (v. seguito) nel suo memoriale del 1837, che segna l'inizio della Teoria Analitica dei Numeri (sta di fatto che è anche l'unico teorema, ancora oggi, sulla rappresentabilità di infiniti primi tramite un polinomio).

I **Caratteri di Dirichlet (o Caratteri Moltiplicativi)**, $\chi(\text{mod } q)$ si possono definire come funzioni aritmetiche moltiplicative e di periodo q , nulle sui naturali non coprimi con q , ma non identicamente nulle (per maggiori dettagli si vedano i capitoli 1 e 4 del [D]).

Si dice **principale** il carattere $\chi_0(\text{mod } q)$ definito da:

$$(2.15) \quad \chi_0(n) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{se } (n, q) = 1, \\ 0 & \text{altrimenti,} \end{cases}$$

primitivo un carattere χ tale che:

$$(2.16) \quad \chi : \mathbf{N} \rightarrow \mathbf{C} \quad \text{non ha periodo } q_1, \quad \forall q_1 < q;$$

(per comodità considereremo il carattere principale né primitivo, né non primitivo)

e **reale** un carattere $\chi : \mathbf{N} \rightarrow \mathbf{R}$.

Si può dimostrare che:

i) per ogni $q \in \mathbf{N}$ esistono esattamente $\phi(q)$ caratteri $\chi(\text{mod } q)$ (ϕ è la funzione di Eulero def. nel §1.1.2);

ii) $|\chi(n)| > 0 \Leftrightarrow \chi(n)$ è una radice dell'unità (e quindi $|\chi(n)| = 1$);

iii) $\chi(mn) = \chi(m)\chi(n) \quad \forall m, n \in \mathbf{N} \quad \forall \chi(\text{mod } q) \quad \forall q \in \mathbf{N}$ (**i caratteri di Dirichlet sono funzioni aritmetiche completamente moltiplicative**).

Valgono, inoltre, le **relazioni di ortogonalità** fra caratteri ([D], cap. 4):

$$(2.17) \quad \sum_{n=1}^q \chi(n) = \begin{cases} \phi(q) & \text{se } \chi = \chi_0, \\ 0 & \text{altrimenti} \end{cases}$$

(per la periodicità dei $\chi(\text{mod } q)$ la somma può essere fatta rispetto a un qualunque insieme completo di resti mod q)

e:

$$(2.18) \quad \sum_{\chi(\bmod q)} \chi(n) = \begin{cases} \phi(q) & \text{se } n \equiv 1(\bmod q), \\ 0 & \text{altrimenti} \end{cases}$$

(la somma é estesa a tutti i $\phi(q)$ caratteri $\chi(\bmod q)$).

Tramite la 2.18 si può costruire una somma che dà la funzione caratteristica della classe di resto $a(\bmod q)$:

$$(2.19) \quad \frac{1}{\phi(q)} \sum_{\chi(\bmod q)} \bar{\chi}(a) \chi(n) = \begin{cases} 1 & \text{se } n \equiv a(\bmod q), \\ 0 & \text{altrimenti;} \end{cases}$$

sta di fatto che tale relazione consente di scegliere i primi $p \equiv a(\bmod q)$ per dimostrare il

TEOREMA 2.5 (DI DIRICHLET SULLE PROGRESSIONI ARITMETICHE). *Sia $q \in \mathbf{N}$ ed a un intero coprimo con q . Allora la progressione aritmetica non banale $\{qn+a : n \in \mathbf{N}\}$ contiene infiniti primi.*

Vediamo un breve sketch della dimostrazione.

Innanzitutto, dalla 1.15 segue che $|L(s, \chi)| > 0$ in $s > 1$:

$$\log L(s, \chi) = \sum_{m=1}^{\infty} m^{-1} \sum_p \chi(p^m) p^{-ms}$$

che, per 2.19, dà (d' ora in poi $n \equiv r(q)$ sta per $n \equiv r(\bmod q)$)

$$(2.20) \quad \frac{1}{\phi(q)} \sum_{\chi(\bmod q)} \bar{\chi}(a) \log L(s, \chi) = \sum_{m=1}^{\infty} m^{-1} \sum_{\substack{p \\ p^m \equiv a(q)}} p^{-ms}.$$

Essendo, per $s > 1$

$$\sum_{m=2}^{\infty} m^{-1} \sum_{\substack{p \\ p^m \equiv a(q)}} p^{-ms} \ll \sum_{m=2}^{\infty} \sum_p p^{-m} \ll \sum_p \sum_{m=2}^{\infty} p^{-m} \ll 1,$$

si ha che (per 2.20)

$$\frac{1}{\phi(q)} \sum_{\chi(\bmod q)} \bar{\chi}(a) \log L(s, \chi) = \sum_{\substack{p \\ p \equiv a(q)}} p^{-s} + \mathcal{O}(1);$$

poichè al primo membro il termine dovuto al carattere principale é la funzione ζ per una costante (cfr. §1.1.4), esso diverge per $s \rightarrow 1^+$; per dimostrare la divergenza di tutto il primo membro (per $s \rightarrow 1^+$), Dirichlet

dimostrò che $L(1, \chi)$ non si annulla per tutti i $\chi(\bmod q)$ non principali tramite la sua **Formula per il numero di classi**.

Tale risultato, di fatto, dimostra anche la seguente relazione asintotica

$$\frac{\sum_{p \leq x, p \equiv a(q)} p^{-s}}{\sum_{p \leq x} p^{-s}} \rightarrow \frac{1}{\phi(q)}, \quad x \rightarrow \infty.$$

Definiamo la **somma di Gauss** $\tau(\chi)$ relativa a χ ($q > 1$ é un intero fissato):

$$(2.21) \quad \tau(\chi) \stackrel{def}{=} \sum_{m=1}^q \chi(m) e_q(m) \quad \forall \chi(\bmod q)$$

dove $e_q(n) \stackrel{def}{=} e^{(2\pi i n)/q}$.

Si possono dimostrare ([D], cap. 9), per $\chi(\bmod q)$ primitivo, le :

$$(2.22) \quad \chi(n) \tau(\bar{\chi}) = \sum_{h=1}^q \bar{\chi}(h) e_q(nh)$$

e :

$$(2.23) \quad |\tau(\chi)| = q^{1/2}.$$

Inoltre, per ogni carattere $\chi(\bmod q)$ non principale

$$(2.24) \quad |\tau(\chi)| \leq q^{1/2}.$$

Dalla 2.17 segue, in particolare, che $\forall N \in \mathbf{Z}, \forall M \in \mathbf{N}$

$$\left| \sum_{n=N}^{N+M} \chi(n) \right| \leq q \quad \text{se } \chi \text{ non é principale}$$

(stima banale), che si può notevolmente migliorare. Infatti vale la

DISUGUAGLIANZA DI POLYA-VINOGRADOV. *Per ogni carattere $\chi(\bmod q)$ ($q > 1$) non principale si ha, $\forall N \in \mathbf{Z}, \forall M \in \mathbf{N}$*

$$\sum_{n=N}^{N+M} \chi(n) \ll q^{1/2} \log q.$$

2.4.3 Teorema dei Numeri Primi nelle Progressioni

Definiamo la funzione che "conta" (con peso logaritmico) i primi nella progressione aritmetica $qn + a$:

$$(2.25) \quad \psi(x; q, a) \stackrel{\text{def}}{=} \sum_{n \equiv a(q)} \Lambda(n),$$

per la quale valgono i seguenti due risultati (**Teorema dei Numeri Primi per le Progressioni Aritmetiche**). Il primo é un risultato effettivo (ovvero si può trovare la costante c)

PROPOSIZIONE 2.2. *Fissato $\delta \in]0, 1[$ abbiamo*

$$q \leq (\log x)^{1-\delta} \Rightarrow \psi(x; q, a) = \frac{x}{\phi(q)} + \mathcal{O}\left(x \exp(-c(\log^{1/2}(x)))\right)$$

dove c é una costante assoluta (computabile).

Il miglior risultato di questo tipo, cioè uniforme rispetto al modulo q , é la seguente applicazione del Teorema di Siegel (v. sezioni precedenti)

TEOREMA 2.6 (DI SIEGEL-WALFISZ). *Data $A > 0$, $\exists C = C(A)$ tale che*

$$q \leq (\log x)^A \Rightarrow \psi(x; q, a) = \frac{x}{\phi(q)} + \mathcal{O}\left(x \exp(-C(A)(\log^{1/2}(x)))\right),$$

uniformemente in q .

A causa degli argomenti non costruttivi nella dimostrazione del Teorema di Siegel, $C(A)$ e la costante implicita nell' " \mathcal{O} " non sono computabili, per cui il Teorema di Siegel-Walfisz non é "effettivo".

Ciononostante si rivela uno strumento prezioso per la stima dei contributi sugli archi maggiori, che compaiono nel Metodo del Cerchio (v. cap. 3).

2.5 Teorema di Bombieri

Il **Teorema di Bombieri** é una (notevole) conseguenza del Teorema di Siegel-Walfisz e del Crivello Largo (perciò non é effettivo); descrive il valore medio del resto

$$E^*(x, q) \stackrel{def}{=} \max_{\substack{a \leq q \\ (a, q) = 1}} \max_{y \leq x} \left| \psi(y; q, a) - \frac{y}{\phi(q)} \right|$$

calcolato sui moduli $q \leq Q$ (cfr. [D], cap. 28):

TEOREMA 2.7 (BOMBIERI). *Per ogni $A > 0$, esiste $B = B(A) > 0$ tale che, per $Q \leq x^{\frac{1}{2}}(\log x)^{-B}$, si ha*

$$(2.26) \quad \sum_{q \leq Q} E^*(x, q) \ll x(\log x)^{-A},$$

con, ad esempio, $B = 3A + 23$ (v. [B(2)]).

(In seguito, valori migliori di $B = B(A)$ sono stati dati, ad es., da Gallagher [Ga(2)], $B = 16A + 103$, e da Vaughan [Va(2)], $B = A + 7/2$).

Il Teorema di Bombieri equivale ad avere, in media sui moduli, la stima

$$\psi(x; q, a) - \frac{x}{\phi(q)} \ll x^{1/2} \log^2 x$$

che segue da GRH (v. §1.3.3).

Il Teorema di Bombieri si dimostra utilizzando il Teorema di Siegel - Walfisz (v. §2.4.3) ed il Crivello Largo (v. §4.3); tali strumenti si possono, però, utilizzare in modo diverso per ottenere varie dimostrazioni. Ad esempio, si può utilizzare (v. [Hu(1)], cap.24, o l' articolo di Bombieri, cit.) il Crivello Largo per trovare stime sul numero di zeri delle funzioni L ; oppure (come su [D], cit.) il Teorema di Siegel - Walfisz sui moduli "piccoli" (appunto $q \leq \log^N x$) e il Crivello Largo sui restanti, dopo aver stimato le forme bilineari che si ottengono dall' identità di Vaughan per la funzione Λ

$$(2.27) \quad \Lambda(n) = a_1(n) + a_2(n) + a_3(n) + a_4(n),$$

con:

$$a_1(n) \stackrel{def}{=} \begin{cases} \Lambda(n) & \text{se } n \leq U \\ 0 & \text{se } n > U, \end{cases}$$

$$\begin{aligned}
a_2(n) &\stackrel{def}{=} - \sum_{\substack{m d r = n \\ m \leq U \\ d \leq V}} \Lambda(m) \mu(d), \\
a_3(n) &\stackrel{def}{=} \sum_{\substack{h d = n \\ d \leq V}} \mu(d) \log(h), \\
a_4(n) &\stackrel{def}{=} - \sum_{\substack{m k = n \\ m > U \\ k > 1}} \Lambda(m) \sum_{\substack{d | k \\ d \leq V}} \mu(d).
\end{aligned}$$

Tale identità (combinatoria) segue dalla identità per le corrispondenti serie di Dirichlet

$$F(s) \stackrel{def}{=} \sum_{m \leq U} \Lambda(m) m^{-s}, \quad G(s) \stackrel{def}{=} \sum_{d \leq V} \mu(d) d^{-s},$$

ovvero, nel semipiano $\sigma > 1$ vale l' **Identità di Vaughan** (v. [Va(3)])

$$-\frac{\zeta'}{\zeta}(s) = F(s) - \zeta(s) F(s) G(s) - \zeta'(s) G(s) - \left(\frac{\zeta'}{\zeta}(s) + F(s) \right) (1 - \zeta(s) G(s)).$$

Analogamente, vale l' **Identità di Heath - Brown** in $\sigma > 1$ e per ogni numero naturale k (v. Lemma 1 in [HB])

$$-\frac{\zeta'}{\zeta}(s) = \sum_{j=1}^k (-1)^j \binom{k}{j} \zeta(s)^{j-1} \zeta'(s) G(s)^j - \zeta(s)^{-1} (1 - \zeta(s) G(s))^k \zeta'(s),$$

dalla quale si ha la corrispondente identità combinatoria per la Λ .

Tramite quest' identità Perelli, Pintz e Salerno hanno generalizzato il Teorema di Bombieri, in modo da ottenere una stima analoga negli intervalli corti (v. [P-P-S(1)] e [P-P-S(2)]).

Capitolo 3

Problemi Additivi

3.1 Problemi Additivi

I problemi additivi sono problemi del tipo:

dato un intero n , ed r insiemi A_1, A_2, \dots, A_r (di interi),

determinare il numero $\nu(n)$ di soluzioni dell'equazione:

$$n = n_1 + n_2 + \dots + n_r, \text{ con } n_i \in A_i;$$

in particolare ci si può interessare ai valori $\nu(n)$, per n "grande", ovvero maggiore di un certo intero N (spesso si ha un risultato puramente esistenziale).

Ad esempio, si può supporre che tutti gli A_j ($j = 1, \dots, s$) siano il sottinsieme di \mathbf{N} delle potenze s -sime; si sta studiando, allora, il **Problema di Waring** (ha avuto origine da due congetture del 1770 di Edward Waring) trovare il numero di rappresentazioni di un naturale come somma di s potenze k -sime.

Definendo le quantità $g(k)$ e $G(k)$:

$$(3.1) \quad g(k) \stackrel{def}{=} \min\{s : \forall n \in \mathbf{N} \exists m_1, \dots, m_s \in \mathbf{N}, n = m_1^k + \dots + m_s^k\}$$

$$G(k) \stackrel{def}{=} \min\{s : \exists N \in \mathbf{N} : \forall n > N \exists m_1, \dots, m_s \in \mathbf{N}, n = m_1^k + \dots + m_s^k\}$$

il *problema di Waring* consiste nella ricerca di $g(k)$ e $G(k)$; Waring ipotizzò che $g(3) = 9$ e $g(4) = 19$ (quest'ultimo dimostrato di recente da Balasubramanian, Deshouillers e Dress, v. [B-D-D]).

Da considerazioni elementari si ha (con $[x]$ parte intera di x) :

$$g(k) \geq 2^k + \left[\left(\frac{3}{2} \right)^k \right] - 2;$$

sappiamo inoltre che $g(4) = 19$ (v. sopra).

Per k diverso da 4, è stato dimostrato ($\{ \}$ sta per parte frazionaria):

$$2^k \left\{ \left(\frac{3}{2} \right)^k \right\} + \left[\left(\frac{3}{2} \right)^k \right] \leq 2^k \Leftrightarrow g(k) = 2^k + \left[\left(\frac{3}{2} \right)^k \right] - 2$$

e, se k non verifica tale ipotesi, si ha $g(k)$ pari a:

$$2^k + \left[\left(\frac{3}{2} \right)^k \right] + \left[\left(\frac{4}{3} \right)^k \right] - 2 \text{ oppure } 2^k + \left[\left(\frac{3}{2} \right)^k \right] + \left[\left(\frac{4}{3} \right)^k \right] - 3$$

secondo che:

$$\left[\left(\frac{4}{3} \right)^k \right] \left[\left(\frac{3}{2} \right)^k \right] + \left[\left(\frac{4}{3} \right)^k \right] + \left[\left(\frac{3}{2} \right)^k \right]$$

sia uguale a 2^k oppure maggiore di 2^k .

I valori $g(k)$ sono quindi tutti noti, poichè g dipende dal comportamento di pochi naturali non molto grandi; $G(k)$ è invece molto più difficile da calcolare.

I migliori risultati per G sono:

$$G(4) = 16 \quad (\text{H. Davenport, 1942})$$

$$G(k) \leq k(\log k)(2 + o(1)) \quad (\text{I. M. Vinogradov, 1959}).$$

Altre questioni additive sono (ad esempio) le equazioni diofantee omogenee, le disequazioni diofantee e le progressioni aritmetiche negli insiemi di naturali.

Il Metodo del Cerchio (v. §3.3 e §3.4) ha innumerevoli applicazioni ai problemi additivi (v., ad es., §3.5 e §3.6; anche, [Va(1)]).

3.2 Problemi di Goldbach

In una lettera ad Eulero del 1742 Christian Goldbach ipotizzava che ogni numero pari é somma di due primi e ogni numero dispari é somma di tre primi; egli includeva 1 fra i primi, per cui le versioni moderne della *Congettura di Goldbach* sono:

- 1) (**Congettura Binaria di Goldbach**) ogni $n > 2$ pari é somma di due primi;
- 2) (**Congettura Ternaria di Goldbach**) ogni $n > 5$ dispari é somma di tre primi.

Il migliore risultato per la congettura ternaria fu ottenuto nel 1937 da I. M. Vinogradov, col famoso Teorema dei Tre Primi (v. §3.5), che dimostra la 2) per ogni dispari n abbastanza grande.

Il Teorema fu il risultato del raffinamento da parte di Vinogradov (cfr. §2.4 e §2.5) del metodo di Hardy e Littlewood (§2.1); essi per primi dimostrarono, nel 1923, la 1) per quasi tutti i pari abbastanza grandi ed il Teorema, assumendo l' Ipotesi di Riemann Generalizzata (*G.R.H.*) (v. §1.3.3); tale Ipotesi era richiesta per trattare gli archi minori.

Vinogradov utilizzò invece a tal fine il suo metodo delle somme esponenziali, ideato intorno alla fine degli anni '20, dando una dimostrazione non condizionale del Teorema.

Per quanto riguarda la 1), il M.C. fornisce ancora una soluzione "per quasi tutti gli n pari abbastanza grandi" (cfr. cor. 2.3); la 1) é indicata, essendo ancora non provata, anche come **problema di Goldbach**.

Esistono altri approcci legati ai metodi di crivello (cfr. cap. 4) che dimostrano l' esistenza di un naturale N (non esplicitabile) tale che:

1-r) (*versione debole del problema di Goldbach*)

ogni pari $n > N$ é somma di un primo e di un quasi-primo P_r ,

dove un **quasi-primo** P_r é per definizione un naturale che é prodotto di al più r primi (distinti o non).

É evidente che la cong. 1) é data dalla 1-r) per $r = 1$; pertanto si deve rendere r minimo per avvicinare 1-r) ad 1).

Nel 1948, Renyi, utilizzando metodi di crivello, dimostrò che esiste un $r \in \mathbf{N}$, fissato, per il quale é vera la 1 - r).

Nel 1966, Chen ha trovato (con i più sofisticati metodi di crivello) il miglior risultato per la versione debole 1- r), dimostrandola per $r = 2$; il teorema di Chen ci assicura, quindi, che ogni pari abbastanza grande é somma di un primo e di un P primo o prodotto di due primi (v. ad es. [H-R]).

3.3 Metodo di Hardy-Littlewood

Il metodo delle somme trigonometriche (anche detto **Metodo di Hardy-Littlewood**, abbrev. metodo H-L) ebbe origine da un articolo di G. H. Hardy e S. Ramanujan del 1918, nel quale veniva trattato il problema del numero $R_s(n)$ di rappresentazioni di un naturale n come somma di s quadrati (e, più in generale, come somma di s potenze k -sime: cfr. §3.1).

Hardy e Ramanujan consideravano la funzione:

$$F(z) = \sum_{m=1}^{\infty} z^{a_m} \quad (|z| < 1)$$

relativa alla successione $(a_m)_{m \in \mathbf{N}}$ strettamente crescente, dalla quale si ottiene:

$$F(z)^s = \sum_{m_1=1}^{\infty} \sum_{m_2=1}^{\infty} \dots \sum_{m_s=1}^{\infty} z^{a_{m_1} + \dots + a_{m_s}} = \sum_{n=0}^{\infty} R_s(n) z^n,$$

dove $R_s(n)$ è il numero di rappresentazioni di n come somma di s elementi di $(a_m)_{m \in \mathbf{N}}$ (quest'ultima è strettamente crescente, quindi le rappresentazioni diverse solo per l'ordine degli addendi sono contate come una); essi trattavano poi, in particolare, il caso $a_m = m^2$.

