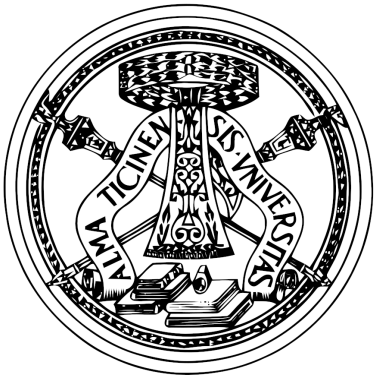
Università degli Studi di Pavia

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Matematica



Risultati asintotici sulla Congettura di Goldbach

Candidato:
Riccardo Invernizzi
Matricola 460156

Relatore:
Chiar.mo Prof. Alberto Canonaco

Anno Accademico 2019-2020

Indice

1 Funzioni Aritmetiche **4**
- 1.1 Somme e integrali . . . 4
- 1.2 Funzioni moltiplicative . . . 6
- 1.3 Somme di Ramanujan . . . 12
- 1.4 Prodotti infiniti . . . 13
- 1.5 Parte intera e parte frazionaria . . . 16

2 Distribuzione dei numeri primi **21**
- 2.1 Teorema di Chebychev . . . 22
- 2.2 Teoremi di Mertens . . . 26

3 I crivelli **31**
- 3.1 Metodo di Brun . . . 31
- 3.2 Metodo di Selberg . . . 34
- 3.3 Applicazioni . . . 39

4 Teorema di Goldbach-Shnirel'man **43**
- 4.1 Densità di Shnirel'man . . . 43
- 4.2 Teorema di Goldbach-Shnirel'man . . . 45

5 Teorema di Vinogradov **47**
- 5.1 Metodo del Cerchio . . . 47
- 5.2 Serie Singolare . . . 48
- 5.3 Arco Maggiore . . . 50
- 5.4 Arco Minore . . . 54
- 5.5 Teorema di Vinogradov . . . 60

Introduzione

La Congettura di Goldbach, talvolta indicata come Congettura forte di Goldbach, è una congettura formulata dal matematico prussiano Christian Goldbach nel 1742. In una lettera ad Eulero, Goldbach scrisse:

"Ogni numero intero maggiore di 5 può essere scritto come somma di tre numeri primi."

In seguito Eulero diede alla congettura una formulazione equivalente, quella più comunemente utilizzata:

"Ogni numero pari maggiore di due può essere scritto come somma di due numeri primi."

Infatti, se è vera la formulazione di Eulero, possiamo esprimere ogni numero dispari D maggiore di 5 come $D = n + 3$, dove n è pari e quindi somma di due primi, e 3 è primo. In questo modo D è somma di tre primi. Analogamente, ogni numero pari P è esprimibile come $P = n + 2$, con n pari e 2 primo. Se invece è vera la formulazione di Goldbach, abbiamo che ogni numero pari P è somma di tre primi. Ma dato che i primi diversi da 2 sono tutti dispari, per ottenere una somma pari devono sempre essere presenti in coppie. Abbiamo quindi solo due possibilità: $2 + 2 + 2$ oppure $d_1 + d_2 + 2$, dove d_1 e d_2 sono primi dispari. Allora, dato un qualsiasi numero pari P, sappiamo che $P + 2$ è somma di tre primi, di cui almeno uno è un 2. Sottraendo 2 abbiamo una rappresentazione di P come somma di due primi, e quindi la formulazione di Eulero. Esiste poi una terza versione, detta Congettura debole di Goldbach:

"Ogni numero dispari maggiore di 7 può essere scritto come somma di tre numeri primi."

L'aggettivo debole deriva dal fatto che, come osservato prima, questa versione è implicata dalle altre due; tuttavia non è vero il contrario. Questi e altri dettagli storici si possono trovare in [1].

Nel corso di questa tesi dimostreremo alcuni risultati asintotici, ovvero validi per numeri sufficientemente grandi, riguardanti la congettura di Goldbach. Il testo di riferimento è [7]. Il primo capitolo è dedicato alle funzioni aritmetiche. In esso verranno date definizioni e dimostrati risultati ampiamente utilizzati nelle sezioni successive. Il secondo capitolo, anch'esso di carattere generale, riguarda alcune stime sulla distribuzione dei numeri primi. Il risultato più importante è il Teorema di Chebyshev (2.12). Esso afferma che esistano due costanti positive c_1 e c_2 tali che

$$c_1 x \leq \pi(x) \log x \leq c_2 x$$

per ogni $x > 2$, ovvero che $\pi(x)$, il numero di primi non maggiori di x, cresce come $x/\log x$. Questo fatto avrà un ruolo importante nella dimostrazione della maggior parte dei teoremi successivi. Nello stesso capitolo dimostreremo anche la Formula di Mertens (Teorema 2.22).