Per la stima di $R_s(n)$ si può impiegare la formula di Cauchy, con C circonferenza di centro 0 e raggio $0 < \rho < 1$ del piano complesso:

$$(3.2) \quad R_s(n) = \frac{1}{2\pi i} \int_C F(z)^s z^{-n-1} dz \quad \forall n \in \mathbf{N} \quad \forall s \in \mathbf{N}$$

(per questo motivo si parla anche di **Metodo del Cerchio**).

Hardy e Ramanujan scoprirono che la funzione F (analitica all'interno di C , ma con un insieme denso di singolarità su C) ha un'espressione asintotica in $z = \rho(\alpha)$ ($0 < \rho < 1$ ed $\alpha \in [-1/2, 1/2]$) "vicino" ad uno dei punti di C , (a/q) , per il quale q è "abbastanza piccolo"; ovvero, se $\rho = 1 - 1/n$, con n "grande" e si ha $\beta = \alpha - a/q$ piccolo (con q opportunamente piccolo), allora vale la:

$$(3.3) \quad F(\rho e(\frac{a}{q} + \beta)) \sim \frac{c}{q} S(q, a) (1 - \rho e(\beta))^{-1/2}$$

(c è una costante opportuna, F si riferisce ad $a_m = m^2$,

$$S(q, a) \stackrel{def}{=} \sum_{m \leq q} e_q(am^2)$$

e la somma parte da $m = 1$).

Per il teorema di approssimazione di Dirichlet ogni $\alpha \in [-1/2, 1/2]$ é "vicino" ad un opportuno a/q (v. [Va(1)]), per cui la (2.1.4) vale per tutti gli α in $[-1/2, 1/2]$ (nel caso dei quadrati).

Dalle 3.2 e 3.3 si ha quindi (per $s \geq 5$):

$$R_s(n) \sim \mathfrak{S}_s(n) J_s(n),$$

dove \mathfrak{S}_s é la **serie singolare**:

$$\mathfrak{S}_s(n) \stackrel{def}{=} \sum_{q=1}^{\infty} \sum_{\substack{a \leq q \\ (a,q)=1}} q^{-s} S(q, a)^s e_q(-an)$$

e J_s é l' **integrale singolare**:

$$J_s(n) \stackrel{def}{=} c^s \int_{-1/2}^{1/2} (1 - \rho e(\beta))^{-s/2} \rho^{-n} e(-n\beta) d\beta.$$

(La serie e l' integrale qui definiti si riferiscono alla particolare successione dei quadrati; ogni successione $(a_m)_{m \in \mathbf{N}}$ ha la propria serie singolare ed il proprio integrale singolare: cfr. le sezioni seguenti).

Hardy, insieme a J. E. Littlewood, applicò la stessa linea di ragionamento ad $a_m = m^k$, con $k \geq 3$, per avere informazioni sul numero $R_s(n)$ di rappresentazioni di n come somma di s potenze k -sime; lo sviluppo della F corrispondente valeva, però, non su tutta la circonferenza C , ma solo su tratti di questa, che furono detti **archi maggiori**; le parti rimanenti di C essendo gli **archi minori** (si noti che "minori" non é riferito alla misura, che, anzi, nella maggior parte dei casi é proprio asintoticamente 1; ma al contributo che essi danno al numero di rappresentazioni).

C' era bisogno, quindi, di una stima di F sugli archi minori; questa fu data, per $a_m = m^k$ ($k \geq 3$), dal lemma di Weyl (cfr. [Ti], cap.6).

3.4 Metodo di Vinogradov

Alla fine degli anni '20 il metodo H-L fu perfezionato da Vinogradov, il quale sostituì ad F la *somma trigonometrica*:

$$f(\alpha) \stackrel{def}{=} \sum_{m \leq N} e(m^k \alpha), \quad \text{con } N = [n^{1/k}];$$

di qui l'altro nome di **Metodo delle Somme Trigonometriche**; è più usato, però, "Metodo del Cerchio" (abbrev. **M.C.**).

Si ha subito che:

$$f(\alpha)^s = \sum_{m \leq sn} R_s(m, n) e(m\alpha)$$

dove $R_s(m, n)$ è il numero di rappresentazioni di n come somma di s potenze k -sime, nessuna delle quali supera n ; se $R_s(m)$ è lo stesso numero di rappresentazioni per m , senza vincoli, si ha:

$$m \leq n \Rightarrow R_s(m, n) = R_s(m);$$

poichè, banalmente, $\forall h \in \mathbb{Z}$ si ha:

$$(3.4) \quad \int_0^1 e(h\alpha) d\alpha = \begin{cases} 1 & \text{se } h = 0 \\ 0 & \text{altrimenti} \end{cases}$$

abbiamo:

$$R_s(n) = \int_0^1 f(\alpha)^s e(-n\alpha) d\alpha.$$

Per la stima di quest'integrale si procede come per il metodo H-L, dividendo l'intervallo di integrazione in archi maggiori e minori (si continua ad usare tale terminologia, nonostante adesso siano intervalli in $[0,1]$).

NOTA 3.1. Per la periodicità di f tutti gli integrali su un intervallo di lunghezza 1 rimangono invariati traslando l'intervallo d'integrazione.

Per un esempio del metodo di Vinogradov si veda la sezione seguente.

3.5 Teorema dei tre primi

Diamo ora l' applicazione migliore del metodo del cerchio: il **Teorema dei Tre Primi di Vinogradov** (Corollario a fine paragrafo).

Definiamo:

$$f(\alpha) \stackrel{def}{=} \sum_{p \leq n} (\log p) e(p\alpha);$$

per n abbastanza grande e $B > 0$, costante, sia $P \stackrel{def}{=} (\log n)^B$; quindi gli **archi maggiori** relativi ad a/q , con $1 \leq a \leq q \leq P$ e $(a, q) = 1$:

$$\mathfrak{M}(q, a) \stackrel{def}{=} \{\alpha \in \mathcal{U} : |\alpha - a/q| \leq P/n\} \quad (\mathcal{U} \stackrel{def}{=}]P/n, 1 + P/n])$$

e la loro unione \mathfrak{M} (per n "grande" gli archi sono a due a due disgiunti); gli **archi minori** saranno dati da $\mathfrak{m} \stackrel{def}{=} \mathcal{U} \setminus \mathfrak{M}$.

Per la nota 3.1:

$$R(n) = \int_{\mathcal{U}} f(\alpha)^3 e(-n\alpha) d\alpha = \int_{\mathfrak{M}} f(\alpha)^3 e(-n\alpha) d\alpha + \int_{\mathfrak{m}} f(\alpha)^3 e(-n\alpha) d\alpha$$

dove adesso:

$$(3.5) \quad R(n) \stackrel{def}{=} \sum_{\substack{p_1, p_2, p_3 \\ p_1 + p_2 + p_3 = n}} (\log p_1)(\log p_2)(\log p_3).$$

Vedremo dapprima come stimare l' integrale sugli archi minori tramite il Teorema 3.1, che si serve del seguente:

LEMMA 3.1. *Siano $\alpha, X, Y \in \mathbf{R}$ con $X, Y \geq 1$; $(a, q) = 1$, $|\alpha - a/q| \leq \frac{1}{q^2}$. Allora:*

$$\sum_{x \leq X} \min(XYx^{-1}, \|\alpha x\|^{-1}) \ll XY \left(\frac{1}{q} + \frac{1}{Y} + \frac{q}{XY} \right) \log(2Xq).$$

TEOREMA 3.1. (I. M. VINOGRADOV) Sia $(a, q) = 1$, $q \leq n$ e $|\alpha - a/q| \leq q^{-2}$; allora:

$$(3.6) \quad f(\alpha) \ll (\log n)^4 (nq^{-1/2} + n^{4/5} + n^{1/2}q^{1/2}).$$

Per stimare l' integrale: $\int_{\mathbf{m}} f(\alpha)^3 e(-n\alpha) d\alpha$ osserviamo che, per l' identità di Parseval ed il Teorema dei Numeri Primi (usiamo di meno : $\psi(x) \ll x$: cfr. §2.2.1 e §2.2.2), si ha:

$$\int_0^1 |f(\alpha)|^2 d\alpha = \sum_{p \leq n} (\log p)^2 \ll n \log n.$$

Come per la dimostrazione del teorema 2.1 abbiamo:

$$\int_{\mathbf{m}} |f(\alpha)|^3 d\alpha \ll \left(\sup_{\alpha \in \mathbf{m}} |f(\alpha)| \right) \int_{\mathbf{m}} |f(\alpha)|^2 d\alpha;$$

da cui, per la nota 2.1 ed il Teorema 2.4, si ha il:

TEOREMA 3.2. (STIMA DI $R(n)$ SUGLI ARCHI MINORI) Se $A > 0$ e $B \geq 2A + 10$:

$$\int_{\mathbf{m}} f(\alpha)^3 e(-n\alpha) d\alpha \ll n^2 (\log n)^{-A}.$$

Per completare la stima di 3.5 ci occuperemo ora degli archi maggiori, per i quali dovremo impiegare la teoria dei primi nelle progressioni aritmetiche (cfr. §2.4.3) e le *somme di Ramanujan* (v. §2.4.1).

(Poichè useremo il Teorema di Siegel-Walfisz le costanti non saranno effettive, cfr. Teor. 2.6).

Definendo $v(\beta) \stackrel{def}{=} \sum_{m \leq n} e(m\beta)$, $\forall \beta \in \mathbf{R}$ ed $\exp(t) \stackrel{def}{=} e^t$, $\forall t \in \mathbf{R}$, si ha il

LEMMA 3.2. Se $1 \leq a \leq q \leq P$ e $(a, q) = 1$ allora $\exists C > 0$ tale che $\forall \alpha \in \mathfrak{M}(q, a)$

$$f(\alpha) = \frac{\mu(q)}{\phi(q)} v(\alpha - a/q) + \mathcal{O}(n \exp(-C(\log n)^{1/2})).$$

Definiamo la **serie singolare per il problema ternario di Goldbach**

$$(3.7) \quad \mathfrak{S}(n) \stackrel{\text{def}}{=} \sum_{q=1}^{\infty} \frac{\mu(q)}{\phi(q)^3} \sum_{\substack{a \leq q \\ (a,q)=1}} e_q(-an);$$

per la 2.14 questa sarà

$$\mathfrak{S}(n) = \sum_{q=1}^{\infty} \frac{\mu(q)}{\phi(q)^2} \frac{\mu(q/(n,q))}{\phi(q/(n,q))}.$$

Le proprietà aritmetiche del problema dei tre primi dipendono in tal modo da \mathfrak{S} ; tramite il Lemma 3.2 si ottiene infatti il:

TEOREMA 3.3. (STIMA DI $R(n)$ SUGLI ARCHI MAGGIORI) *Se $A > 0$ e $B \geq 2A$, allora :*

$$\int_{\mathfrak{M}} f(\alpha)^3 e(-n\alpha) d\alpha = \frac{1}{2} n^2 \mathfrak{S}(n) + \mathcal{O}(n^2 (\log n)^{-A}).$$

Dalla 3.7 si ottengono le relazioni:

$$(3.8) \quad n \text{ é dispari} \Rightarrow \mathfrak{S}(n) \gg 1,$$

$$(3.9) \quad n \text{ é pari} \Rightarrow \mathfrak{S}(n) = 0.$$

La stima dell' integrale su tutto \mathcal{U} segue dai Teoremi 3.2 e 3.3:

TEOREMA 3.4. (I. M. VINOGRADOV) *Sia $A > 0$ costante, $R(n)$ definita da 3.5 e da 3.5; allora:*

$$R(n) = \frac{1}{2} n^2 \mathfrak{S}(n) + \mathcal{O}(n^2 (\log n)^{-A}).$$

Per sommazione parziale e per la 3.8 abbiamo il:

COROLLARIO 3.1 (TEOREMA DEI TRE PRIMI DI VINOGRADOV). *Ogni numero dispari abbastanza grande é somma di tre primi.*

Si noti che, per la 3.9, il Teorema 3.4 non dà nessuna informazione riguardo al problema binario di Goldbach (v. par. seg.); mentre non solo dimostra la congettura ternaria, ma dà anche una stima asintotica per il numero di rappresentazioni di ogni dispari abbastanza grande come somma di tre primi.

Per le dimostrazioni di questa sezione, si veda [Va(1)] (in tutto il presente Capitolo ne seguiremo le notazioni, da non confondere con le notazioni, indipendenti, del §5.3).

Per un' esposizione delle principali varianti del Corollario 3.1 (che é detto anche **Teorema di Goldbach-Vinogradov**), si veda il recente articolo di Liu e Zhan [L-Z].

Vedremo, brevemente, nel prossimo paragrafo come ottenere informazioni sul problema di Goldbach (binario) utilizzando il Metodo del Cerchio; la stima che si otterrà dimostra solo che la congettura é vera per "**quasi tutti**" i pari abbastanza grandi.

3.6 Metodo del Cerchio e Problema di Goldbach

Il metodo del cerchio fornisce, per il problema binario di Goldbach, solo una stima non banale di:

$$\sum_{m \leq n} (R_1(m) - m \mathfrak{S}_1(m))^2,$$

dove, per $m \leq n$:

$$R_1(m) = R_1(m, n) \stackrel{def}{=} \sum_{\substack{p_1, p_2 \leq n \\ p_1 + p_2 = m}} (\log p_1)(\log p_2)$$

e:

$$\mathfrak{S}_1(m) \stackrel{def}{=} \sum_{q=1}^{\infty} \frac{\mu(q)^2}{\phi(q)^2} \sum_{\substack{a \leq q \\ (a, q) = 1}} e_q(-am).$$

Come nel paragrafo precedente abbiamo:

$$R_1(m) = R_2(m) + R_3(m),$$

dove:

$$R_2(m) \stackrel{def}{=} \int_{\mathfrak{M}} f(\alpha)^2 e(-n\alpha) d\alpha$$

e:

$$R_3(m) \stackrel{def}{=} \int_{\mathfrak{m}} f(\alpha)^2 e(-n\alpha) d\alpha.$$

R_3 é il coefficiente della serie di Fourier della funzione che vale $f(\alpha)^2$ su \mathfrak{m} e 0 altrove; per la disuguaglianza di Bessel:

$$\sum_{m \leq n} |R_3(m)|^2 \leq \int_{\mathfrak{m}} |f(\alpha)|^4 d\alpha.$$

Quest' ultima disuguaglianza, insieme agli argomenti del teorema 3.2, dimostra il:

TEOREMA 3.5. (STIMA DI R_1 SUGLI ARCHI MINORI) Se $A > 0$ e $B \geq A + 9$, allora :

$$\sum_{m \leq n} |R_3(m)|^2 \ll n^3 (\log n)^{-A}.$$

Per le stime elementari (cfr. [Va(1)] e [Te]):

$$\int_{P/n}^{1/2} |v(\beta)|^2 d\beta \ll \frac{n}{P} \text{ (per def. di } v) \text{ e: } \sum_{q \leq P} \phi(q)^{-1} \ll \log n$$

si ha, con:

$$\mathfrak{S}_1(m, P) \stackrel{\text{def}}{=} \sum_{q \leq P} \frac{\mu(q)^2}{\phi(q)^2} \sum_{\substack{a \leq q \\ (a, q) = 1}} e_q(-am),$$

la stima :

$$R_2(m) = \mathfrak{S}_1(m, P) J_1(m) + \mathcal{O}(n(\log n)^{1-B});$$

ma questa volta:

$$J_1(m) \stackrel{\text{def}}{=} \int_{-1/2}^{1/2} v(\beta)^2 e(-n\beta) d\beta$$

é il numero di soluzioni dell' equazione:

$$m_1 + m_2 = n, \quad 1 \leq m_1, m_2 \leq n$$

cioè

$$J_1(m) = m - 1, \quad \text{se } m \leq n.$$

La (2.4.38) dà $\phi(n)^{-2}/n^{2\delta-2} \rightarrow 0$ per $n \rightarrow \infty$, da cui: $\sum_{q > Z} \phi(q)^{-2} \ll \frac{1}{Z}$; quest' ultima, insieme all' espressione di R_2 , dimostra il:

TEOREMA 3.6. (STIMA DI R_1 SUGLI ARCHI MAGGIORI) Se $A > 0$ e $B \geq A + 2$, allora :

$$\sum_{m \leq n} |R_2(m) - m \mathfrak{S}_1(m)|^2 \ll n^3 (\log n)^{-A}.$$

Per i teoremi precedenti abbiamo quindi il:

TEOREMA 3.7 (STIMA DI R_1). Per ogni $A > 0$ abbiamo

$$\sum_{m \leq n} |R_1(m) - m\mathfrak{S}_1(m)|^2 \ll n^3(\log n)^{-A}.$$

Stavolta, per quanto riguarda la serie singolare, abbiamo

$$\mathfrak{S}_1(m) = \prod_p (1 - (p-1)^{-2}) \prod_{p|m} (1 + (p-1)^{-1}),$$

(il primo prodotto é sui primi che non dividono m), da cui:

$$m \text{ pari} \Rightarrow \mathfrak{S}_1(m) \gg 1,$$

$$m \text{ dispari} \Rightarrow \mathfrak{S}_1(m) = 0;$$

perciò la congettura binaria vale "per quasi tutti i pari $n \leq N$ ", ovvero per tutti, tranne $o(N)$ di essi; definiamo, infatti, l' **insieme eccezionale per il problema binario di Goldbach** :

$$E(n) \stackrel{def}{=} |\{m \leq n : m \text{ é pari e non é somma di due primi}\}|.$$

Chudakov, Estermann e van der Corput (cfr. [Va(1)]) dimostrarono (indipendentemente) il seguente risultato (che segue dal Teorema 3.7 grazie a quanto detto sulla serie singolare \mathfrak{S}_1):

COROLLARIO 3.2 (STIMA PER L' INSIEME ECCEZIONALE NELLA CONGETTURA BINARIA DI GOLDBACH). Per ogni $A > 0$ abbiamo

$$E(n) \ll n(\log n)^{-A}.$$

La stima migliore possibile sull' insieme eccezionale per il Problema di Goldbach é dovuta a Montgomery e Vaughan (risultato del 1975, v. [M-V])

PROPOSIZIONE 3.1 (MONTGOMERY-VAUGHAN). Esiste una costante assoluta $\delta > 0$, computabile, tale che

$$E(n) \ll n^{1-\delta}.$$

Capitolo 4

Crivello e Somme Esponenziali

4.1 Crivello e Somme Esponenziali

In questo Paragrafo diamo l'idea generale che é alla base dei metodi di Crivello, di cui daremo una breve rassegna nei prossimi due Paragrafi, e la definizione generale di Somma Esponenziale.

La nostra definizione di ”**Crivello Aritmetico**” segue quella data da Halberstam e Richert nel loro ”Sieve Methods” [H-R].

Nell'ambito dei ”Metodi di Crivello” \mathcal{A} non indica piú l'insieme delle funzioni aritmetiche, ma un sottinsieme finito dei numeri naturali $\mathcal{A} \subseteq \mathbf{N}$; e $\mathcal{B} \subseteq \mathbf{P}$ un sottinsieme (eventualmente infinito) dei numeri primi. Definito

$$P(z) = \prod_{\substack{p < z \\ p \in \mathcal{B}}} p,$$

vogliamo stimare, diciamo, $S(\mathcal{A}, \mathcal{B}, z)$, il numero di elementi di \mathcal{A} che restano dopo aver tolto tutti quelli divisibili per almeno un primo di \mathcal{B} minore di z ; ovvero definiamo

$$S(\mathcal{A}; \mathcal{B}, z) \stackrel{def}{=} |\{a \in \mathcal{A} : (a, P(z)) = 1\}|,$$

che rappresenta, quindi, il numero di elementi di \mathcal{A} rimasti dopo tale operazione di ”crivello”.

I Metodi di Crivello stimano appunto la quantità $S(\mathcal{A}; \mathcal{B}, z)$ (che viene detta anche **sifting function**, ovvero ”funzione di crivello”) oppure quantità pesate ad essa collegate.

Si definisce **somma esponenziale** una somma di $N \in \mathbf{N}$ numeri complessi dipendenti da $M \in \mathbf{Z}$, da $\alpha \in \mathbf{R}$, e da una successione $\{a_n\}_{n \in \mathbf{N}}$ (di numeri complessi)

$$S(\alpha) \stackrel{def}{=} \sum_{n=M+1}^{M+N} a_n e(n\alpha), \quad \text{dove } e(\beta) \stackrel{def}{=} e^{2\pi i \beta} \quad \forall \beta \in \mathbf{R}.$$

4.2 Crivello Piccolo

Nel presente paragrafo diamo una breve rassegna dei principali metodi di Crivello "Piccolo", ovvero metodi in cui si considera il numero di fattori primi di q , $\omega(q)$, "piccolo" rispetto alle grandezze di riferimento (di solito, la lunghezza dell'intervallo: x per gli intervalli "lunghi", h per i "corti": v. §5.4, §5.5, §5.6); in particolare, vedremo il Crivello di Eratostene-Legendre, il Crivello Combinatorio di Brun ed il Crivello di Selberg (nel seguito, $\omega(q)$ indicherà sia la funzione "numero di fattori primi", sia una generica funzione aritmetica; la scelta sarà chiara dal contesto).

4.2.1 Crivello di Eratostene-Legendre

La prima idea di crivello viene attribuita ad Eratostene (III sec. a.C.), il quale si accorse che, togliendo dall'intervallo $[z, z^2[$ (con $z \geq 2$ intero) successivamente i multipli dei primi 2, 3, 5, ..., gli interi sopravvissuti a quest'operazione di "crivello" erano necessariamente primi.

Tale algoritmo di ricerca dei primi, conosciuto sin dal XIII sec.d.C., venne trasformato da Legendre nella seguente formula

$$(4.1) \quad \pi(x) - \pi(\sqrt{x}) + 1 = \sum_{d|P(\sqrt{x})} \mu(d) \left[\frac{x}{d} \right],$$

dove (come sempre, p indicherà un primo)

$$P(z) \stackrel{def}{=} \prod_{p < z} p.$$

Più in generale, dalla definizione di sifting function e dalla proprietà (1.1) della funzione di Möbius segue infatti che ($n \equiv 0 \pmod{q}$ sarà indicato con $n \equiv 0(q)$ nel seguito)

$$S(\mathcal{A}; \mathcal{B}, z) = \sum_{a \in \mathcal{A}} \sum_{\substack{d|a \\ d|P(z)}} \mu(d) = \sum_{d|P(z)} \mu(d) \sum_{\substack{a \in \mathcal{A} \\ a \equiv 0(d)}} 1 = \sum_{d|P(z)} \mu(d) |\mathcal{A}_d|,$$

avendo posto

$$\mathcal{A}_d = \{a \in \mathcal{A} : a \equiv 0(d)\}.$$

Con una buona approssimazione per quest'ultima quantità si può sperare di ottenere delle buone stime per la sifting function.

A tale scopo, introduciamo le seguenti quantità:

$$X > 1, \quad r_1 \stackrel{def}{=} |\mathcal{A}| - X$$

in modo che r_1 sia piccolo (ovvero X è una buona approssimazione per $|\mathcal{A}|$) ed $\omega_0(p)$ tale che (\mathbf{P} è l'insieme dei primi)

$$r_p \stackrel{def}{=} |\mathcal{A}_p| - \frac{\omega_0(p)}{p} X \quad \forall p \in \mathbf{P}$$

sia piccolo (quindi $\frac{\omega_0(p)}{p} X$ è una buona approssimazione per $|\mathcal{A}_p|$).

Dopo aver definito le nostre approssimazioni sui primi p , definiamo in modo naturale ω_0 sugli **square-free** d (ovvero d non ha fattori quadrati; equivalentemente, $\mu(d)^2 = 1$):

$$\omega_0(1) \stackrel{def}{=} 1, \quad \omega_0(d) \stackrel{def}{=} \prod_{p|d} \omega_0(p) \quad (\mu(d)^2 = 1),$$

così che, per definizione, ω_0 è moltiplicativa; in maniera analoga definiamo

$$r_d \stackrel{def}{=} |\mathcal{A}_d| - \frac{\omega_0(d)}{d} X \quad (\mu(d)^2 = 1).$$

Ad esempio (cfr. example 1, p.16 [H-R]), se

$$\mathcal{A} = \{n : x - y < n \leq x\} \quad (1 < y \leq x)$$

abbiamo

$$|\mathcal{A}_d| = \frac{y}{d} + \theta, \quad |\theta| \leq 1,$$

da cui una buona approssimazione è data dalla scelta

$$X = y, \quad \omega(d) = 1 \quad \forall d \text{ square-free},$$

dato che sugli square-free otteniamo allora

$$|r_d| \leq 1.$$

Come altro esempio, supponiamo di avere come insieme \mathcal{A} l'insieme dei valori di un polinomio (a valori in \mathbf{N}) F , di grado g

$$\mathcal{A} = \{F(n) : x < n \leq x + h\}$$

(se $h = o(x)$ allora $[x, x + h]$ é un intervallo corto: v. §5.5).

Denotando con $\rho(d) = \rho_F(d)$ il numero di soluzioni distinte (mod d) della congruenza

$$F(n) \equiv 0 \pmod{d}$$

abbiamo

$$\begin{aligned} |\mathcal{A}_d| &= |\{n : x < n \leq x + h, F(n) \equiv 0 \pmod{d}\}| = \\ &= \rho(d) \left(\frac{h}{d} + \theta \right), \quad |\theta| \leq 1 \end{aligned}$$

e quindi una buona scelta é $X = h$, $\omega_0(d) = \rho(d)$ (infatti ρ é anch' essa moltiplicativa), da cui $|r_d| \leq \rho(d)$.

In particolare, per

$$F(n) = n(n + 2)$$

e piú in generale per

$$F(n) = (an + b)(cn + d), \quad \text{con } ac \text{ non nullo}$$

si ha $\rho(2) = 1$ e (tranne che per i primi p che dividono a, c , oppure $ad - bc$) $\rho(p) = 2$ (cfr. §5.4, §5.5 e §5.6).

Analogamente, se scegliamo q square-free, coprimo con ogni primo $p < z$ in \mathcal{B} e che "si fattorizza in \mathcal{B} ", cioè ha tutti i fattori primi in \mathcal{B} (scriviamo q f. in \mathcal{B}), queste condizioni equivalgono rispettivamente a $\mu^2(q) = 1$, $(q, P(z)) = 1$ e $(q, p) = 1 \quad \forall p$ primo non in \mathcal{B} ; abbiamo quindi

$$(4.2) \quad S(\mathcal{A}_q; \mathcal{B}, z) = \sum_{d|P(z)} \mu(d) |\mathcal{A}_{qd}|,$$

da cui possiamo sperare di ottenere una prima stima della sifting function di \mathcal{A}_q , dopo aver inserito una "buona" stima di $|\mathcal{A}_k|$ (al variare di k fra gli square-free).

A tale scopo, definiamo una funzione ω a partire da ω_0 , ma dipendente non solo da \mathcal{A} , ma anche da \mathcal{B} : per ogni primo p

$$\omega(p) \stackrel{def}{=} \begin{cases} \omega_0(p) & \text{se } p \in \mathcal{B} \\ 0 & \text{altrimenti} \end{cases}$$

e, come per ω_0 , per ogni square-free d

$$\omega(1) \stackrel{def}{=} 1, \quad \omega(d) \stackrel{def}{=} \prod_{p|d} \omega(p) \quad (\mu^2(d) = 1).$$

Di nuovo, come per ω_0 , ω é moltiplicativa.

I "nuovi" resti

$$R_d \stackrel{def}{=} |\mathcal{A}_d| - \frac{\omega(d)}{d} X \quad (\mu^2(d) = 1)$$

coincidono con i "vecchi" r_d , cosí come $\omega(d) = \omega_0(d)$, quando $\mu^2(d) = 1$ (d é square-free) e $p|d \Rightarrow p \in \mathcal{B}$ (d f. in \mathcal{B}).

Definiamo, inoltre, i seguenti prodotti ($\forall z \geq 2$ reale)

$$V(z) \stackrel{def}{=} \prod_{p < z} \left(1 - \frac{1}{p}\right), \quad W(z) \stackrel{def}{=} \prod_{\substack{p < z \\ p \in \mathcal{B}}} \left(1 - \frac{\omega(p)}{p}\right) = \prod_{\substack{p < z \\ p \in \mathcal{B}}} \left(1 - \frac{\omega_0(p)}{p}\right).$$

Se q soddisfa le ipotesi per la 4.2, da quest' ultima abbiamo, per definizione di ω e per la Proposizione 1.1

$$\begin{aligned} S(\mathcal{A}_q; \mathcal{B}, z) &= \frac{X}{q} \omega(q) \sum_{d|P(z)} \mu(d) \frac{\omega(d)}{d} + \sum_{d|P(z)} \mu(d) R_{qd} = \\ &= \frac{X}{q} \omega(q) W(z) + \theta \sum_{d|P(z)} |R_{qd}|, \end{aligned}$$

dove $|\theta| \leq 1$.

In particolare, per la sifting function, se supponiamo che

$$(R) \quad \mu^2(d) = 1, d \text{ si fattorizza in } \mathcal{B} \Rightarrow |R_d| \leq \omega(d)$$

e che

$$(\Omega_0) \quad p \text{ primo} \Rightarrow \omega(p) \leq A_0$$

allora, ponendo $q = 1$ nella stima precedente otteniamo

$$S(\mathcal{A}; \mathcal{B}, z) = XW(z) + \theta(1 + A_0)^z, \quad |\theta| \leq 1,$$

poichè per la Proposizione 1.1, con $\omega(n) \stackrel{def}{=} |\{p : p|n\}|$ **numero dei divisori primi** di n

$$\sum_{d|P(z)} |R_d| \leq \sum_{d|P(z)} A_0^{\omega(d)} = \prod_{\substack{p < z \\ p \in \mathcal{B}}} (1 + A_0) \leq (1 + A_0)^z$$

(cfr. il Teor. 1.1 dell'[H-R]).

Vediamo, in particolare, la formula 4.1 a che cosa ci porta. Banalmente, $z = \sqrt{x}$, $\mathcal{B} = \mathbf{P}$,

$$\mathcal{A} = \{n : n \leq x\}, \quad \mathcal{A}_d = \{n : n \leq x, n \equiv 0(d)\}, \quad |\mathcal{A}_d| = \left\lfloor \frac{x}{d} \right\rfloor,$$

ovvero poniamo $X = x$ e

$$\omega(d) = \omega_0(d) = 1, \quad r_d = \left\{ \frac{x}{d} \right\}, \quad \forall d : \mu^2(d) = 1,$$

da cui

$$\begin{aligned} \pi(x) &= \sum_{d|P(\sqrt{x})} \mu(d) \frac{x}{d} - \sum_{d|P(\sqrt{x})} \mu(d) \left\{ \frac{x}{d} \right\} + \pi(\sqrt{x}) - 1 = \\ &= x \prod_{p < \sqrt{x}} \left(1 - \frac{1}{p} \right) - \sum_{d|P(\sqrt{x})} \mu(d) \left\{ \frac{x}{d} \right\} + \mathcal{O}(\sqrt{x}). \end{aligned}$$

Dato che vale la formula di Mertens (v. [Te], p.17)

$$(4.3) \quad \prod_{p < x} \left(1 - \frac{1}{p} \right) = \frac{e^{-\gamma}}{\log x} (1 + \mathcal{O}(1/\log x)) \quad (x \geq 2)$$

abbiamo che il termine "principale"

$$x \prod_{p < \sqrt{x}} \left(1 - \frac{1}{p} \right) \sim 2x \frac{e^{-\gamma}}{\log x}$$

é diverso da $x/\log x$ (come deve essere dal Teorema dei Numeri Primi, v. §2.2.3).

Ciò significa che vi é cancellazione fra

$$x \prod_{p < \sqrt{x}} \left(1 - \frac{1}{p}\right)$$

e

$$\sum_{d|P(\sqrt{x})} \mu(d) \left\{\frac{x}{d}\right\}.$$

Inoltre, la nostra stima sui resti (v. (R) e (Ω_0)) $|R_d| = |\{x/d\}| \leq 2 = A_0$ fornisce

$$\sum_{d|P(\sqrt{x})} \left\{\frac{x}{d}\right\} \ll 2^{\sqrt{x}},$$

che é, chiaramente, un termine enorme rispetto all' $o(x/\log x)$ atteso.

Quest' ultimo problema é dovuto al fatto che tale somma contiene troppi termini, per cui, se anche la stima (R) viene migliorata, non si ottiene informazione sufficiente ad ottenere un resto accettabile.

Il limite di questo metodo di crivello, come di tutti i metodi di crivello, sta appunto nel fatto che, ad un certo stadio, per ottenere formule asintotiche, é sempre richiesta un' informazione aritmetica.

Tale problema é esposto esaurientemente nell' articolo di Glyn Harman "Eratosthenes, Legendre, Vinogradov and beyond - The hidden power of the simplest sieve" (v. [G-H-H], articolo 9, p.161), nel quale viene anche data una versione "dimostrativa" ed "esemplificata" del famoso metodo di Vinogradov, col quale I.M. Vinogradov diede la stima sulla somma esponenziale sui primi (v. §3.5) (tramite la quale dimostrò il suo famoso Teorema dei tre primi, v. §3.5); tale versione é data dal Lemma 1 di tale articolo (cit. in [G-H-H]).

4.2.2 Crivello Combinatorio

Come appena visto nella sezione precedente, il Crivello di Eratostene-Legendre originario é insufficiente ad ottenere il Teorema dei Numeri Primi e, anzi, non fornisce nemmeno buoni upper-bounds (cfr. le stime di Cebicev nel §2.2.1).

L' idea-chiave del Crivello di Eratostene-Legendre sta nell' identit a aritmetica 1.2 :

$$\mu * \mathbf{1} = \mathbf{e};$$

dalla funzione μ , per o, abbiamo visto discendere la somma

$$\sum_{d|P(\sqrt{x})} \mu(d) \left\{ \frac{x}{d} \right\} = \sum_{d|P(\sqrt{x})} \mu(d) R_d$$

che ha "troppi termini".

Il matematico norvegese Viggo Brun, negli anni fra il 1917 ed il 1924, invent  il **Crivello Combinatorio**, ovvero introdusse due funzioni ausiliarie, μ_1 e μ_2 , che "approssimano μ dal basso e dall' alto" (nel senso che sar  chiaro fra poco), ma che sono nulle "pi  spesso di μ ".

Vediamole nel **Crivello "Puro" di Brun** :

Teorema 4.1 (Brun Pure Sieve). *Sia χ_t la funzione caratteristica dell' insieme $\{n \in \mathbf{N} : \omega(n) \leq t\}$ (qui ω   la funzione "fattori primi").*

Allora $\forall h \geq 0$ intero le funzioni

$$\mu_1(n) \stackrel{def}{=} \mu(n) \chi_{2h+1} \quad e \quad \mu_2(n) \stackrel{def}{=} \mu(n) \chi_{2h}$$

soddisfano la seguente disuguaglianza

$$\mu_1 * \mathbf{1} \leq \mathbf{e} \leq \mu_2 * \mathbf{1}.$$

Ne discende immediatamente il

Corollario 4.1. *Per ogni intero $h \geq 0$*

$$\sum_{d|P(y)} \mu_1(d) |\mathcal{A}_d| \leq S(\mathcal{A}; \mathcal{B}, y) \leq \sum_{d|P(y)} \mu_2(d) |\mathcal{A}_d|.$$

Dal Corollario si ottengono i seguenti lower bound ed upper bound

$$\frac{x \log \log x}{\log x} \ll \pi(x) \ll \frac{x \log \log x}{\log x},$$

che migliorano notevolmente le stime della sezione precedente (anche se, comunque, sono inferiori alle stime elementari di Cebicev, 2.2 in §2.2.1).

Più in generale vale il "Lemma fondamentale del Crivello Combinatorio", ovvero il

Teorema 4.2. *Supponiamo che $\exists X \in \mathbf{R}$ ed $\exists K, A > 0$ tali che*

$$|\mathcal{A}_d| = X\omega(d)/d + R_d \quad (\forall d|P(z))$$

e che

$$\prod_{\eta \leq p \leq \xi} \left(1 - \frac{\omega(p)}{p}\right)^{-1} < \left(\frac{\log \xi}{\log \eta}\right)^K \left(1 + \frac{A}{\log \eta}\right) \quad (2 \leq \eta \leq \xi).$$

Allora, uniformemente rispetto ad \mathcal{A} , X , z ed $u \geq 1$, abbiamo

$$S(\mathcal{A}; \mathcal{B}, z) = X \prod_{\substack{p \leq z \\ p \in \mathcal{B}}} \left(1 - \frac{\omega(p)}{p}\right) \left(1 + \mathcal{O}(u^{-u/2})\right) + \mathcal{O}\left(\sum_{\substack{d \leq z^u \\ d|P(z)}} |R_d|\right).$$

Da tale risultato si ottengono adesso stime di tipo-Cebicev.

Tramite il Corollario 4.1 si può stimare il numero di **primi gemelli**, ovvero di **primi la cui differenza é 2**, fino ad x

$$J(x) \stackrel{def}{=} |\{p \leq x : p+2 \text{ é primo}\}|;$$

per tale quantità Hardy e Littlewood (nel 1922, v. [H-R]) congetturarono la stima asintotica

$$J(x) \sim 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \frac{x}{\log^2 x} \quad (x \rightarrow \infty);$$

il Crivello Combinatorio fornisce, invece, la stima

$$J(x) \ll x \left(\frac{\log \log x}{\log x}\right)^2$$

da cui, per sommazione parziale, segue che la serie dei reciproci converge

$$\sum_{\substack{p \in \mathbf{P} \\ p+2 \in \mathbf{P}}} \frac{1}{p} < \infty.$$

Dal Crivello di Brun seguono anche buone stime asintotiche per il numero di interi (fino ad x) con tutti i divisori primi maggiori di y (fissato) (si veda [Te], p.59 opp. per ulteriori applicazioni il cap.2 dell' [H-R]).

4.2.3 Crivello di Selberg

Il **Crivello di Selberg**, nella sua forma più semplice, é dato dalla disuguaglianza

$$S(\mathcal{A}; \mathcal{B}, z) \leq \sum_{a \in \mathcal{A}} \left(\sum_{\substack{d|a \\ d|P(z)}} \lambda_d \right)^2$$

dove $\lambda_1 \stackrel{def}{=} 1$ e i $\lambda_d \in \mathbf{R} \quad \forall d \geq 2$ sono numeri reali arbitrari.

Infatti, se $a \in \mathcal{A}$ e $(a, P(z)) = 1$, nella somma interna compare solo $d = 1$ e quindi $\lambda_1 = 1$; se, invece $a \in \mathcal{A}$ e $(a, P(z)) > 1$, comunque la somma interna é un reale, il cui quadrato dà un contributo non negativo.

Sviluppando il quadrato e scambiando le tre somme così ottenute

$$S(\mathcal{A}; \mathcal{B}, z) \leq \sum_{\substack{d_1|P(z) \\ d_2|P(z)}} \lambda_{d_1} \lambda_{d_2} \sum_{\substack{a \in \mathcal{A} \\ a \equiv 0(D)}} 1, \quad D \stackrel{def}{=} [d_1, d_2],$$

avendo indicato con $[a, b]$ il minimo comune multiplo di a e b .

Come nelle sezioni precedenti

$$\sum_{\substack{a \in \mathcal{A} \\ a \equiv 0(D)}} 1 = |\mathcal{A}_D| = X \frac{\omega(D)}{D} + R_D$$

e quindi diciamo

$$S(\mathcal{A}; \mathcal{B}, z) \leq X \sum_{\substack{d_1|P(z) \\ d_2|P(z)}} \lambda_{d_1} \lambda_{d_2} \frac{\omega(D)}{D} + \sum_{\substack{d_1|P(z) \\ d_2|P(z)}} |\lambda_{d_1} \lambda_{d_2} R_D| \stackrel{def}{=} X \Sigma_1 + \Sigma_2.$$

L'idea originaria di Selberg é di scegliere i λ_d ($d \geq 2$) in modo che $X \Sigma_1 + \Sigma_2$ sia minimo.

Tuttavia, anche per insiemi \mathcal{A} "semplici" questo é un problema arduo. Quindi, dobbiamo fare delle ipotesi sui λ_d . Per esempio, scegliamo nulli quelli con indice $\geq z$

$$(4.4) \quad \lambda_d = 0 \quad \forall d \geq z$$

e poi scegliamo gli altri λ_d ($2 \leq d < z$) in modo che la forma quadratica Σ_1 abbia un minimo. Inoltre, lavoriamo con l' ipotesi che

$$\Sigma_2 = \sum_{\substack{d_1 | P(z) \\ d_2 | P(z)}} |\lambda_{d_1} \lambda_{d_2} R_D|$$

sia un termine d' errore (ovvero trascurabile risp. Σ_1). D' altra parte gli R_D sono termini (auspicabilmente) trascurabili e d' altronde i λ_d non nulli non sono troppi, per la scelta 4.4.

Supponendo che

$$(\Omega_1) \quad \exists A_1 \geq 1 : 1 \leq \frac{1}{1 - \frac{\omega(p)}{p}} \leq A_1$$

abbiamo che la funzione moltiplicativa

$$g(d) \stackrel{def}{=} \frac{\omega(d)}{d \prod_{p|d} (1 - (\omega(p)/p))} \quad (\mu^2(d) = 1)$$

é ben definita e inoltre $g(d) = 0 \Leftrightarrow \omega(d) = 0$.