Il terzo capitolo è dedicato alla teoria dei crivelli. I crivelli sono metodi per ottenere stime sulla cardinalità di insiemi di numeri con particolari proprietà. Si tratta generalmente di metodi elementari, ovvero che non fanno uso di tecniche avanzate, e questo li rende applicabili in diverse situazioni. L'idea alla base è quella di prendere un insieme di partenza, generalmente $\mathbb{N}$, ed eliminare da esso in passi successivi tutti i numeri che certamente non fanno parte dell'insieme di arrivo. L'esempio più famoso è il crivello di Eratostene, per la ricerca dei primi: presi i numeri da 2 a n, ad ogni passo si prende il più piccolo numero non eliminato (certamente primo) e si eliminano tutti i suoi multipli. In questo modo resteranno non eliminati solo i primi minori o uguali a n. Qui presenteremo il crivello di Brun (3.2) e quello di Selberg (3.10). Il crivello di Brun, un raffinamento del principio di inclusione-esclusione, ci permetterà di ottenere una stima su $\pi_2(x)$, il numero di primi p minori o uguali ad x tali che anche $p + 2$ è primo. Questi numeri sono detti primi gemelli. In questo modo dimostreremo che la somma sui reciproci dei primi gemelli converge (3.6). La congettura dei primi gemelli, che afferma la loro infinità, è un altro importante problema aperto in teoria dei numeri. Se la somma dei reciproci dei primi gemelli divergesse, ne esisterebbero certamente un numero infinito, dato che ogni somma finita converge. Il viceversa però non è vero: la convergenza di questa serie lascia aperto il problema. Il crivello di Selberg ci fornirà sia una stima migliore per $\pi_2(x)$, sia una stima su $r(N)$, il numero di rappresentazioni di N come somma di due primi, che ci servirà in seguito.

Il quarto capitolo è dedicato al primo dei due risultati sulla congettura di Goldbach che dimostreremo: il Teorema di Goldbach-Shnirel'man (4.14). Esso afferma che esiste una costante S, detta costante di Shnirel'man, tale che ogni numero è somma di al più S numeri primi. La congettura di Goldbach è quindi equivalente alla richiesta aggiuntiva $S = 3$. Per dimostrare questo teorema ci serviremo della densità di Shnirel'man (4.1), che valuta il rapporto tra i numeri minori di N contenuti in un insieme e N stesso. Dimostrare che tutti i naturali godono di una certa proprietà è equivalente a dimostrare che l'insieme dei naturali aventi quella proprietà ha densità 1. Grazie ad un teorema, dovuto sempre a Shnirel'man (4.10), se un insieme ha densità positiva allora considerando le somme di un numero finito di copie di quell'insieme otteniamo un insieme di densità 1, ovvero $\mathbb{N}$. È sufficiente allora, a meno di alcune questioni principalmente tecniche, dimostrare che l'insieme "somme di coppie di primi" ha densità positiva, e questo verrà fatto nel Teorema 4.13 grazie al Teorema di Chebyshev e alla stima di Selberg per $r(N)$.

Il quinto e ultimo capitolo è dedicato invece al Teorema di Vinogradov (5.18). Questo teorema dimostra che la congettura debole di Goldbach è valida per tutti gli interi sufficientemente grandi. Fornisce inoltre una formula asintotica per $r(N)$, usato qui, a differenza del teorema precedente, per indicare il numero di rappresentazioni di N intero dispari come somma di tre numeri primi. La tecnica utilizzata per arrivare a questo risultato è il metodo del cerchio, introdotto da Hardy, Littlewood e Ramanujan e poi perfezionato da Vinogradov. Il metodo del