Definiamo inoltre le funzioni

$$G(z) \stackrel{def}{=} \sum_{d < z} \mu^2(d) g(d), \quad G(x, z) \stackrel{def}{=} \sum_{\substack{d < x \\ d | P(z)}} g(d), \quad G_k(x) \stackrel{def}{=} \sum_{\substack{d < x \\ (d, k) = 1}} \mu^2(d) g(d).$$

I coefficienti

$$\lambda_d = \frac{\mu(d)}{\prod_{p|d} (1 - \omega(p)/p)} \frac{G_d(z/d)}{G(z)}$$

rispettano $\lambda_1 = 1$ e la 4.4 (per definizione di G e G_k) ed é possibile dimostrare che realizzano, con tali vincoli, il minimo di Σ_1 (ed inoltre esso é pari a $1/G(z)$).

Diamo di seguito il principale risultato riguardo il Crivello di Selberg (per la dim. ed ulteriori risultati ed approfondimenti v. [H-R], cap.3 \rightarrow 7).

Teorema 4.3. Sotto l'ipotesi (Ω_1) si ha

$$S(\mathcal{A}; \mathcal{B}, z) \leq \frac{X}{G(z)} + \Sigma_2,$$

con la stima (l'apice indica che d si fattorizza in \mathcal{B} , v. §4.2.1; $\omega(d)$ é il numero di fattori primi di d , cfr. §4.2.1)

$$\Sigma_2 \leq \sum'_{d < z^2} \mu^2(d) 3^{\omega(d)} |R_d|$$

o, anche, con la stima

$$\Sigma_2 \leq \sum_{\substack{d_1 < z, d_1 | P(z) \\ d_2 < z, d_2 | P(z)}} |R_{[d_1, d_2]}| \sum_{\substack{d < z^2 \\ d | P(z)}} \mu^2(d) 3^{\omega(d)} |R_d|.$$

Inoltre, sotto l'ulteriore ipotesi (R) abbiamo

$$S(\mathcal{A}; \mathcal{B}, z) \leq \frac{X}{G(z)} + \frac{z^2}{W^3(z)}.$$

(Si vedano i Teoremi 3.1 e 3.2 in [H-R]).

Una notevole applicazione del Crivello di Selberg é data dalla **Disuguaglianza di Brun-Titchmarsh** (v. [H-R])

Teorema 4.4. Siano $1 \leq k < y \leq x$, con k intero. Allora, detto $\pi(x; k, l) \stackrel{\text{def}}{=} |\{p \leq x : p \equiv l(k)\}|$ il numero di primi fino ad x congrui ad l modulo k , si ha, per $c > 0$ costante assoluta

$$\pi(x + y; k, l) - \pi(x; k, l) < c \frac{y}{\phi(k) \log x}.$$

Come costante c possiamo scegliere $c = 2 + o(1)$, quando $y/k \rightarrow \infty$ (v. [Te], p.73 per una dim. tramite il Crivello di Brun), oppure $c=2$ (dovuta a Montgomery e Vaughan, cit. in [Te], p.76). In seguito, comunque, useremo la versione

$$(4.5) \quad \pi(x + y; k, l) - \pi(x; k, l) \ll \frac{y}{\phi(k) \log x}.$$

4.3 Crivello Largo

Ricordiamo che una generica *somma esponenziale* di coefficienti a_n é

$$S(\alpha) \stackrel{def}{=} \sum_{n=M+1}^{M+N} a_n e(n\alpha), \quad \text{dove } e(\beta) \stackrel{def}{=} e^{2\pi i\beta} \quad \forall \beta \in \mathbf{R}$$

e siano $\alpha_1, \alpha_2, \dots, \alpha_R \in \mathbf{R}$ distinti modulo 1; inoltre, per $\delta > 0$, sia

$$\| \alpha_r - \alpha_s \| \geq \delta \quad \forall r, s \text{ distinti}$$

(con $\| \alpha \| \stackrel{def}{=} \min_{z \in \mathbf{Z}} |\alpha - z|$), ovvero sono δ - **distanti**; si definisce **Crivello Largo** una disuguaglianza del tipo (Δ dipende solo da N e da δ):

$$(4.6) \quad \sum_{r=1}^R |S(\alpha_r)|^2 \leq \Delta \sum_{n=M+1}^{M+N} |a_n|^2.$$

La stima ottimale $\Delta = \Delta(N, \delta) = N + \delta^{-1} - 1$ é stata ottenuta da Montgomery e Vaughan e da Selberg (cfr. [Te] e [B(1)]).

Ad esempio, gli $x_j \stackrel{def}{=} j/n$ ($j = 1, 2, \dots, n$) formano un insieme di numeri $1/n$ - *distanti*, per cui segue il Corollario 1 in [B(1)] (p.13):

Proposizione 4.1.

$$\sum_{j=1}^R |S(j/q)|^2 \leq (N + n - 1) \sum_{n=M+1}^{M+N} |a_n|^2.$$

Inoltre, scegliendo le **frazioni di Farey** a/q , dove $(a, q) = 1 \quad \forall q \leq Q$,

$$\| a/q - a'/q' \| = \| (aq' - a'q)/(qq') \| \geq 1/(qq') \geq (1/Q^2),$$

si ottiene il Corollario 2 in [B(1)] (p.13):

Proposizione 4.2.

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^q |S(a/q)|^2 \leq (N + Q^2 - 1) \sum_{n=M+1}^{M+N} |a_n|^2.$$

Una breve storia del Crivello Largo si può dare ricordando il primo lavoro di Linnik (del 1941), seguito da una serie di articoli di Renyi, che inaugurava un approccio probabilistico, però non ancora ottimale.

Quindi, nel 1965, Roth dava all'argomento l'attuale sistemazione, tramite le somme esponenziali; tale approccio, a meno di ulteriori "ritocchi" dovuti a Bombieri (v. [B(2)] del 1965, [Ga(2)] del 1968 e [B(1)] del 1974) è ottimale. Bombieri, inoltre, applicò il Crivello Largo allo studio della distribuzione dei primi nelle progressioni aritmetiche: v. §2.5.

Renyi considerava un'estensione della disuguaglianza di Bessel con vettori della base "quasi ortogonali", per applicarla direttamente a funzioni aritmetiche; laddove Roth, in seguito, la applicò alle somme esponenziali.

Tale disuguaglianza (che possiamo considerare un Crivello Largo "ante litteram") è data dalla

Proposizione 4.3. *Sia V un \mathbf{C} -spazio vettoriale, con prodotto interno (\cdot, \cdot) e siano ϕ_1, \dots, ϕ_R e ξ vettori di V . Allora*

$$\sum_{r=1}^R |(\xi, \phi_r)|^2 \leq A \|\xi\|^2,$$

dove

$$A \stackrel{\text{def}}{=} \max_{r \leq R} \sum_{s=1}^R |(\phi_r, \phi_s)|.$$

Nel 1967 P. X. Gallagher [Ga(1)] trovava una linea dimostrativa diversa dalla precedente, basata su quella che oggi è nota come "**disuguaglianza di Gallagher-Sobolev**" (v. [M(1)]).

Vediamo più in dettaglio l'approccio "probabilistico" di Renyi (cfr. il Metodo della Dispersione nel §4.4).

Sia \mathcal{N} un insieme di Z interi nell'intervallo $[M+1, M+N]$ ($M \in \mathbf{Z}$ ed $N \in \mathbf{N}$) e

$$Z(q, h) \stackrel{\text{def}}{=} |\{n \in \mathcal{N} : n \equiv h \pmod{q}\}|.$$

Ovviamente

$$\sum_{h=1}^q Z(q, h) = Z,$$

in modo che il **valor medio** (o valore atteso) di $Z(q, h)$ è Z/q .

Renyi considerava la "varianza"

$$V(q) \stackrel{\text{def}}{=} \sum_{h=1}^q \left(Z(q, h) - \frac{Z}{q} \right)^2$$

(qui dovremmo normalizzare dividendo per q).

Dall' ortogonalità dei caratteri additivi (v. §2.4.1) e dalla Proposizione 4.2 segue allora che

$$\sum_{p \leq Q} pV(p) \leq (N + 3Q^2)Z.$$

Da tale disuguaglianza si ha come conseguenza per i crivelli aritmetici la

Proposizione 4.4. *Sia \mathcal{N} un insieme di Z interi in $[M + 1, M + N]$. Sia \mathcal{P} un insieme di P numeri primi p , con $p \leq Q$, $\forall p \in \mathcal{P}$. Sia $\tau \in]0, 1[$ e supponiamo che $Z(p, h) = 0$ per almeno τp valori di $h \pmod{p}$, $\forall p \in \mathcal{P}$. Allora*

$$Z \leq \frac{N + 3Q^2}{\tau P}.$$

4.4 Metodo della Dispersione

Il metodo della Dispersione é stato introdotto, nell' ambito della Teoria Additiva dei Numeri, da Yu. V. Linnik nella seconda metà di questo secolo (v. [L]).

Consiste nel considerare, in generale, la **media quadratica**

$$(4.7) \quad \sum_m \left| \left(\sum_n c_{m,n} - E(m) \right) \right|^2,$$

dove m ed n variano in certi sottinsiemi degli interi, diciamo \mathcal{M} ed \mathcal{N} , ed $E(m)$ é il "valore atteso" della somma $\sum_n c_{m,n}$.

Qui i **momenti d'ordine** K rispetto al valore atteso (anzi, i **momenti assoluti** rispetto al valore atteso, dato che, in generale, si ha a che fare con somme complesse) sono dati da

$$\sum_m \left| \left(\sum_n c_{m,n} - E(m) \right) \right|^K$$

(dovremmo normalizzare dividendo per $\sum_{m \in \mathcal{M}} 1 = |\mathcal{M}|$).

In particolare, per $K = 2$, stiamo considerando la media quadratica della 4.7, di cui sopra.

Essa rappresenta una "varianza", in cui, però, la probabilità non é normalizzata (si può normalizzare dividendo, come sopra, per $|\mathcal{M}|$) e il "valore atteso" $E(m)$ non é definito come "valore medio" (ovvero come media aritmetica), ma in modo tale che

$$\sum_m \left(\sum_n c_{m,n} - E(m) \right)$$

sia "piccolo".

In Probabilità la varianza misura la Dispersione di una variabile aleatoria intorno al suo valore medio (o valore atteso).

Tali idee ispirarono il lavoro di Yu. V. Linnik (cfr. anche i collegamenti col Crivello Largo, v. §4.3); che venne, in seguito, usato soprattutto nell' ambito della Teoria Analitica dei Numeri (che, al contrario della Teoria Probabilistica dei Numeri, non usa tecniche della Teoria della Probabilità; cfr. a proposito l' introduzione del [Te]).

In tale ambito si usa soprattutto (cfr. le applicazioni del metodo che seguono ed il §5.5) quello che é il punto centrale del metodo (usato anche in

[C-S(2)]; ovvero lo scambio delle somme su m e sulle variabili n_1, n_2 (che si ottengono svolgendo il quadrato), in modo da ottenere cancellazione:

$$\sum_{n_1, n_2} \sum_m c_{m, n_1} \overline{c_{m, n_2}} - \sum_{n_1} \sum_m c_{m, n_1} \overline{E(m)} - \sum_{n_2} \sum_m \overline{c_{m, n_2}} E(m) + \sum_m |E(m)|^2$$

(cfr. l' applicazione del metodo in §5.5.2).

Infatti si valutano separatamente i quattro termini, scrivendoli come un termine principale più un termine d' errore. A causa dei segni, poichè i quattro termini principali sono uguali fra loro, restano solo i termini d' errore, che quindi forniscono una stima (spesso in \mathcal{O}) della media quadratica di partenza 4.7.

Tale Metodo é stato utilizzato (ad esempio) nel 1978 da H.Iwaniec [Iw(1)] per dimostrare che ci sono infiniti numeri naturali del tipo $n^2 + 1$ che si possono scrivere come prodotto di due primi (o sono primi).

Si veda anche l' applicazione al problema della distribuzione di $n(n+2)$ (e, più in generale, dei polinomi quadratici riducibili) nelle progressioni aritmetiche, negli intervalli corti $x < n \leq x + h$ (cfr. §5.5 e [C-S(2)]).

4.5 Somme Esponenziali

In generale, una somma esponenziale di coefficienti a_n é data da

$$\sum_{N < n \leq N+M} a_n e(n\alpha),$$

dove $\alpha \in [0, 1]$.

Le stime di somme esponenziali sono fondamentali in T.A.N.

Ne sono un esempio le stime di Vinogradov (cfr. §3.4 e §3.5), in cui $a_n = \log n$ sui primi oppure $a_n = \Lambda(n)$.

Più in generale, si dice somma esponenziale una somma del tipo

$$\sum_{N < n \leq N+M} a_n e(f(n)\alpha),$$

per un certo $\alpha \in [0, 1]$ ed una certa funzione f .

L' approccio standard (se f é abbastanza "liscia" ed $a_n = 1$ oppure é quasi costante) é di ricondurre tali somme ad integrali di esponenziali (v. per es. [Ti], cap. 4).

Può darsi, però, che f abbia un significato aritmetico, ma non sia una funzione "regolare"; infatti, scelto $q \in \mathbf{N}$, ed $\alpha = j/q$, con j intero, si può prendere $f(n) \stackrel{def}{=} \bar{n}(\text{mod } q)$, ovvero l' **inverso di** $n(\text{mod } q)$, in modo da ottenere, per $a_n = 1$, (un caso particolare di) somme di Kloosterman (v. §4.7).

Un caso analogo é dato da ($f(n) = n$) $a_n = \Lambda(n)$, che é "circa" la funzione caratteristica dei primi per un logaritmo (cfr. §2.2.2). In questo caso, I.M.Vinogradov (nel 1937) si ricondusse a funzioni di tipo divisori e forme bilineari (cfr. §4.6), per poter dimostrare la stima (v. Teorema 3.1) da cui segue il suo famoso Teorema dei tre Primi (v. §3.5).

Un altro caso notevole di somma esponenziale si ottiene per ($a_n = 1$) $f(n) = n^K$, nel qual caso si hanno le stime di H.Weyl, che consentono di utilizzare il Metodo del Cerchio per studiare il Problema di Waring (cfr. §3.1 e [Va(1)], specialmente capp. 1 e 2).

Le stime di Weyl si basano sull' idea di applicare ad f il metodo delle differenze finite; tale Metodo si chiama, appunto, "Weyl differencing" (risale al 1916) ed é stato perfezionato da J.G.Van der Corput negli anni '20 (v. [G-K], specialmente capp. 1 e 2).

4.6 Forme Bilineari

La stima di forme bilineari del tipo

$$\sum_m \sum_n \alpha_m \beta_n f(m, n),$$

dove si può supporre che i range di m ed n siano del tipo $]M, 2M]$ e $]N, 2N]$ (risp.) ed f sia una data funzione, consente di ottenere risultati non banali in diverse aree della T.A.N.

Ad esempio, per migliorare il livello di distribuzione di una successione nelle progressioni aritmetiche (v. [Iw(1)] e cfr. §5.4). Oppure, tramite l'Identità di Vaughan, per dimostrare le stime di Vinogradov sulle somme esponenziali sui primi (cfr. §2.5). Inoltre, si possono dare anche stime di somme che possono essere valutate solo in media su un'ulteriore variabile, come ad esempio nel caso di forme bilineari con frazioni di Kloosterman (v. [D-F-I], cfr. §5.6).

Inoltre, H.Iwaniec le utilizzò per dare una forma più flessibile del termine di resto nel "Crivello Lineare" (v. [Iw(2)] ed [H-R]).

4.7 Somme di Kloosterman

La generica **somma di Kloosterman** é una somma del tipo ($a, b \in \mathbf{Z}$)

$$(4.8) \quad S(q; a, b) \stackrel{def}{=} \sum_{\substack{n \leq N \\ (n, q) = 1}} e_q(an + b\bar{n})$$

dove $n\bar{n} \equiv 1 \pmod{q}$, ovvero \bar{n} é l' inverso di $n \pmod{q}$ (qui $q, N \in \mathbf{N}$ sono fissati ed $N \leq q$).

Nelle applicazioni é molto usata anche la **somma di Kloosterman incompleta**

$$(4.9) \quad S(q; b) \stackrel{def}{=} \sum_{\substack{n \leq N \\ (n, q) = 1}} e_q(b\bar{n})$$

per la quale vale la **stima di Weil** [W] quando il modulo q é primo (e, banalmente, q non divide b , altrimenti vale $\phi(q)$):

$$(4.10) \quad |S(q; b)| \leq 2q^{1/2}.$$

Dalle proprietà delle somme di Kloosterman, segue la stima di Estermann [Es]

$$(4.11) \quad |S(q; a, b)| \leq d(q)q^{1/2}(q, a, b)^{1/2},$$

dove abbiamo indicato con $d(q)$ il numero di divisori di q e con (q, a, b) il massimo comune divisore dei tre interi q, a, b .

In particolare, dalla stima $d(q) \ll q^\varepsilon$ (v. [H-W], p.260), si ha il seguente bound per le somme di Kloosterman incomplete:

$$(4.12) \quad |S(q; b)| \ll q^{1/2+\varepsilon}(q, b)^{1/2}.$$

Più in generale, vale la seguente stima (Lemma 8 in [D-F-I])

Proposizione 4.4. *Sia I un "segmento di una progressione aritmetica", ovvero*

$$I \stackrel{def}{=} \{n \in]M, M + N] : n \equiv l \pmod{k}\},$$

χ un carattere di Dirichlet \pmod{c} con $(c, k) = 1$ ed $a, b \in \mathbf{Z}$. Allora (detta τ la funzione divisori)

$$\left| \sum_{n \in I} \bar{\chi}(n) e\left(\frac{a\bar{n} + bn}{c}\right) \right| \leq \left(\frac{X}{ck} + 2 \log 3c\right) (a, c)^{1/2} c^{1/2} \tau(c).$$

Capitolo 5

Problemi in Intervalli Corti

5.1 Problemi in Intervalli Corti

Questo Capitolo é dedicato ai risultati originali ottenuti dall' Autore nell' ambito di particolari problemi moltiplicativi e additivi negli intervalli corti.

Il primo problema in questo capitolo (§5.2) di cui si é occupato l' Autore é quello della stima dell' integrale di Selberg, che é una quantità che consente di controllare il numero dei primi in "quasi tutti" gli intervalli corti; in particolare, si é ottenuto un legame fra tale integrale e la media quadratica (discreta) di un termine di resto della Formula Esplicita di Riemann-von Mangoldt, che dipende dalla simmetria di distribuzione attorno ad x dei primi negli intervalli corti del tipo $[x - h, x + h]$ (qui si può supporre che $x \in \mathbf{N}$).

Tale simmetria di distribuzione é collegata in maniera naturale ai numeri di Goldbach $2x = p_1 + p_2$, con $p_1, p_2 \in [x - h, x + h]$; per tale motivo l' Autore si é occupato, successivamente, del problema di Goldbach con primi quasi uguali (§5.3).

In seguito, l' Autore si é dedicato al problema della distribuzione della successione polinomiale $n(n + 2)$ nelle progressioni aritmetiche negli intervalli corti, ovvero quando $n \in [x, x + h]$ (in particolare della stima, in media su $q \in]Q, 2Q]$ ed $r \in]R, 2R]$, del numero di elementi del tipo $n(n + 2)$, con $n \in [x, x + h]$, che sono multipli di qr); tale problema ha applicazioni allo studio dei primi gemelli (cfr. §4.2).

Per tale problema, si sono ottenuti risultati (in sostanza indipendenti fra loro) tramite le seguenti tre tecniche :

- nel §5.4 con il Crivello Largo (v. §4.3);
- nel §5.5 con il metodo della Dispersione (v. §4.4);
- nel §5.6 con le somme di Kloosterman (v. §4.7).

5.2 Primi in quasi tutti gli Intervalli Corti

In questo paragrafo seguiremo [C-V].

5.2.1 Introduzione ed enunciato dei risultati

Il problema dei primi in quasi tutti gli intervalli corti é stato esposto in §2.3.

Per ottenere la 2.10 in quasi tutti gli intervalli corti $[x, x+h]$ (scriveremo anche q.t.) si studia l' integrale di Selberg

$$J(N, H) \stackrel{def}{=} \int_N^{2N} |\psi(x+H) - \psi(x) - H|^2 dx$$

(v. §1.1.2 e §2.2.2).

Ovviamente

$$J(N, H) = o(NH^2) \Leftrightarrow \psi(x+H) - \psi(x) \sim H \quad q.t. \ x \in [N, 2N]$$

e il risultato citato prima si ottiene attraverso la stima $J(N, H) = o(NH^2)$, che vale nel caso in cui $H \geq N^{1/6+\epsilon}$ ed $\epsilon > 0$ (cfr. §2.3).

Le tecniche usate in letteratura per stimare l' integrale di Selberg si basano sulla formula esplicita classica di Riemann-von Mangoldt 1.41.

Usando la stima di Huxley (v. §1.2.5) A. Perelli [P] ha dimostrato che, definendo

$$I'(N, T) \stackrel{def}{=} \int_N^{2N} |E(x, T)|^2 dx,$$

dove $E(x, T)$ é il termine di resto nella formula esplicita di Riemann-von Mangoldt 1.41, si ha:

$$I'(N, T) = o\left(\frac{N^3}{T^2 L}\right), T \leq N^{1-\vartheta} \Rightarrow J(N, H) = o(NH^2), H \geq N^\vartheta$$

(qui $0 < \vartheta < 1$ e $L = \log N$ nel seguito).

Allo scopo di poter ottenere l' implicazione inversa J. Kaczorowski e A. Perelli hanno introdotto una nuova forma della formula esplicita di Riemann-von Mangoldt, cioè il Teorema 1 in [K-P(2)] (con le scelte $q = 1$ e $\chi = \chi_0$).

Come in quell' articolo, definiamo le quantità

$$w(u) \stackrel{def}{=} \begin{cases} 1 & \text{se } 0 \leq u \leq 1/2 \\ 2(1-u) & \text{se } 1/2 \leq u \leq 1 \end{cases}, \quad \text{sgn}(u) \stackrel{def}{=} \begin{cases} 1 & \text{se } u > 0 \\ 0 & \text{se } u = 0 \\ -1 & \text{se } u < 0 \end{cases}$$

$$G(x, T, n) \stackrel{def}{=} \frac{2}{T} \int_{T/2}^T \int_{\tau|\log \frac{x}{n}|}^{\infty} \frac{\sin u}{u} du dt$$

per derivarne (nello stesso modo della dimostrazione del Corollario in [K-P(2)]) il risultato seguente (cfr. la formula esplicita classica 1.41)

Siano $16 \leq N \leq x \leq 2N$, $4 \leq T \leq N/4$ e $1 \leq M \leq \frac{\min(N^{1/16}, T^{1/5})}{L^9}$; allora

$$(5.1) \quad \psi(x) = x - \sum_{|\gamma| \leq T} w\left(\frac{|\gamma|}{T}\right) \frac{x^\rho}{\rho} + R(x, T)$$

dove

$$(5.2) \quad R(x, T) = \frac{1}{\pi} \sum_{x - \frac{MN}{T} < n \leq x + \frac{MN}{T}} \Lambda(n) \text{sgn}(x-n) G(x, T, n) + \mathcal{O}\left(\frac{NL}{TM \log \frac{N}{T}} + \Lambda([x]) + 1\right).$$

In [K-P(1)] Kaczorowski e Perelli danno quindi un collegamento fra $J(N, H)$ e la media quadratica di $R(x, T)$, definita da

$$I(N, T) \stackrel{def}{=} \int_N^{2N} |R(x, T)|^2 dx,$$

nel caso in cui $N^\epsilon \leq H \leq N^{1-\epsilon}$, $0 < \epsilon < 1/4$ e T é circa N/H .

Noi, invece, ci interessiamo all' analogo di tale relazione nel caso $H = \log^A N$, con A opportuna (v. seguito).

Per quanto riguarda i risultati condizionali, Selberg dimostrò che $J(N, H) = o(NH^2)$, per $H = \infty(\log^2 N)$, sotto l' ipotesi di Riemann e, recentemente, alcuni autori hanno dimostrato lo stesso per $H = \infty(\log N)$, sotto un' ipotesi più forte (la congettura della correlazione delle coppie di Montgomery).

Nel Teorema 1 di [K-P(1)] abbiamo una stima non banale di $I(N, T)$ attraverso una stima non banale di $J(N, H)$; dato che trattiamo potenze del logaritmo di N , invece di potenze di N , otteniamo un fattore logaritmo in più dalla disuguaglianza di Brun-Titchmarsh 4.5 nel resto di 5.2; ciò porta, alla fine, ad un quadrato del logaritmo in più nel nostro

Teorema 5.1 *Siano* $B > 1/2$, $0 < \delta < 1/4$, $N^\delta \leq T \leq NL^{-2B}$ ed $1 \leq M \leq L^B$. Allora

$$I(N, T) \ll M^2 J(N, H) + \frac{N^3}{T^2} \left(\frac{L \log(M+1)}{M \log \frac{N}{TM}} \right)^2,$$

dove $H = \frac{N}{TM}$.

Poiché la nostra dimostrazione é essenzialmente la stessa di quella del Teorema 1 in [K-P(1)] (ma stavolta dobbiamo usare 5.1 e 5.2 invece del Corollario di [K-P(2)]), l' ometteremo.

La maggiorazione opposta, di $J(N, H)$ attraverso $I(N, T)$, data dal Teorema 2 di [K-P(1)], richiede una stima migliore del resto di $R(x, T)$, dato che, adesso, T varia in un range più grande di valori.

La principale novità del nostro articolo é la stima della differenza $R(x, T) - R([x], T)$; che é data dal Lemma nel paragrafo seguente, nel quale maggioriamo il termine principale dei resti in 5.2 per avere una stima non banale.

Siano $0 < \delta < 1/8$, $K \geq 1$,

$$J \stackrel{def}{=} \log_2 \left(\frac{L^{1/2} K N^{1-\delta}}{H} \right)$$

(logaritmo in base 2) e per $j = 1, \dots, J$ definiamo

$$H_j \stackrel{def}{=} \frac{2^j H}{2L^{1/2} K} \quad \text{e} \quad T_j \stackrel{def}{=} \frac{N}{100H_j},$$

da cui

$$\frac{H}{L^{1/2}K} \leq H_j \leq \frac{N^{1-\delta}}{2} \quad \text{e} \quad \frac{N^\delta}{50} \leq T_j \leq \frac{NL^{1/2}K}{100H}.$$

Abbiamo il seguente

Teorema 5.2. *Siano $\epsilon > 0$, $H \geq L^{311+\epsilon}$ e $1 \leq K \leq L^{1/2}$. Allora*

$$J(N, H) \ll H^2 \sum_{j=1}^J H_j^{-2} I(N, T_j) + \\ + NH^2 \left(\frac{1}{K^2} + \left(\frac{KL^{1/2}}{H} \right)^{\frac{6}{155}} + \frac{HL^2}{N \log^2 H} \right).$$

Se scegliamo $B = 1 + \epsilon$, $\epsilon > 0$ ed $M = L^B$ nel Teorema 5.1 otteniamo facilmente il seguente

Corollario 5.1. *Se $\epsilon > 0$, $0 < \delta < 1/4$ e $L^{1+\epsilon} \leq H \leq N^{1-\delta}$ allora*

$$J(N, H) = o(NH^2) \Rightarrow I(N, T) = o\left(\frac{N^3}{T^2}\right), \forall T : N^\delta \leq T \leq \frac{N}{L^{2+2\epsilon}}.$$

Il Teorema 5.2 dà l' inverso dell' ultimo risultato, se $K \rightarrow \infty$ e $K = o(L^\epsilon)$, grazie al seguente

Corollario 5.2. *Siano $\epsilon > 0$, $0 < \delta < 1/8$; allora, per $H \geq L^{311+\epsilon}$ ed $H = o(N)$ abbiamo*

$$I(N, T) = o\left(\frac{N^3}{T^2 L}\right), \forall T \in \left[\frac{N^\delta}{50}, \frac{NL^{1/2}K}{100H}\right] \Rightarrow J(N, H) = o(NH^2),$$

dove $K \rightarrow \infty$ e $K = o(L^\epsilon)$ (per $N \rightarrow \infty$).

Osserviamo che, per i nostri intervalli corti, la richiesta sulla media quadratica di $R(x, T)$ per ottenere $J(N, H) = o(NH^2)$ é estesa ad un insieme abbastanza più grande di valori di T .

Vedremo, nella prossima sezione, la dimostrazione del Lemma 1 di [C-V].

Per la dimostrazione completa del Teorema 5.2 si vedano [C-V] e la correzione:

G. Coppola, A. Vitolo - CORRIGENDUM TO OUR PAPER "ON THE DISTRIBUTION OF PRIMES IN INTERVALS OF LENGTH $\log^\theta N$ " - Acta Math. Hungar. **78(4)** (1998), 359-361.

5.2.2 Enunciato e dimostrazione del Lemma 1

Lemma 5.1. Sia $\{a_n\}_{n \in \mathbf{N}}$ una successione di numeri complessi, $x \geq 4$, $c = 1 + \frac{1}{\log x}$, $A_0(x) = \sum_{n < x} a_n + \frac{a_x}{2}$ (qui $a_x = 0$ se x non é in \mathbf{N}) ed $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ sia assolutamente convergente in $\sigma = \text{Re}(s) > 1$; allora per $\tau \in (T/2, T]$, $T \rightarrow \infty$ e $T = o(x)$ quando $x \rightarrow \infty$, abbiamo

$$A_0(x) = \frac{1}{2\pi i} \int_{c-i\tau}^{c+i\tau} f(s) \frac{x^s}{s} ds + g(x, \tau),$$

dove

$$\begin{aligned} \frac{2}{T} \int_{T/2}^T (g(x, \tau) - g([x], \tau)) d\tau &\ll \frac{1}{T^2} \sum_{n \leq \frac{x}{2}} \frac{|a_n|}{\log^2 \frac{x}{n}} + \sum_{x - \frac{x}{T} < n \leq x + \frac{x}{T}} |a_n| + \\ &+ \frac{1}{T} \sum_{n \in I} |a_n| \left(\frac{1}{x \log^2 \frac{x}{n}} + \frac{1}{T} \right) + \frac{x}{T^2} \sum_{n > 2x} \frac{|a_n|}{n^c \log^2 \frac{x}{n}}, \end{aligned}$$

con I insieme degli interi negli intervalli $(x/2, x - \frac{x}{T}]$, $(x + \frac{x}{T}, 2x]$.

Dimostrazione Per la formula di inversione di Perron e la assoluta convergenza di $f(s)$ per $\sigma > 1$ abbiamo

$$\begin{aligned} (5.3) \quad A_0(y) &= \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} f(s) \frac{y^s}{s} ds = \\ &= \frac{1}{2\pi i} \int_{c-i\tau}^{c+i\tau} f(s) \frac{y^s}{s} ds + \sum_{n=1}^{\infty} a_n \mathcal{I}(n, y, \tau) \end{aligned}$$

con $y = x$ oppure $y = [x]$, $\tau \in (T/2, T]$ e

$$(5.4) \quad \mathcal{I}(n, y, \tau) = \frac{1}{2\pi i} \int_{\substack{\sigma=c \\ |t|>\tau}} \left(\frac{y}{n}\right)^s \frac{ds}{s}.$$

Osserviamo che, in virtú delle 5.3 e 5.4, la stima nella dimostrazione del Teorema 1 nell' articolo di Dieter Wolke (cit. in [C-V]), combinata con

$$\frac{2}{T} \int_{T/2}^T (\mathcal{I}(n, x, \tau) - \mathcal{I}(n, [x], \tau)) d\tau \ll \left| \frac{2}{T} \int_{T/2}^T \mathcal{I}(n, x, \tau) d\tau \right| +$$

$$+ \left| \frac{2}{T} \int_{T/2}^T \mathcal{I}(n, [x], \tau) d\tau \right|,$$

danno il Lemma per n non in I .

Se $n \in I$ procediamo nel seguente modo.

Poniamo $y = x$ in 5.4 ed $\ell \stackrel{def}{=} \log(x/n)$ per avere

$$\begin{aligned} \mathcal{I}(n, x, \tau) &= \frac{1}{\pi} \left(\frac{x}{n}\right)^c \int_{\tau}^{\infty} \frac{c \cos \ell t + t \sin \ell t}{c^2 + t^2} dt \\ &= \frac{1}{\pi} \left(\frac{x}{n}\right)^c \int_{\tau}^{\infty} \frac{c \cos \ell t + t \sin \ell t}{t^2} dt + \mathcal{O} \left(\left(\frac{x}{n}\right)^c \left(\int_{\tau}^{\infty} \frac{1}{t^4} d\tau + \int_{\tau}^{\infty} \frac{1}{t^3} d\tau \right) \right); \end{aligned}$$

dato che $\tau \gg T$ e $(x/n)^c \ll 1 \quad \forall n \in I$, otteniamo

$$(5.5) \quad \mathcal{I}(n, x, \tau) = \frac{1}{\pi} \left(\frac{x}{n}\right)^c \int_{\tau}^{\infty} \frac{c \cos \ell t + t \sin \ell t}{t^2} dt + \mathcal{O} \left(\frac{1}{T^2} \right);$$

allo stesso modo, ponendo $y = [x]$ in 5.4 e $w = \log([x]/n)$ si ha

$$(5.6) \quad \mathcal{I}(n, [x], \tau) = \frac{1}{\pi} \left(\frac{[x]}{n}\right)^c \int_{\tau}^{\infty} \frac{c \cos w t + t \sin w t}{t^2} dt + \mathcal{O} \left(\frac{1}{T^2} \right).$$

Osserviamo che, diciamo, $D \stackrel{def}{=} \ell - w = \log \left(1 + \frac{\{x\}}{[x]} \right) \ll \frac{1}{x}$ e

$$(5.7) \quad n \in I \Rightarrow 1 \ll |\ell|T, |w|T \ll T;$$

in particolare, $T = o(x)$ implica

$$(5.8) \quad \frac{1}{|w|} \ll \frac{1}{|\ell|}.$$

Quindi, dato che $\left(1 + \frac{\{x\}}{[x]} \right)^c = 1 + \mathcal{O}(\frac{1}{x})$, integrando 5.5 per parti

$$\mathcal{I}(n, x, \tau) = \frac{1}{\pi} \left(\frac{[x]}{n}\right)^c \int_{\tau}^{\infty} \frac{\sin \ell t}{t} + \frac{c \cos \ell t}{t^2} dt + \mathcal{O} \left(\frac{1}{xT|\ell|} + \frac{1}{T^2} \right);$$

allo stesso modo otteniamo dalla 5.6, grazie alla 5.7 e alla 5.8

$$\begin{aligned} & \mathcal{I}(n, x, \tau) - \mathcal{I}(n, [x], \tau) = \\ &= \frac{1}{\pi} \left(\frac{[x]}{n} \right)^c \int_{\tau}^{\infty} \frac{\sin \ell t - \sin wt}{t} + c \frac{\cos \ell t - \cos wt}{t^2} dt + \mathcal{O} \left(\frac{1}{xT|\ell|} + \frac{1}{T^2} \right). \end{aligned}$$

Essendo $([x]/n)^c \ll 1 \quad \forall n \in I$, dobbiamo provare, diciamo, che

$$(5.9) \quad \frac{2}{T} \int_{T/2}^T \int_{\tau}^{\infty} \frac{\sin \ell t - \sin wt}{t} dt d\tau \ll \frac{1}{xT\ell^2}$$

e che

$$(5.10) \quad \frac{2}{T} \int_{T/2}^T \int_{\tau}^{\infty} \frac{\cos \ell t - \cos wt}{t^2} dt d\tau \ll \frac{1}{xT\ell^2}$$

per ottenere il Lemma.

Integrando due volte per parti la 5.9 e la 5.10, dato che per x abbastanza grande $1/D > [x] > T$, possiamo maggiorare gli integrali su $(\tau, 1/D)$ e su $(1/D, \infty)$ per ottenere la media richiesta.

5.3 Problema di Goldbach con primi quasi uguali

In questo paragrafo diamo la generalizzazione del Teorema di Chudakov-van der Corput-Estermann (cit. in [Va(1)]) sull'insieme eccezionale nel problema di Goldbach binario ad un problema con primi "quasi uguali"; cioè proviamo che l'equazione $p_1 + p_2 = 2n$ è soddisfatta da quasi tutti i $2n \in [N, 2N]$ quando i primi p_1 e p_2 stanno nell'intervallo $[n-U, n+U]$, con $U = n^{5/8+\epsilon}$. Inoltre, stimiamo esplicitamente il numero di rappresentazioni di questi $2n$ come somme di tali primi (v. Teorema 5.3).

(Il paragrafo sarà strutturato in sezioni che seguiranno le sezioni di [C-L(2)]; la notazione non segue quella del Capitolo 3, ma è indipendente, v. anche §5.3.1).

Nel problema binario di Goldbach, dal Teorema di Chudakov-van der Corput-Estermann [Va(1), cap.3] segue che il numero $E(N)$ dei pari $n \leq N$ per i quali n non è somma di 2 primi soddisfa $E(N) \ll NL^{-A}$, dove $L = \log N$ ed $A > 0$ è una costante assoluta.

Il Teorema dei 3 primi di Vinogradov [Vi] asserisce che ogni dispari sufficientemente grande N si può rappresentare come $N = p_1 + p_2 + p_3$, con p_i ($i = 1, 2, 3$) primi (v. §3.5 e §3.6). Molti autori hanno provato che tale Teorema vale ancora sotto l'ulteriore restrizione $|p_i - N/3| \ll N^{\theta+\epsilon}$ ($\theta < 1$), $i = 1, 2, 3$ ($\theta = 63/64, 160/183, 2/3, 91/96$: risultati cit. in [C-L(2)]).

Assumendo G.R.H. (v. §1.3.3), Wolke (cit. in [C-L(2)]) ottenne lo stesso risultato con $|p_i - N/3| \leq N^{1/2}(\log N)^{7+\epsilon}$, $i = 1, 2, 3$.

In seguito, migliorando precedenti risultati incondizionali, Zhan Tao [Z] dimostrò il Teorema per $\theta = 5/8$. Inoltre, il suo metodo dà anche una formula asintotica per il numero $R(N)$ di rappresentazioni. Usando il metodo del cerchio (v. §3.3), il problema in [Z] si riduce ad ottenere stime non banali per somme esponenziali sui primi in intervalli corti.

In qualche caso le stime dipendono da teoremi di densità in intervalli corti. In altri casi si applicano l'identità di Heath-Brown (v. §2.5) e tecniche analitiche standard basate sui valori medi delle funzioni L di Dirichlet.

Noi, usando le tecniche di Zhan Tao, dimostriamo un risultato analogo per il corrispondente problema binario

$$(5.11) \quad 2n = p_1 + p_2, \quad n - U \leq p_1, p_2 \leq n + U.$$

Più precisamente, sia (queste notazioni e le seguenti del paragrafo sono diverse da quelle del Capitolo 3)

$$R(2n) = R(2n, U) \stackrel{def}{=} \sum_{\substack{h+k=2n \\ n-U < h, k \leq n+U}} \Lambda(h)\Lambda(k),$$

$$\mathfrak{S}(2n) \stackrel{def}{=} 2 \prod_{\substack{p|n \\ p>2}} \left(\frac{p-1}{p-2} \right) \prod_{p>2} \left(1 - \frac{1}{(p-1)^2} \right),$$

dove Λ é la funzione di von-Mangoldt (v. §1.1.2).

Abbiamo il

Teorema 5.3. *Siano $\varepsilon, A > 0$ costanti arbitrarie ed $N^{5/8+\varepsilon} \leq U \leq N$. Allora*

$$\sum_{N \leq 2n \leq 2N} |R(2n) - 2U\mathfrak{S}(2n)|^2 \ll_{\varepsilon, A} NU^2 L^{-A}.$$

Il Teorema 5.3 implica il

Corollario 5.3. *Siano $\varepsilon > 0$ ed $A > 0$ costanti arbitrarie. Allora $\forall 2n \in [N, 2N]$, tranne $\mathcal{O}(NL^{-A})$ eccezioni, l'equazione 5.11 é risolubile per $U = n^{5/8+\varepsilon}$ ed abbiamo*

$$R(2n) = 2U\mathfrak{S}(2n) + \mathcal{O}(UL^{-A}).$$

Ulteriori miglioramenti dei risultati di Zhan Tao sono stati ottenuti da Jia, con $U = n^{7/12+\varepsilon}$ (cit. in [C-L(2)] e [C-L(3)]). Comunque, egli usa metodi di Crivello (v. §4.2 e §4.3), che danno solo una minorazione per il numero di rappresentazioni. Jia deduce il suo risultato stabilendo che per un pari n tale che $2P < n \leq 2P + U$, con $\mathcal{O}(U \log^{-2} P)$ eccezioni, si ha

$$(5.12) |\{(p_1, p_2) : n = p_1 + p_2, P < p_1 \leq P + U, P - U < p_2 \leq P + U\}|$$

$$\gg \mathfrak{S}(n) \frac{U}{\log^2 P},$$

dove P é un intero sufficientemente grande, ε é una costante positiva sufficientemente piccola, ed $U = P^{7/12+40\varepsilon}$. Recentemente, Mikawa ha stabilito indipendentemente lo stesso risultato di Jia senza usare un Teorema della forma 5.12 (cit. in [C-L(2)] e [C-L(3)]). Si veda anche [C-L(3)], per quanto riguarda le applicazioni dei metodi di Crivello a tale problema.