cerchio, presentato nella Sezione 5.1, è un metodo molto generale per calcolare il numero di rappresentazioni di un intero come somma di elementi appartenenti ad un dato insieme. Hardy e Littlewood lo applicarono in origine al Problema di Waring, ovvero l'esprimibilità di ogni intero come somma finita di potenze n-esime, ottenendo anche in quel caso una formula asintotica per la soluzione. I dettagli di questo approccio si possono trovare in [7]. In questo caso l'insieme scelto è quello dei numeri primi. A partire da questo insieme si considera una funzione, detta anche funzione generatrice dell'insieme, dalla quale è possibile ottenere $r(N)$ tramite integrazione sul cerchio unitario. Il passaggio successivo consiste nel dividere il cerchio unitario, identificato con il segmento $[0, 1]$, in due parti, dette arco maggiore e arco minore. Fissato un intero Q, per tutti i $q \leq Q$ si prendono tutti i razionali esprimibili come frazioni con denominatore minore o uguale a q. L'arco maggiore consiste nell'insieme dei numeri sufficientemente vicini a queste frazioni, mentre l'arco minore è il suo complementare. Si stimano poi i contributi dell'integrale su questi due insiemi; l'arco maggiore fornisce la stima cercata, mentre il contributo di quello minore risulta trascurabile.
Il Teorema di Vinogradov non indica un limite inferiore per definire gli interi sufficientemente grandi. Nel corso degli anni sono state fatte diverse ricerche per abbassare questo limite. Nel 2013, il matematico peruviano Harald A. Helfgott è riuscito finalmente a dimostrare la congettura debole di Goldbach, ponendo quindi questo limite a 5 ([4], [5] e [6]). Questo risultato implica inoltre che ogni numero è somma di al più 4 numeri primi (è sufficiente aggiungere 3 a tutti i numeri dispari per ottenere tutti i numeri pari), abbassando la costante di Shnirel'man S definita prima al valore di 4.

1 Funzioni Aritmetiche

Definizione 1.1 *Una funzione aritmetica è una una funzione a valori complessi il cui dominio è l'insieme degli interi positivi* $\mathbb{N}$.

Definizione 1.2 *Definiamo la somma di due funzioni aritmetiche* f, g *come*

$$(f+g)(n) = f(n) + g(n)$$

Definizione 1.3 (Convoluzione di Dirichlet) *Date* f *e* g *funzioni aritmentiche definiamo la loro convoluzione come*

$$(f*g)(n) = \sum_{d|n} f(d)g(n/d).$$

Teorema 1.4 *L'insieme delle funzioni aritmetiche forma un anello commutativo con somma e convoluzione, di elementi neutri rispettivamente la funzione identicamente nulla* $0(n)$ *e la funzione*

$$\delta(n) = \begin{cases} 1 \ se \ n = 1 \\ 0 \ se \ n \geq 2. \end{cases}$$

Dimostrazione: Commutatività e associatività della somma seguono dalle proprietà della somma in $\mathbb{C}$. Inoltre la funzione nulla è chiaramente l'elemento neutro in quanto $f(n)+0 = f(n)$ per ogni f ed n. $f*g = g*f$, dato che sia d che n/d nella definizione scorrono su tutti i divisori di n. La convoluzione è quindi commutativa. Vale inoltre la distributività rispetto alla somma, infatti

$$(f*(g+h))(n) = \sum_{d|n} f(d)((g+h)(n/d)) = \sum_{d|n} f(d)g(n/d) + \sum_{d|n} f(d)h(n/d) = (f*g)(n) + (f*h)(n).$$

Per quanto riguarda l'elemento neutro abbiamo

$$(f*\delta)(n) = \sum_{d|n} f(d)\delta(n/d) = f(n).$$

Resta quindi da verificare solo l'associatività di $(*)$. Abbiamo

$$((f*g)*h) = \sum_{d|n} (f*g)(d)h\left(\frac{n}{d}\right) = \sum_{dm=n} (f*g)(d)h(m) =$$

$$= \sum_{dm=n} \sum_{kl=d} f(k)g(l)h(m) = \sum_{klm=n} f(k)g(l)h(m) = \sum_{k|n} f(k) \sum_{lm=n/k} g(l)h(m) =$$

$$= \sum_{k|n} f(k) \sum_{l|(n/k)} g(l)h\left(\frac{n}{kl}\right) = (f*(g*h))(n).$$

□

1.1 Somme e integrali

Teorema 1.5 *Siano* $a < b$ *interi e* $f(t)$ *una funzione monotona sull'intervallo* $[a, b]$. *Allora*

$$\min(f(a), f((b)) \leq \sum_{k=a}^{b} f(k) - \int_a^b f(t)dt \leq \max(f(a), f(b)).$$