5.3.1 Notazioni

A - una costante positiva arbitraria,
 B, C, D - costanti positive dipendenti da A ,
 ε - una costante positiva arbitrariamente piccola,
 V, Y - interi positivi tali che $N^{7/12+\varepsilon} \leq Y \leq V$,
 N, U - interi positivi tali che $N^{5/8+\varepsilon} \leq U \leq N$,
 $H = UL^{-B}$,
 $T \sim \frac{N}{4H}$,
 $\omega = N^{-1}U^2L^{-D}$,
 $P = L^C$,
 n_1, n_2, \dots, n_T - interi tali che $N/2 \leq n_1 < n_2 < \dots < n_T \leq N$,

$$S(\alpha; V, Y) \stackrel{def}{=} \sum_{V-Y < h \leq V} \Lambda(h)e(h\alpha),$$

$$S_n(\alpha) \stackrel{def}{=} S(\alpha; n+U, 2U), \quad T_n(\eta) \stackrel{def}{=} \sum_{n-U < h \leq n+U} e(h\eta).$$

$$I_{q,a} \stackrel{def}{=} \left\{ \frac{a}{q} + \eta, \eta \in \xi_q \right\}, \quad \text{con } \xi_q = \left(-\frac{L^D}{U}, \frac{L^D}{U} \right).$$

$$\mathfrak{M} \stackrel{def}{=} \bigcup_{q \leq P} \bigcup_{\substack{a=1 \\ (a,q)=1}}^q I_{q,a}, \quad \text{ed } \mathfrak{m} \stackrel{def}{=} \left[\frac{1}{\omega}, 1 + \frac{1}{\omega} \right] \setminus \mathfrak{M}.$$

$$\sum_{a=1}^q \stackrel{*}{def} \sum_{\substack{a=1 \\ (a,q)=1}}^q, \quad \delta_\chi \stackrel{def}{=} \begin{cases} 1 & \text{se } \chi = \chi_o \\ 0 & \text{altrimenti} \end{cases}, \quad \|\beta\| \stackrel{def}{=} \min_{n \in \mathbf{Z}} |\beta - n|.$$

$$\tau(\chi) \stackrel{def}{=} \sum_{a=1}^q \chi(a) e\left(\frac{a}{q}\right), \quad \text{somma di Gauss (v. §2.4.2)}$$

$$\psi(x, \chi) \stackrel{def}{=} \sum_{n \leq x} \Lambda(n) \chi(n) \quad (\text{v. §1.4.3}).$$

5.3.2 Sketch del metodo di dimostrazione

Abbiamo

$$R(2n) = \int_0^1 S_n(\alpha)^2 e(-2n\alpha) d\alpha.$$

Quindi

$$\sum_{N \leq 2n \leq 2N} |R(2n) - 2U \mathfrak{S}(2n)|^2 \ll \sum_{\mathfrak{m}} + \sum_{\mathfrak{M}},$$

dove

$$\begin{aligned} \sum_{\mathfrak{m}} &= \sum_{N \leq 2n \leq 2N} \left| \int_{\mathfrak{m}} S_n(\alpha)^2 e(-2n\alpha) d\alpha \right|^2, \\ \sum_{\mathfrak{M}} &= \sum_{N \leq 2n \leq 2N} \left| \int_{\mathfrak{M}} S_n(\alpha)^2 e(-2n\alpha) d\alpha - 2U \mathfrak{S}(2n) \right|^2. \end{aligned}$$

Allo scopo di provare il Teorema 5.3 é sufficiente dimostrare che

$$(5.13) \quad \sum_{\mathfrak{M}} \ll NU^2 L^{-A},$$

$$(5.14) \quad \sum_{\mathfrak{m}} \ll NU^2 L^{-A}.$$

5.3.3 Stime sugli archi maggiori

Sia $\alpha \in I_{q,a}$. Allora

$$\begin{aligned} S_n(\alpha) &= \sum_{n-U < h \leq n+U} \Lambda(h) e(h\alpha) = \\ &= \sum_{\substack{n-U < h \leq n+U \\ (h,q)=1}} \Lambda(h) e\left(\frac{ah}{q}\right) e(h\eta) + \mathcal{O}(L^2) = \\ &= \sum_{b=1}^q e\left(\frac{ab}{q}\right) \sum_{\substack{n-U < h \leq n+U \\ h \equiv b \pmod{q}}} \Lambda(h) e(h\eta) + \mathcal{O}(L^2) = \end{aligned}$$

$$\begin{aligned} \frac{1}{\varphi(q)} \sum_{\chi} \sum_{n-U < h \leq n+U} \Lambda(h) \chi(h) e(h\eta) \sum_{b=1}^q \bar{\chi}(b) e\left(\frac{ab}{q}\right) + \mathcal{O}(L^2) = \\ \frac{1}{\varphi(q)} \sum_{\chi} \chi(a) \tau(\bar{\chi}) W_n(\chi, \eta) + \frac{\mu(q)}{\varphi(q)} T_n(\eta) + \mathcal{O}(L^2), \end{aligned}$$

dove

$$W_n(\chi, \eta) \stackrel{def}{=} \sum_{n-U < h \leq n+U} \Lambda(h) \chi(h) e(h\eta) - \delta_{\chi} T_n(\eta).$$

Adesso usiamo la seguente versione del Teorema di Siegel-Walfisz per intervalli corti (v. [P-P-S(1)], [P-P-S(2)] e §2.4.3).

Se $V^{7/12+\varepsilon} \leq Y \leq V$ e $q \leq P = L^C$, allora

$$\psi(V, \chi) - \psi(V - Y, \chi) = \delta_{\chi} Y + \mathcal{O}_{\varepsilon, C, C_1}(Y L^{-C_1}), \quad \forall \chi \pmod{q}, \forall C_1 > 0.$$

Se $U \geq n^{5/8+\varepsilon}$, allora per somministrazione parziale (v. Lemma 2.1, §2.2.2), dal risultato di cui sopra e la stima $\tau(\chi) \ll q^{\frac{1}{2}}$ (v. §2.4.2),

$$S_n(\alpha) = \frac{\mu(q)}{\varphi(q)} T_n(\eta) + \mathcal{O}(U P^{1/2} L^{D-C_1}),$$

uniformemente per $\eta \in \xi_q$, $q \leq P$ e $(a, q) = 1$.

Quindi scriviamo

$$\begin{aligned} \int_{I_{a,q}} S_n(\alpha)^2 e(-2n\alpha) d\alpha &= \frac{\mu(q)^2}{\varphi(q)^2} e\left(-\frac{2na}{q}\right) \int_{\xi_q} T_n(\eta)^2 e(-2n\eta) d\eta \\ &+ \mathcal{O}(U P L^{-2C_1+3D}) = \frac{\mu(q)^2}{\varphi(q)^2} e\left(-\frac{2na}{q}\right) \int_0^1 T_n(\eta)^2 e(-2n\eta) d\eta \\ &+ \mathcal{O}(U P L^{-2C_1+3D}) + \mathcal{O}\left(\frac{U L^{-D}}{\varphi(q)^2}\right). \end{aligned}$$

Quindi, abbiamo che

$$\int_{\mathfrak{M}} S_n(\alpha)^2 e(-2n\alpha) d\alpha = 2U \mathfrak{S}(2n, P) + \mathcal{O}(T_1) + \mathcal{O}(T_2),$$

dove

$$\mathfrak{S}(2n, P) = \sum_{q \leq P} \sum_{a=1}^q \frac{\mu(q)^2}{\varphi(q)^2} e\left(-\frac{2na}{q}\right),$$

$$T_1 = UP^3L^{-2C_1+3D}, \quad T_2 = UL^{-D+1}.$$

Grazie ad argomenti classici ([Va], cap.3), otteniamo

$$\sum_{N \leq 2n \leq 2N} |\mathfrak{S}(2n, P) - \mathfrak{S}(2n)|^2 \ll NP^{-1}L^2,$$

dove

$$\mathfrak{S}(2n) = \sum_{q=1}^{\infty} \sum_{a=1}^q \frac{\mu(q)^2}{\varphi(q)^2} e\left(-\frac{2na}{q}\right).$$

Ne ricaviamo

$$\begin{aligned} \sum_{\mathfrak{M}} &= \sum_{N \leq 2n \leq 2N} \left| \int_{\mathfrak{M}} S_n(\alpha)^2 e(-2n\alpha) d\alpha - 2U\mathfrak{S}(2n) \right|^2 \ll \\ &U^2 \sum_{N \leq 2n \leq 2N} |\mathfrak{S}(2n, P) - \mathfrak{S}(2n)|^2 + \\ &+ \sum_{N \leq 2n \leq 2N} \left| \int_{\mathfrak{M}} S_n(\alpha)^2 e(-2n\alpha) d\alpha - 2U\mathfrak{S}(2n, P) \right|^2 \ll \\ &\ll NU^2P^{-1}L^2 + NU^2P^6L^{-4C_1+6D} + NU^2L^{-2D+2} \ll NU^2L^{-A}, \end{aligned}$$

ovvero la 5.13, nelle ipotesi

$$C > A + 2, \quad 2D > A + 2, \quad 4C_1 > A + 6(C + D).$$

5.3.4 Stime sugli archi minori

Adesso proviamo la 5.14.

Consideriamo degli interi n_1, n_2, \dots, n_T tali che

$$N/2 \leq n_1 < n_2 < \dots < n_T \leq N \quad e \quad \left[\frac{N}{2}, N\right] \subset \bigcup_{i=1}^T I_i,$$

con $I_i \stackrel{def}{=} [n_i - H, n_i + H]$. Per ogni $n \in I_i$, poniamo

$$S_n(\alpha) - S_{n_i}(\alpha) = S^+(\alpha) + S^-(\alpha),$$

dove

$$S^+(\alpha) \stackrel{def}{=} \begin{cases} S(\alpha; n_i - U, n_i - n), & \text{se } n < n_i, \\ 0, & \text{se } n = n_i, \\ S(\alpha; n + U, n - n_i), & \text{se } n_i < n, \end{cases}$$

$$S^-(\alpha) \stackrel{def}{=} \begin{cases} -S(\alpha; n_i + U, n_i - n), & \text{se } n < n_i, \\ 0, & \text{se } n = n_i, \\ -S(\alpha; n - U, n - n_i), & \text{se } n_i < n. \end{cases}$$

Quindi scriviamo

$$\begin{aligned} & \left| \int_{\mathbf{m}} S_n(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 \ll \left| \int_{\mathbf{m}} S_{n_i}(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 + \\ & \quad + \left| \int_{\mathbf{m}} S^+(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 + \\ & + \left| \int_{\mathbf{m}} S^-(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 + \left| \int_{\mathbf{m}} S^+(\alpha) S^-(\alpha) e(-2n\alpha) d\alpha \right|^2 + \\ & + \left| \int_{\mathbf{m}} S_{n_i}(\alpha) S^+(\alpha) e(-2n\alpha) d\alpha \right|^2 + \left| \int_{\mathbf{m}} S_{n_i}(\alpha) S^-(\alpha) e(-2n\alpha) d\alpha \right|^2. \end{aligned}$$

Usando la disuguaglianza di Cauchy-Schwarz e l'identità di Parseval, otteniamo

$$\begin{aligned} & \left| \int_{\mathbf{m}} S^+(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 \ll H^2 L^4, \\ & \left| \int_{\mathbf{m}} S^-(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 \ll H^2 L^4, \\ & \left| \int_{\mathbf{m}} S^+(\alpha) S^-(\alpha) e(-2n\alpha) d\alpha \right|^2 \ll H^2 L^4, \\ & \left| \int_{\mathbf{m}} S_{n_i}(\alpha) S^+(\alpha) e(-2n\alpha) d\alpha \right|^2 \ll UHL^4, \\ & \left| \int_{\mathbf{m}} S_{n_i}(\alpha) S^-(\alpha) e(-2n\alpha) d\alpha \right|^2 \ll UHL^4. \end{aligned}$$

Perciò si può scrivere

$$(5.15) \quad \sum_{\mathbf{m}} \ll \sum_{i=1}^T \sum_{n \in I_i} \left| \int_{\mathbf{m}} S_n(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 \ll \\ \sum_{i=1}^T \sum_{n \in I_i} \left| \int_{\mathbf{m}} S_{n_i}(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 + NUHL^4.$$

Dato che $N^{5/8+\varepsilon} \leq U \leq N$, dai Teoremi 2 e 3 di [Z], otteniamo che, $\forall B' > 0$,

$$S_{n_i}(\alpha) = S(\alpha; n_i + U, 2U) \ll UL^{-B'}, \quad \forall \alpha \in \mathbf{m}.$$

Quindi, per la disuguaglianza di Bessel e l'identità di Parseval, concludiamo che

$$(5.16) \quad \sum_{n \in I_i} \left| \int_{\mathbf{m}} S_{n_i}(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 \ll \int_{\mathbf{m}} |S_{n_i}(\alpha)|^4 d\alpha \\ \ll U^3 L^{-2(B'-1)}.$$

La 5.14 segue da 5.15 e 5.16 se $A+4 < B < 2B' - A - 2$ e da ciò il Teorema 5.3 é completamente dimostrato.

5.4 Crivello Largo ed $n(n+2)$ in Intervalli Corti

In questo paragrafo esponiamo i risultati di cui in [C-S(1)] sulla distribuzione nelle progressioni aritmetiche del polinomio $n(n+2)$, come, anche, dei polinomi quadratici riducibili, negli intervalli corti $n \in [x, x+h]$.

5.4.1 Enunciato dei risultati

Ci aspettiamo che, in media sui moduli dispari square-free d , valga la seguente stima (d' ora in poi scriveremo $m \equiv 0(q)$ per $m \equiv 0(\text{mod } q)$)

$$\sum_{\substack{x < n \leq x+h \\ n(n+2) \equiv 0(d)}} 1 = \frac{h}{d} \sum_{\substack{t|d \\ \frac{d}{x+h} < t < x+h}} 1 + R_d(x, h)$$

dove $h = x^\vartheta$ è la lunghezza intervallo corto ed $R_d(x, h)$ è un "buon" termine d' errore, in media su $d \sim D$, cioè su $D < d \leq 2D$.

Se ciò vale con $D = x^{\alpha-\varepsilon}$ ($\varepsilon \in]0, \alpha[$), diciamo che il **livello di distribuzione** della nostra successione (qui $n(n+2)$), nelle progressioni aritmetiche, è (almeno) α .

Per esempio, tramite argomenti standard, il livello di distribuzione di $n(n+2)$ con $n \in [x, x+x^\vartheta]$ è almeno ϑ . Per esempio, si veda [H-R], dove sono applicati metodi di Crivello classico (v. anche §4.2.1).

Un miglior livello di distribuzione di una successione nelle progressioni aritmetiche è di solito ottenuto attraverso l' introduzione delle forme bilineari (v. §4.6).

Nelle forme bilineari che considereremo i coefficienti γ_q e δ_r (con $q \sim Q$ e $r \sim R$) sono funzioni aritmetiche limitate.

Qui il livello di distribuzione è ovviamente $\log(QR)/\log(x)$.

Un importante esempio di trattamento non banale della forma bilineare del termine di resto che citiamo è relativo alla sequenza n^2+1 .

Iwaniec dimostrò nel 1978 [Iw(1)] che il livello di distribuzione in questo caso é $16/15$. Usando ciò provò che $n^2 + 1 = P_2$ per infiniti n (qui P_k denota **un intero con al massimo k fattori primi**), mentre il livello banale di distribuzione, cioè 1, permette di ottenere solo P_3 .

Nel nostro caso studiamo la forma bilineare ristretta ai moduli primi, cioè

$$\sum_{q \sim Q} \sum_{r \sim R} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n(n+2) \equiv 0(qr)}} 1,$$

dove q e r sono primi distinti (assumendo $QR > 2h + 2$).

Questa restrizione é legata alla natura aritmetica del problema ed é essenziale nella nostra dimostrazione, così come nei risultati su tale problema che citeremo in seguito.

Pensiamo di trattare, in futuro, anche il caso dei moduli generali.

Ci aspettiamo che la seguente stima valga in media

$$\sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n(n+2) \equiv 0(qr)}} 1 = \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \left(\frac{2h}{qr} + \sum_{\substack{x < n \leq x+h \\ n \equiv 0(qr)}} 1 + \sum_{\substack{x < n \leq x+h \\ n \equiv -2(qr)}} 1 \right),$$

con un "buon" termine d' errore, cioè $\mathcal{O}(h^{1-\varepsilon})$.

In [S-V] Salerno e Vitolo ottengono livello di distribuzione $4/3$ per gli intervalli lunghi, usando la stima di Weil per le somme di Kloosterman (v. il Lemma 3 di [Ho]; anche, §4.7).

In questo paragrafo usiamo il Crivello Largo per migliorare il livello di distribuzione da $4/3$ a $3/2$ (quando $h = x$) e, anche, per generalizzare i risultati di [S-V] agli intervalli corti.

Il livello di distribuzione raggiunto in questo modo per gli intervalli corti del tipo $[x, x + x^\vartheta]$ é $3\vartheta - 3/2$ e quindi é migliore del livello classico (cioé ϑ) quando $\vartheta > 3/4$ (includiamo il caso $\vartheta = 1$ degli intervalli "lunghi").

Vediamo i risultati ottenuti.

Teorema 5.4. *Siano $x > 4$, $3/4 < \vartheta \leq 1$, $x^\vartheta \leq h \leq x$, $0 < \varepsilon < \frac{4\vartheta-3}{10}$; siano $Q, R \in [1, h/2[$ e γ_q, δ_r siano funzioni aritmetiche limitate con supporto sui primi negli intervalli $]Q, 2Q],]R, 2R]$ (rispettivam.). Allora per $(q, r) = 1$*

$$(5.17) \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n(n+2) \equiv 0(qr)}} 1 = \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \left(\frac{2h}{qr} + \sum_{\substack{x < n \leq x+h \\ n \equiv 0(qr)}} 1 + \sum_{\substack{x < n \leq x+h \\ n \equiv -2(qr)}} 1 \right) + \mathcal{O}(h^{1-\varepsilon}),$$

nell' ipotesi che $R \leq h^2/x^{1+3\varepsilon}$, $Q \leq h/x^{1/2+2\varepsilon}$, $QR > 2h + 2$.

Come applicazione ricaviamo il livello di distribuzione $3(\vartheta - 1/2)$:

Corollario 5.4. *Siano $x, \vartheta, \varepsilon, q, r, \gamma_q, \delta_r$ come sopra; sia $h = x^\vartheta$. Allora la stima 5.17 del Teorema 5.4 vale per $QR = x^{3\vartheta-3/2-5\varepsilon}$.*

Come in [S-V] possiamo facilmente generalizzare i risultati del Teorema 5.4 e del Corollario 5.4 a polinomi quadratici riducibili, ricavando il

Corollario 5.5. *Sia $(an + b)(cn + d)$ un polinomio senza divisori fissi. Siano $x, \vartheta, h, \varepsilon, q, r, \gamma_q$ e δ_r come sopra, con qr coprimo con $[a, c, ad - bc]$. Allora le stesse conclusioni del Teorema 5.4 e del Corollario 5.4 valgono con $(an + b)(cn + d)$ al posto di $n(n + 2)$.*

5.4.2 Dimostrazione del Teorema e dei Corollari

Siano q ed r primi distinti (come in seguito) e definiamo

$$I \stackrel{def}{=} \sum_{q \sim Q} \sum_{r \sim R} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n(n+2) \equiv 0(qr)}} 1.$$

Dato che q ed r sono primi distinti

$$I = \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \left(\sum_{\substack{x < n \leq x+h \\ n \equiv 0(r) \\ n \equiv -2(q)}} 1 + \sum_{\substack{x < n \leq x+h \\ n \equiv 0(q) \\ n \equiv -2(r)}} 1 + \sum_{\substack{x < n \leq x+h \\ n \equiv 0(qr)}} 1 + \sum_{\substack{x < n \leq x+h \\ n \equiv -2(qr)}} 1 \right).$$

Quindi per provare la 5.17 basta provare che

$$(5.18) \quad \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n \equiv 0(r) \\ n \equiv -2(q)}} 1 = h \sum_{\substack{q \sim Q \\ r \sim R}} \frac{\gamma_q \delta_r}{qr} + \mathcal{O}(h^{1-\varepsilon}).$$

Chiaramente, é sufficiente allora dimostrare che

$$(5.19) \quad \Sigma \stackrel{def}{=} \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n \equiv 0(r) \\ n \equiv -2(q)}} 1 - \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n \equiv 0(r)}} \frac{1}{q} \ll h^{1-\varepsilon};$$

infatti la differenza fra i termini principali delle 5.18 e 5.19 é trascurabile, perchè

$$\sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n \equiv 0(r)}} \frac{1}{q} - h \sum_{\substack{q \sim Q \\ r \sim R}} \frac{\gamma_q \delta_r}{qr} = \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \mathcal{O}(1/q) \ll R$$

ed $R \ll h^{1-\varepsilon}$ per ipotesi.

Dalla ortogonalità dei caratteri additivi (v. §2.4.1 opp. [Vi], cap.1, Lemma 5)

$$(5.20) \quad \Sigma = \sum_{r \sim R} \delta_r \sum_{q \sim Q} \frac{\gamma_q}{q} \sum_{j < q} \sum_{x/r < m \leq (x+h)/r} e_q(j(m + 2\bar{r})).$$

Usiamo la trasformata di Mellin per scegliere gli interi m nell' intervallo $]x/r, (x+h)/r]$ (cioé per esprimere la relativa funzione caratteristica). Per fare ciò usiamo un opportuno kernel $K_r(\tau)$, con la proprietà

$$\int_{\mathbf{R}} |K_r(\tau)| d\tau \ll \log x;$$

in questo modo scrivendo $m \simeq x/R$ per indicare che $m \in]x/2R, 2x/R]$ otteniamo dalla 5.20

$$\begin{aligned} \Sigma &= \sum_{r \sim R} \delta_r \sum_{q \sim Q} \frac{\gamma_q}{q} \sum_{j < q} \sum_{m \simeq x/R} e_q(j(m + 2\bar{r})) \int_{\mathbf{R}} K_r(\tau) m^{i\tau} d\tau = \\ &= \sum_{r \sim R} \delta_r \int_{\mathbf{R}} K_r(\tau) \sum_{q \sim Q} \frac{\gamma_q}{q} \sum_{j < q} e_q(2j\bar{r}) \sum_{m \simeq x/R} m^{i\tau} e_q(jm) d\tau; \end{aligned}$$

quindi, per la disuguaglianza di Hölder (ricordando che $\gamma_q, \delta_r \ll 1$) ricaviamo (per un certo $\tau \in \mathbf{R}$)

$$\begin{aligned} \Sigma &\ll (\log x) \sum_{r \sim R} \left| \sum_{q \sim Q} \frac{\gamma_q}{q} \sum_{j < q} \left(\sum_{m \simeq x/R} m^{i\tau} e_q(jm) \right) e_q(2j\bar{r}) \right| \ll \\ &\ll (\log x) \sum_{r \sim R} \left| \sum_{q \sim Q} \frac{\gamma_q}{q} \sum_{j < q} \left(\sum_{m \simeq x/R} m^{i\tau} e_q(\bar{2}jm) \right) e_q(j\bar{r}) \right|. \end{aligned}$$

Applicando la disuguaglianza di Cauchy otteniamo (dato che q è primo, quindi la somma su j è sulle classi di resto ridotte mod q)

$$\Sigma \ll (\log x) \sqrt{R} \sqrt{\sum_{r \sim R} \left| \sum_{q \sim Q} \frac{\gamma_q}{q} \sum_{j \leq q}^* \left(\sum_{m \simeq x/R} m^{i\tau} e_q(\bar{2}jm) \right) e_q(j\bar{r}) \right|^2},$$

da cui, per il Lemma 5.3 (v. prossimo sottoparagrafo)

$$\begin{aligned} (5.21) \quad \Sigma &\ll (\log x) \sqrt{R} \sqrt{x^{2\delta} (R + Q^2) \sum_{q \sim Q} \frac{1}{q^2} \sum_{j \leq q} \left| \sum_{m \simeq x/R} m^{i\tau} e_q(jm) \right|^2} \\ &\ll x^{2\delta} \sqrt{R} \sqrt{(R + Q^2) \sum_{q \sim Q} \frac{1}{q} \frac{x}{R}} \ll x^{2\delta} \sqrt{(R + Q^2)x}. \end{aligned}$$

Per poter avere $\Sigma \ll h^{1-\varepsilon}$ basta, per la 5.19, scegliere in 5.21, per esempio, $\delta = \varepsilon/4$ e

$$R \leq (h^2/x)x^{-3\varepsilon}, \quad Q \leq (h/x^{1/2})x^{-2\varepsilon};$$

da qui il Teorema 5.4.

(Quindi questo approccio non impone vincoli a ϑ , tranne il banale, cioè $\vartheta > 1/2$; comunque, il livello di distribuzione diventa maggiore di ϑ , come già detto, solo per $\vartheta > 3/4$).

La dimostrazione del Corollario 5.4 é immediata, perché basta scegliere nel Teorema 5.4 $R = (h^2/x)x^{-3\varepsilon}$, $Q = (h/x^{1/2})x^{-2\varepsilon}$. Il Corollario 5.5 si può dimostrare in maniera analoga al Corollario 1.2 in [S-V].

5.4.3 Una variante del Crivello Largo

Lemma 5.2. *Siano $Q, N \in \mathbf{N}$ ed $\{a_n\}$ una successione di numeri complessi; allora*

$$(5.22) \quad \sum_{q \leq Q} \sum_{a \leq q}^* \left| \sum_{n \leq N} a_n e_q(an) \right|^2 \ll (N + Q^2) \sum_{n \leq N} |a_n|^2,$$

dove lo $*$ significa (come al solito) che la somma é sulle classi di resto ridotte (mod q).

Questa é la ben nota disuguaglianza di Crivello Largo (per una dimostrazione standard v. [B(1)], p.13; cfr. anche §4.3).

Da tale Lemma deriviamo, in modo elementare, un Crivello Largo nel quale ci sono le classi di resto inverse:

Lemma 5.3. *Siano $Q, N \in \mathbf{N}$ e $\lambda_{a,q} \in \mathbf{C}$ ($\forall a, q \in N$); allora $\forall \delta > 0$ abbiamo*

$$(5.23) \quad \sum_{n \leq N} \left| \sum_{\substack{q \leq Q \\ (q, n) = 1}} \sum_{a \leq q}^* \lambda_{a,q} e_q(a\bar{n}) \right|^2 \ll (QN)^\delta (N + Q^2) \sum_{q \leq Q} \sum_{a \leq q}^* |\lambda_{a,q}|^2.$$

Dimostrazione. Proviamo che

$$(5.24) \quad \sum_{q \leq Q} \sum_{a \leq q}^* \left| \sum_{\substack{n \leq N \\ (n, q) = 1}} a_n e_q(a\bar{n}) \right|^2 \ll (QN)^\delta (N + Q^2) \sum_{n \leq N} |a_n|^2,$$

poichè la 5.23 segue per il Principio di Dualità (v. [M(2)], p.134; v. anche [Te], Lemma 5.1, p.63).

A tale scopo svolgiamo il quadrato nella 5.24 ottenendo

$$\sum_{q \leq Q} \sum_{a \leq q}^* \sum_{\substack{n_1 \leq N \\ (n_1, q) = 1}} \sum_{\substack{n_2 \leq N \\ (n_2, q) = 1}} a_{n_1} \overline{a_{n_2}} e_q(a(\overline{n_1} - \overline{n_2})),$$

da cui, ponendo $b = a\overline{n_1 n_2}$ ricaviamo (dato che $(n_1, q) = (n_2, q) = 1$)

$$\sum_{q \leq Q} \sum_{b \leq q}^* \left| \sum_{\substack{n \leq N \\ (n, q) = 1}} a_n e_q(bn) \right|^2,$$

cioè il primo membro della 5.24; perciò basterà provare la seguente variante del Crivello Largo :

$$(5.25) \quad \sum_{q \leq Q} \sum_{a \leq q}^* \left| \sum_{\substack{n \leq N \\ (n, q) = 1}} a_n e_q(bn) \right|^2 \ll (QN)^\delta (N + Q^2) \sum_{n \leq N} |a_n|^2.$$

Qui il primo membro é

$$\sum_{q \leq Q} \sum_{a \leq q}^* \left| \sum_{\substack{n \leq N \\ d|n \\ d|q}} \mu(d) a_n e_q(an) \right|^2 = \sum_{q \leq Q} \sum_{a \leq q}^* \left| \sum_{\substack{d \leq N \\ d|q}} \mu(d) \sum_{\substack{m \leq \frac{N}{d}}} a_{md} e_q(amd) \right|^2,$$

da cui (per la disuguaglianza di Cauchy e la stima per la funzione divisori $\tau(q) \ll q^\delta$, v. [H-W], p. 260)

$$\sum_{q \leq Q} \sum_{a \leq q}^* \left| \sum_{\substack{n \leq N \\ (n, q) = 1}} a_n e_q(bn) \right|^2 \ll Q^\delta \sum_{d \leq N} d \sum_{\substack{g \leq \frac{Q}{d} \\ c \leq g}} \sum_{m \leq N/d}^* \left| \sum_{m \leq N/d} a_{md} e_g(cm) \right|^2.$$

Quindi, applicando il Crivello Largo, cioè per la 5.22, abbiamo

$$\sum_{q \leq Q} \sum_{a \leq q}^* \left| \sum_{\substack{n \leq N \\ (n, q) = 1}} a_n e_q(bn) \right|^2 \ll Q^\delta \sum_{d \leq N} d \left(\frac{N}{d} + \frac{Q^2}{d^2} \right) \sum_{m \leq N/d} |a_{md}|^2 \ll$$

$$\begin{aligned} &\ll Q^\delta \left(N \sum_{n \leq N} |a_n|^2 \sum_{\substack{d|n \\ d \leq N}} 1 + Q^2 \sum_{n \leq N} |a_n|^2 \sum_{\substack{d|n \\ d \leq N}} \frac{1}{d} \right) \\ &\ll Q^\delta (N + Q^2) N^\delta \sum_{n \leq N} |a_n|^2, \end{aligned}$$

da cui la stima 5.25, che completa la dimostrazione del Lemma 5.3.

5.5 Dispersione ed $n(n+2)$ in Intervalli Corti

In questo paragrafo continuiamo lo studio della distribuzione nelle progressioni aritmetiche del polinomio $n(n+2)$ e, anche, dei polinomi quadratici riducibili, negli intervalli corti che abbiamo cominciato con il paragrafo precedente. Qui, invece del Crivello Largo (v. [B(1)] e [B(2)]; cfr. anche §4.3), usiamo il metodo della Dispersione (v. [L]; cfr. anche §4.4) per avere risultati che sono indipendenti (anche se da qualche punto di vista più forti) rispetto ai precedenti.

5.5.1 Enunciato dei risultati

Tramite il metodo della Dispersione otteniamo i seguenti risultati.

Teorema 5.5. *Siano $x > 4$, $0 < \vartheta \leq 1$, $x^\vartheta \leq h \leq x$, $0 < \varepsilon \leq \frac{1}{8}$; siano $Q, R \in [1, h/2[$ e γ_q, δ_r siano funzioni aritmetiche limitate con supporto sui primi di $]Q, 2Q],]R, 2R]$ (rispettivamente). Allora, per $(q, r) = 1$, vale la 5.17, sotto le ipotesi $R \leq h^{1-2\varepsilon}$, $Q \leq R^{1/2}h^{-\varepsilon}$, $QR > 2h + 2$.*

Come applicazione abbiamo livello di distribuzione $3\vartheta/2$

Corollario 5.6. *Siano $x, \vartheta, \varepsilon, q, r, \gamma_q, \delta_r$ come sopra. Allora la stima 5.17 del Teorema 5.5 vale per $QR = h^{3/2-4\varepsilon}$.*

Come nel paragrafo precedente, generalizziamo il Teorema 5.5 ed il Corollario 5.6 per avere il

Corollario 5.7. *Sia $(an+b)(cn+d)$ un polinomio senza divisori fissi. Siano $x, \vartheta, h, \varepsilon, q, r, \gamma_q$ e δ_r come sopra, con qr coprimo con $[a, c, ad-bc]$. Allora le stesse conclusioni del Teorema 5.5 e del Corollario 5.6 valgono con $(an+b)(cn+d)$ al posto di $n(n+2)$.*

(Stavolta non dimostreremo i Corollari, perchè ci riferiremo al §5.4.).

Osserviamo che tramite il metodo della Dispersione andiamo oltre il livello banale di distribuzione ϑ per ogni $\vartheta > 0$, mentre con il Crivello Largo (v. paragrafo precedente) ciò é vero solo per $\vartheta > 3/4$.

Infatti, il livello di distribuzione dato dal Crivello Largo é minore di quello dato dalla Dispersione.

Nonostante ciò i Teoremi principali (come, anche, i rispettivi Corollari) sono indipendenti fra loro, a causa di differenti range di Q ed R dati dai due risultati.

5.5.2 Dimostrazione del Teorema

Partiamo, per dimostrare il Teorema 5.5, dalla 5.19 del paragrafo precedente ed osserviamo che, poichè $qr > 2h + 2$ e q è primo

$$\Sigma = \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \left(\sum_{\substack{\frac{x}{r} < m \leq \frac{x+h}{r} \\ mr \equiv -2(q)}} 1 - \sum_{\substack{\frac{x}{r} < m \leq \frac{x+h}{r} \\ (m,q)=1}} \frac{1}{q} \right) + \mathcal{O}(R),$$

$\mathcal{O}(R)$ essendo trascurabile come prima; quindi per la disuguaglianza di Cauchy

$$\Sigma \ll \sqrt{R} \sqrt{\Delta},$$

dove, diciamo, $\Delta = \Delta(x, h, Q, R)$ è uguale a

$$\Delta \stackrel{def}{=} \sum_{r \sim R} \left| \sum_{q \sim Q} \gamma_q \left(\sum_{\substack{\frac{x}{r} < m \leq \frac{x+h}{r} \\ mr \equiv -2(q)}} 1 - \sum_{\substack{\frac{x}{r} < m \leq \frac{x+h}{r} \\ (m,q)=1}} \frac{1}{q} \right) \right|^2.$$

Quindi, per provare che $\Sigma \ll h^{1-\varepsilon}$, proveremo la maggiorazione

$$(5.26) \quad \Delta \ll h^{2-2\varepsilon} / R.$$

Per poter fare ciò applichiamo il metodo della Dispersione a Δ ; svolgiamo il quadrato e scambiamo la somma su r e le somme interne per avere

$$\Delta = \sum_{q_1, q_2 \sim Q} \gamma_{q_1} \overline{\gamma_{q_2}} \sum_{\substack{\frac{x}{2R} < m_1 \leq \frac{x+h}{R} \\ (m_1, q_1)=1}} \sum_{\substack{\frac{x}{2R} < m_2 \leq \frac{x+h}{R} \\ (m_2, q_2)=1}} E,$$

dove $E = E(m_1, m_2, q_1, q_2, x, h, R)$ è definito da

$$E \stackrel{def}{=} \sum_{\substack{X < r \leq Y \\ rm_1 \equiv -2(q_1) \\ rm_2 \equiv -2(q_2)}} 1 - \sum_{\substack{X < r \leq Y \\ rm_1 \equiv -2(q_1)}} \frac{1}{q_2} - \sum_{\substack{X < r \leq Y \\ rm_2 \equiv -2(q_2)}} \frac{1}{q_1} + \sum_{X < r \leq Y} \frac{1}{q_1 q_2},$$

$X = X(m_1, m_2, x, R) \stackrel{def}{=} \max(R, x/m_1, x/m_2)$, $Y = Y(m_1, m_2, x, h, R) \stackrel{def}{=} \min(2R, (x+h)/m_1, (x+h)/m_2)$; qui tutte le somme sugli r hanno $(r, q_1 q_2) = 1$.

Quindi, per queste definizioni e le nostre ipotesi su R , ognuna delle somme su m_1 e m_2 ha lunghezza $\mathcal{O}(h/R)$.

(Tale informazione sarà implicita nel seguito.)

Innanzitutto, valutiamo la diagonale di Δ , cioè Δ' , diciamo

$$\Delta' \stackrel{def}{=} \sum_{q \sim Q} |\gamma_q|^2 \sum_{\substack{\frac{x}{2R} < m_1 \leq \frac{x+h}{R} \\ (m_1, q_1)=1}} \sum_{\substack{\frac{x}{2R} < m_2 \leq \frac{x+h}{R} \\ (m_2, q_2)=1}} E,$$

dove stavolta $E = E(m_1, m_2, q, q, x, h, R)$ é per definizione $E \stackrel{def}{=} E_1 + E_2 + E_3 + E_4$, pari a

$$\sum_{\substack{X < r \leq Y \\ r m_1 \equiv -2(q) \\ r m_2 \equiv -2(q)}} 1 - \sum_{\substack{X < r \leq Y \\ r m_1 \equiv -2(q)}} \frac{1}{q} - \sum_{\substack{X < r \leq Y \\ r m_2 \equiv -2(q)}} \frac{1}{q} + \sum_{X < r \leq Y} \frac{1}{q^2}.$$

Il contributo di E_1 in Δ' é maggiorato da

$$\begin{aligned} \sum_{q \sim Q} \sum_{\substack{\frac{x}{2R} < m_1 \leq \frac{x+h}{R} \\ r m_1 \equiv -2(q)}} \sum_{\substack{R < r \leq 2R \\ \frac{x}{m_1} < r \leq \frac{x+h}{m_1} \\ r m_1 \equiv -2(q)}} \sum_{\substack{\frac{x}{r} < m_2 \leq \frac{x+h}{r} \\ r m_2 \equiv -2(q)}} 1 \ll \sum_{q \sim Q} \sum_{\substack{\frac{x}{2R} < m_1 \leq \frac{x+h}{R} \\ r m_1 \equiv -2(q)}} \left(\frac{h}{m_1 q} + 1 \right) \ll \\ \ll h \frac{h R}{R x} + Q \frac{h}{R} \ll h + \frac{Qh}{R} \end{aligned}$$

(avendo scambiato la somma su r con la somma su m_2), dal momento che, per le nostre ipotesi, $QR > h$ e $h \leq x$.

Il contributo di E_2 (quello di E_3 é analogo) é maggiorato da (dato che $QR > h$)

$$\sum_{q \sim Q} \frac{1}{q} \sum_{r \sim R} \sum_{\substack{\frac{x}{r} < m_2 \leq \frac{x+h}{r} \\ \frac{x}{m_1} < r \leq \frac{x+h}{m_1} \\ m_1 r \equiv -2(q)}} 1 \ll \sum_{q \sim Q} \frac{1}{q} \sum_{r \sim R} \frac{h}{R} \ll h,$$

dopo lo scambio della somma su r con la doppia somma su m_1, m_2 .

Infine, il contributo di E_4 é dato da

$$\sum_{q \sim Q} \frac{1}{q^2} \sum_{\substack{\frac{x}{2R} < m_1 \leq \frac{x+h}{R} \\ \frac{x}{2R} < m_2 \leq \frac{x+h}{R}}} \sum_{X < r \leq Y} 1 \ll \frac{1}{Q} \sum_{r \sim R} \frac{h^2}{R^2} \ll \frac{h^2}{QR} \ll h.$$

Quindi

$$\Delta' \ll h + \frac{hQ}{R} \ll \frac{h^{2-2\varepsilon}}{R},$$

come richiesto nella 5.26 (le nostre ipotesi su Q, R implicano $R \leq h^{1-2\varepsilon}$ e $Q \leq h^{1-2\varepsilon}$).

Adesso stimiamo $\Delta - \Delta'$ (i termini non diagonali di Δ).

Dapprima proviamo che si può togliere la condizione $(r, q_1 q_2) = 1$ dalle ultime tre somme di E in $\Delta - \Delta'$. Infatti le somme in E che hanno $(r, q_1 q_2) > 1$ sono (dato che q_1 e q_2 sono primi distinti), diciamo

$$E' \stackrel{def}{=} - \sum_{\substack{X < r \leq Y \\ rm_1 \equiv -2(q_1) \\ q_2 | r}} \frac{1}{q_2} + \sum_{\substack{X < r \leq Y \\ (r, q_1) = 1 \\ q_2 | r}} \frac{1}{q_1 q_2} - \sum_{\substack{X < r \leq Y \\ rm_2 \equiv -2(q_2) \\ q_1 | r}} \frac{1}{q_1} + \sum_{\substack{X < r \leq Y \\ (r, q_2) = 1 \\ q_1 | r}} \frac{1}{q_1 q_2}$$

e, diciamo,

$$E'' \stackrel{def}{=} \sum_{\substack{X < r \leq Y \\ q_1 q_2 | r}} \frac{1}{q_1 q_2}.$$

Il loro contributo a $\Delta - \Delta'$ é trascurabile, cioè é $\mathcal{O}(h^{2-2\varepsilon}/R)$, come richiesto nella 5.26; infatti tornando a scambiare le somme su r e su m_1, m_2 otteniamo

$$\begin{aligned} & \sum_{\substack{\frac{x}{2R} < m_1 \leq \frac{x+h}{R} \\ (m_1, q_1) = 1}} \sum_{\substack{\frac{x}{2R} < m_2 \leq \frac{x+h}{R} \\ (m_2, q_2) = 1}} E' = \\ &= \frac{1}{q_2} \sum_{\substack{r \sim R \\ (r, q_1) = 1 \\ q_2 | r}} \sum_{\substack{\frac{x}{r} < m_2 \leq \frac{x+h}{r}}} \mathcal{O}(1) + \frac{1}{q_1} \sum_{\substack{r \sim R \\ (r, q_2) = 1 \\ q_1 | r}} \sum_{\substack{\frac{x}{r} < m_1 \leq \frac{x+h}{r}}} \mathcal{O}(1), \end{aligned}$$

e quest' ultima dà un contributo $\mathcal{O}(h)$ in $\Delta - \Delta'$, che é trascurabile, come visto prima (abbiamo usato l' ipotesi $QR > h$).

Allo stesso modo, E'' contribuisce a $\Delta - \Delta'$ con (dato che $4Q^2 < R$)

$$\sum_{q_1, q_2 \sim Q} \frac{1}{q_1 q_2} \sum_{\substack{r \sim R \\ q_1 q_2 | r}} \sum_{\substack{\frac{x}{r} < m_1 \leq \frac{x+h}{r} \\ \frac{x}{r} < m_2 \leq \frac{x+h}{r}}} 1 \ll \sum_{q_1, q_2 \sim Q} \frac{1}{q_1^2 q_2^2} \frac{h^2}{R} \ll \frac{h^2}{Q^2 R} \ll h,$$

che é anch' esso trascurabile (di nuovo, usando $QR > h$).

Quindi, da un calcolo diretto, E in $\Delta - \Delta'$ é

$$\begin{aligned} & \left(\left[\frac{Y-c}{q_1 q_2} \right] - \left[\frac{X-c}{q_1 q_2} \right] \right) - \frac{1}{q_2} \left(\left[\frac{Y+2\overline{m}_1}{q_1} \right] - \left[\frac{X+2\overline{m}_1}{q_1} \right] \right) \\ & - \frac{1}{q_1} \left(\left[\frac{Y+2\overline{m}_2}{q_2} \right] - \left[\frac{X+2\overline{m}_2}{q_2} \right] \right) + \frac{Y-X}{q_1 q_2} \end{aligned}$$

(dove

$$(5.27) \quad c \equiv -2\overline{m}_2 q_1 \overline{q}_1 - 2\overline{m}_1 q_2 \overline{q}_2 \pmod{q_1 q_2},$$

con $\overline{m}_1 m_1 \equiv 1 \pmod{q_1}$, $\overline{m}_2 m_2 \equiv 1 \pmod{q_2}$, $\overline{q}_1 q_1 \equiv 1 \pmod{q_2}$
e $\overline{q}_2 q_2 \equiv 1 \pmod{q_1}$),

che é $\mathcal{O}(1)$, perchè i termini principali si cancellano e le parti frazionarie danno $\mathcal{O}\left(1 + \frac{1}{q_2} + \frac{1}{q_1}\right)$.

Quindi otteniamo

$$\Delta - \Delta' \ll \sum_{q_1, q_2 \sim Q} \sum_{\frac{x}{2R} < m_1 \leq \frac{x+h}{R}} \sum_{\frac{x}{2R} < m_2 \leq \frac{x+h}{R}} 1 \ll Q^2 \frac{h^2}{R^2}$$

e quest' ultimo é $\mathcal{O}(h^{2-2\varepsilon}/R)$, dato che $Q^2 \leq Rh^{-2\varepsilon}$, come richiesto dalle ipotesi del Teorema 5.5.

5.6 Somme di Kloosterman ed $n(n+2)$ in Intervalli Corti

In questa sezione continuiamo lo studio della distribuzione nelle progressioni aritmetiche di $n(n+2)$ (e anche dei polinomi quadratici riducibili) negli intervalli corti, cominciata nelle sezioni precedenti (v. [C-S(1)] e [C-S(2)]). Adesso, invece del Crivello Largo (v. [B(1)] e [B(2)]; cfr. anche §4.3), usiamo ancora la Dispersione (v. [L]; cfr. anche §4.4), combinata stavolta non con una stima banale sulle parti frazionarie, ma con una stima per le forme bilineari di somme di Kloosterman (v. [D-F-I]) che ci consente di dimostrare risultati più forti di quelli in §5.5 (anche se ancora indipendenti da quelli in §5.4). Infatti, stavolta il livello di distribuzione é $143\vartheta/95$, cioè $143/95$ negli intervalli "lunghi" (v. il seguente Corollario 5.8).

Assumeremo d' ora in poi che $Q > R^{1/2}h^{-\varepsilon/2}$, altrimenti ci si riconduce alla dimostrazione della sezione precedente.

Nella sezione successiva alla prossima daremo, ovviamente, solo la parte di dimostrazione di [C-S(3)] non contenuta già in [C-S(2)] (per la quale v. §5.5).

5.6.1 Enunciato dei risultati

Abbiamo il

Teorema 5.6. *Siano $x > 4$, $0 < \vartheta \leq 1$, $x^\vartheta \leq h \leq x$, $0 < \varepsilon < \frac{12}{119}$; siano $Q, R \in [1, h/2[$ e γ_q, δ_r siano funzioni aritmetiche limitate, con supporto sui primi di $]Q, 2Q],]R, 2R]$ (rispettivam.). Allora per $(q, r) = 1$ vale la 5.17, nelle ipotesi $h^{3\varepsilon} \leq R \leq h^{1-3\varepsilon}$, $h^{3\varepsilon} \leq Q \leq R^{48/95}h^{-2\varepsilon}$, $QR > 2h + 2$.*

Come applicazione abbiamo livello di distribuzione $143\vartheta/95$

Corollario 5.8. *Siano $x, \vartheta, \varepsilon, q, r, \gamma_q, \delta_r$ come sopra. Allora la stima 5.17 del Teorema 5.6 vale per $QR = h^{143/95-7\varepsilon}$.*

Come in [S-V] generalizziamo il Teorema 5.6 ed il Corollario 5.8 ai polinomi quadratici riducibili

Corollario 5.9. *Sia $(an+b)(cn+d)$ un polinomio senza divisori fissi. Siano $x, \vartheta, h, \varepsilon, q, r, \gamma_q$ e δ_r come sopra, con qr coprimo con $[a, c, ad-bc]$. Allora le stesse conclusioni del Teorema 5.6 e del Corollario 5.8 valgono con $(an+b)(cn+d)$ al posto di $n(n+2)$.*

5.6.2 Stime sulle parti frazionarie tramite somme di Kloosterman

Abbiamo (v. §5.5)

$$(5.28) \quad E - E' - E'' = \sum_{\substack{X < r \leq Y \\ r \equiv c(q_1 q_2)}} 1 - \sum_{X < r \leq Y} \frac{1}{q_1 q_2} + \mathcal{O}\left(\frac{1}{q_2} + \frac{1}{q_1}\right),$$

nella quale il resto é accettabile, dato che (per l' ipotesi $Q \leq Rh^{-2\varepsilon}$) contribuisce con $\mathcal{O}(h^{2-2\varepsilon}/R)$ alla 5.26.

Prima di proseguire, dobbiamo trattare il caso in cui la 5.28 é sommata con $m_1 = m_2$ in $\Delta - \Delta'$, per mostrare che il suo contributo alla 5.26 é pure trascurabile. Dato che la condizione $r \equiv c(q_1 q_2)$ nella 5.28 é equivalente, in questo caso, ad $r \equiv -2\overline{m} \pmod{q_1 q_2}$, otteniamo

$$\sum_{\substack{q_1, q_2 \sim Q \\ (q_1, q_2) = 1}} \gamma_{q_1} \overline{\gamma_{q_2}} \sum_{\substack{\frac{x}{2R} < m \leq \frac{x+h}{R} \\ (m, q_1 q_2) = 1}} (E - E' - E'') \ll \sum_{r \sim R} \sum_{\substack{\frac{x}{r} < m \leq \frac{x+h}{r}}} \sum_{\substack{Q^2 < d \leq 4Q^2 \\ d | (mr+2)}} \tau(d)$$

e quest' ultimo é $\mathcal{O}(h^{1+\varepsilon})$, usando la stima $\tau(d) \ll d^\mu$, $\mu > 0$ "piccolo" (v. [H-W], p.260) due volte; dato che $R \leq h^{1-3\varepsilon}$, ciò dà un contributo trascurabile alla 5.26.

Perciò nel seguito possiamo supporre che m_1 ed m_2 sono distinti.

Qui é richiesta la seguente espansione di Fourier (regolarizzata) della parte frazionaria.

Lemma 5.4. *Per ogni $0 < \sigma < 1/2$ e per ogni numero naturale k esistono due funzioni f e g periodiche di periodo 1 (dipendenti da σ e k) tali che ($e(t)$ é definita, come al solito, da $e^{2\pi it}$)*

$$\left| \{y\} - \frac{1}{2} - f(y) \right| \leq g(y), \quad f(y) = \sum_{j \in \mathbf{Z}^*} a_j e(jy), \quad g(y) = \sum_{j \in \mathbf{Z}} b_j e(jy),$$

dove i coefficienti di Fourier (dipendenti da σ e k) soddisfano

$$b_0 \ll_k \sigma \quad e \quad |a_j|, |b_j| \ll_k \min\left(\frac{1}{|j|}, \frac{1}{|j|} \left(\frac{1}{|j|\sigma}\right)^{k+1}\right) \quad \forall j \in \mathbf{Z}^*.$$

5.6. SOMME DI KLOOSTERMAN ED $N(N+2)$ IN INTERVALLI CORTI 113

Applichiamo il Lemma 5.4 per scrivere

$$(5.29) \quad \{y\} - \frac{1}{2} = \sum_{j \in \mathbf{Z}^*} c_j e(jy) + \mathcal{O}_k(\sigma),$$

dove

$$(5.30) \quad |c_j| \ll_k \min \left(\frac{1}{|j|}, \frac{1}{|j|} \left(\frac{1}{|j|\sigma} \right)^k \right) \quad \forall j \in \mathbf{Z}^*.$$

Quindi, definendo $\mathcal{F} = \mathcal{F}(q_1, q_2, m_1, m_2, R, x, h)$ come

$$\mathcal{F} \stackrel{def}{=} \sum_{\substack{X < r \leq Y \\ r \equiv c \pmod{q_1 q_2}}} 1 - \sum_{X < r \leq Y} \frac{1}{q_1 q_2} = \left\{ \frac{X-c}{q_1 q_2} \right\} - \left\{ \frac{Y-c}{q_1 q_2} \right\}$$

otteniamo

$$(5.31) \quad \mathcal{F} = \sum_{j \in \mathbf{Z}^*} c_j (e_{q_1 q_2}(jX) - e_{q_1 q_2}(jY)) e_{q_1 q_2}(-jc) + \mathcal{O}_k(\sigma),$$

dove c é dato dalla 5.27 (e, come al solito, $e_d(n) \stackrel{def}{=} e(n/d)$).

Per le 5.29 e 5.30 scegliamo (dato che, come già detto, possiamo supporre che $Q^2 > Rh^{-\varepsilon}$)

$$\sigma \stackrel{def}{=} \frac{R}{Q^2} h^{-2\varepsilon} \quad (\rightarrow 0)$$

per rendere il contributo di σ nella 5.31 alla 5.26 trascurabile. Inoltre, scegliendo

$$J \stackrel{def}{=} \frac{Q^2}{R} h^{3\varepsilon} \quad (\geq h^{2\varepsilon} \rightarrow \infty)$$

abbiamo

$$\sum_{|j| > J} |c_j| \ll_k \frac{1}{\sigma^k} \sum_{|j| > J} |j|^{k+1} \ll_k \left(\frac{1}{\sigma J} \right)^k,$$

che é $\mathcal{O}_k \left(\frac{R}{Q^2} h^{-2\varepsilon} \right)$, cioè $\mathcal{O}_\varepsilon \left(\frac{R}{Q^2} h^{-2\varepsilon} \right)$ (con la scelta di un k "grande", dipendente da ε); ciò porta ancora ad un contributo alla 5.26 che é trascurabile nella 5.28.

Ovviamente, allo stesso modo,

$$(5.32) \quad \sum_{|j| > G} |c_j| \ll_\varepsilon \frac{R}{Q^2} h^{-2\varepsilon}, \quad \forall G \geq J.$$

Quindi la serie nella 5.31 può essere sostituita (riducendoci, senza ledere di generalità, agli indici j positivi) dalla somma :

$$\mathcal{F} = \sum_{j \leq q_1 q_2} c_j (e_{q_1 q_2}(jX) - e_{q_1 q_2}(jY)) e_{q_1}(2j\overline{m_1 q_2}) e_{q_2}(2j\overline{m_2 q_1}),$$

diciamo, e più in generale da ogni somma su $j \leq G$, dove per la 5.32 possiamo scegliere qualunque $G \geq J$; in particolare, la nostra scelta di G é ammissibile, essendo $q_1 q_2 > Q^2$ and $Q^2 \geq J$ (grazie all' ipotesi $R \geq h^{3\epsilon}$). (Nel seguito ometteremo da \mathcal{F} tutti i contributi che, per la 5.32 sono, nella 5.28, termini trascurabili per le somme nella 5.26).

Senza ledere di generalità stimiamo (con $W = X, Y \ll R$, dipendente da m_1, m_2, R, x, h , ma non da q_1, q_2)

$$(5.33) \quad \mathcal{F} = \sum_{j \leq q_1 q_2} c_j e_{q_1 q_2}(jW) e_{q_1}(2j\overline{m_1 q_2}) e_{q_2}(2j\overline{m_2 q_1}).$$

Poniamo $j = gm_1 m_2 \pmod{q_1 q_2}$, così che \mathcal{F} nella 5.33 diventa

$$\sum_{g \leq q_1 q_2} d_g e_{q_1 q_2}(gm_1 m_2 W) e_{q_1}(2gm_2 \overline{q_2}) e_{q_2}(2gm_1 \overline{q_1}),$$

dove d_g é il coefficiente c_v , con indice $1 \leq v \leq q_1 q_2$ tale che si abbia $v \equiv gm_1 m_2 \pmod{q_1 q_2}$.

Qui vogliamo applicare la **relazione di reciprocità**, ovvero

$$(5.34) \quad \frac{\overline{q_1}}{q_2} \equiv -\frac{\overline{q_2}}{q_1} + \frac{1}{q_1 q_2} \pmod{1},$$

che fornisce

$$\mathcal{F} = \sum_{g \leq q_1 q_2} d_g e_{q_1 q_2}(gm_1 m_2 W) e_{q_1}(2g(m_2 - m_1)\overline{q_2}) e_{q_1 q_2}(2gm_1)$$

e, tornando a $j = m_1 m_2 g$ e per la 5.32

$$(5.35) \quad \mathcal{F} = \sum_{j \leq J} c_j e_{q_1 q_2}(jW) e_{q_1}(2j(\overline{m_1} - \overline{m_2})\overline{q_2}) e_{q_1 q_2}(2j\overline{m_2}).$$

In questo modo, sommando su q_2 abbiamo somme di Kloosterman con coefficienti arbitrari (qui ci saranno i $\overline{\gamma_{q_2}}$) e la loro stima si può fare solo in media sui moduli (qui q_1); essa é stata data recentemente da Duke-Friedlander-Iwaniec [D-F-I].

5.6. SOMME DI KLOOSTERMAN ED $N(N+2)$ IN INTERVALLI CORTI 115

Il Lemma seguente é il Teorema 2 in [D-F-I]:

Lemma 5.5. *Siano α e β due funzioni aritmetiche $\alpha, \beta : \mathbf{N} \rightarrow \mathbf{C}$, con norma l^2 $\|\alpha\|$, $\|\beta\|$, (rispettivam.); allora $\forall k \in \mathbf{Z}^*$ e $\forall \mu > 0$*

$$\sum_{m \sim M} \sum_{\substack{n \sim N \\ (n, m) = 1}} \alpha_m \beta_n e\left(k \frac{\overline{m}}{n}\right) \ll_{\mu} \|\alpha\| \|\beta\| (k + MN)^{\frac{3}{8}} (M + N)^{\frac{11}{48} + \mu}.$$

Per poter applicare il Lemma 5.5, dobbiamo innanzitutto eliminare le classi di resto reciproche $\overline{m_1}$ ed $\overline{m_2}$, dato che (anche se m_1 ed m_2 sono costanti rispetto a q_1 e q_2) dipendono dai moduli.

Per fare ciò li riguardiamo come residui reciproci modulo, diciamo,

$$B \stackrel{def}{=} \prod_{\substack{q \sim Q \\ q \text{ primo}}} q,$$

e ciò é possibile, dato che $(m_1 m_2, B) = 1$.

Poichè (per la 5.32 e l' ipotesi $Q < Rh^{-3\epsilon}$) possiamo scegliere $j < Q$, abbiamo (per definizione di B) $(j, B) = 1$ e possiamo scrivere, per la 5.35,

$$(5.36) \quad \mathcal{F} = \sum_{\substack{j \leq B \\ (j, B) = 1}} c_j e_{q_1 q_2}(j(W + 2\overline{m_2})) e_{q_1}(2j(\overline{m_1} - \overline{m_2})\overline{q_2});$$

ponendo $j = gm_1 m_2 \pmod{B}$ gli esponenziali diventano

$$e\left(\frac{gm_1(m_2 W + 2)}{q_1 q_2}\right) e\left(\frac{2g(m_2 - m_1)\overline{q_2}}{q_1}\right).$$

Per poter applicare due volte il Lemma 5.5, dobbiamo usare il Lemma 2.1 di sommazione parziale; ma prima cambiamo ancora variabile per eliminare i coefficienti $m_1(m_2 W + 2)$; quindi, poniamo $k = gm_1(m_2 W + 2) \pmod{B}$, per ottenere nella 5.36

$$\begin{aligned} & \sum_{\substack{q_1, q_2 \sim Q \\ (q_1, q_2) = 1}} \gamma_{q_1} \overline{\gamma_{q_2}} \mathcal{F} = \sum_{\substack{k \leq B \\ (k, B) = 1}} d_k \times \\ & \times \left(\sum_{\substack{q_1, q_2 \sim Q \\ (q_1, q_2) = 1}} \gamma_{q_1} \overline{\gamma_{q_2}} e_{q_1 q_2}(k) e_{q_1}\left(2k(m_2 - m_1)\overline{m_1(m_2 W + 2)q_2}\right) \right), \end{aligned}$$

dove adesso $d_k \stackrel{def}{=} c_l$, con $l \leq B$, $(l, B) = 1$, $l \equiv gm_1(m_2 W + 2) \pmod{B}$; quindi, per sommazione parziale, possiamo scrivere la stessa equazione con

coefficienti \widetilde{d}_k invece di d_k , dove $\widetilde{d}_k = d_k$ oppure $\widetilde{d}_k = 0$; tornando alla variabile j abbiamo (qui $\widetilde{c}_j = c_j$ oppure $\widetilde{c}_j = 0$)

$$\sum_{\substack{q_1, q_2 \sim Q \\ (q_1, q_2) = 1}} \gamma_{q_1} \overline{\gamma_{q_2}} \mathcal{F} \ll \sum_{\substack{j \leq B \\ (j, B) = 1}} |\widetilde{c}_j| \left| \sum_{\substack{q_1, q_2 \sim Q \\ (q_1, q_2) = 1}} \gamma_{q_1} \overline{\gamma_{q_2}} e_{q_1}(2j(m_2 - m_1)\overline{q_2}) \right|.$$

Scegliendo $\mu = \varepsilon/2$ nel Lemma 5.5 otteniamo, dalle stime dalla 5.28 in poi,

$$\begin{aligned} \Delta &\ll_{\varepsilon} \sum_{\substack{\frac{x}{2R} < m_1 < m_2 \leq \frac{x+h}{R}}} \left| \sum_{\substack{q_1, q_2 \sim Q \\ (q_1, q_2) = 1}} \gamma_{q_1} \overline{\gamma_{q_2}} \mathcal{F} \right| \ll_{\varepsilon} \\ &\ll_{\varepsilon} \sum_{\substack{\frac{x}{2R} < m_1, m_2 \leq \frac{x+h}{R}}} \sum_{j \leq B} |c_j| Q^{95/48} h^{\varepsilon/2} \ll_{\varepsilon} \frac{h^2}{R^2} Q^{\frac{95}{48}} h^{\varepsilon} \end{aligned}$$

e quest' ultimo é $\mathcal{O}_{\varepsilon}(h^{2-2\varepsilon}/R)$, poichè $Q \leq R^{\frac{48}{95}} h^{-2\varepsilon}$, come richiesto nelle ipotesi del Teorema 5.6.