Dimostrazione: Se f è crescente su $[a, b]$ $\min f = f(a)$ e $\max f = f(b)$. Abbiamo poi

$$\int_k^{k+1} f(t)dt \geq f(k)$$

per $k = a, a+1, ..., b-1$ e analogamente

$$\int_{k-1}^{k} f(t)dt \leq f(k)$$

per $k = a+1, ..., b$. Otteniamo quindi

$$\sum_{k=a}^{b} f(k) = \sum_{k=a}^{b-1} f(k) + f(b) \leq \int_a^b f(t)dt + f(b)$$

e analogamente

$$\sum_{k=a}^{b} f(k) = \sum_{k=a+1}^{b} f(k) + f(a) \geq \int_a^b f(t)dt + f(a).$$

Mettendo insieme le due disuguaglianze otteniamo la tesi. Per f decrescente le stime sono le stesse con verso cambiato. □

Teorema 1.6 *Per ogni intero positivo n vale*

$$e\left(\frac{n}{e}\right)^n \leq n! \leq en\left(\frac{n}{e}\right)^n.$$

Dimostrazione: La funzione $f(t) = \log t$ è monotona sull'intervallo $[1, n]$. Applicando il Teorema 1.5 otteniamo

$$\log n! = \sum_{k=1}^{n} \log n \leq \int_1^n \log t dt + \log n = (n \log n - n + 1) + \log n$$

e

$$\log n! \geq \int_1^n \log t dt = n \log n - n + 1.$$

Passando all'esponenziale delle due disuguaglianze, e sfruttando $e^{x \log y} = y^x$, otteniamo la tesi. □

Teorema 1.7 *Siano $u(n)$ e $f(n)$ funzioni aritmetiche. Definiamo*

$$U(t) = \sum_{n \leq t} u(n).$$

Allora presi a, b interi con $0 \leq a < b$ abbiamo

$$\sum_{n=a+1}^{b} u(n)f(n) = U(b)f(b) - U(a)f(a+1) - \sum_{n=a+1}^{b-1} U(n)(f(n+1) - f(n)).$$

Siano invece x, y reali tali che $0 \leq y < x$. Se $f(t)$ ha derivata continua in $[y, x]$, vale

$$\sum_{y < n \leq x} u(n)f(n) = U(x)f(x) - U(y)f(y) - \int_y^x U(t)f'(t)dt.$$

In particolare, se $f(t)$ ha derivata continua in $[1, x]$, allora

$$\sum_{n \leq x} u(n)f(n) = U(x)f(x) - \int_1^x U(t)f'(t)dt.$$

Dimostrazione:

$$\sum_{n=a+1}^{b} u(n)f(n) = \sum_{n=a+1}^{b} (U(n) - U(n-1))f(n) = \sum_{n=a+1}^{b} U(n)f(n) - \sum_{n=a}^{b-1} U(n)f(n+1) =$$

$$= U(b)f(b) - U(a)f(a+1) - \sum_{n=a+1}^{b-1} U(n)(f(n+1) - f(n)).$$

Se $f \in C^1([y, x])$

$$f(n+1) - f(n) = \int_n^{n+1} f'(t)dt$$

e quindi

$$U(n)(f(n+1) - f(n)) = \int_n^{n+1} U(t)f'(t)dt,$$

dato che $U(t)$ è costante su $(n, n+1)$. Poniamo $a = [y]$ e $b = [x]$. Ora, se $a = b$ la somma a sinistra dell'uguaglianza che vogliamo dimostrare è vuota, e la tesi vale applicando a destra il teorema fondamentale del

calcolo. Se invece $a < b$ sfruttando la prima parte di dimostrazione abbiamo

$$\sum_{y<n\leq x} u(n)f(n) = \sum_{n=a+1}^{b} u(n)f(n) =$$

$$U(b)f(b) - U(a)f(a+1) - \sum_{n=a+1}^{b-1} U(n)(f(n+1) - f(n)) =$$

$$= U(x)f(b) - U(y)f(a+1) - \sum_{n=a+1}^{b-1} \int_n^{n+1} U(t)f'(t)dt =$$

$$U(x)f(x) - U(x)(f(x) - f(b)) - U(y)f(y) - U(y)(f(a+1) - f(y)) - \int_{a+1}^{b} U(t)f'(t)dt =$$

$$= U(x)f(x) - U(y)f(y) - \int_y^x U(t)f'(t)dt.$$

Se $f \in C^1([1,x])$, sfruttando il punto precedente e il fatto che per definizione $U(1) = u(1)$ abbiamo

$$\sum_{n\leq x} u(n)f(n) = u(1)f(1) + \sum_{1<n\leq x} u(n)f(n) =$$

$$= u(1)f(1) - U(1)f(1) + U(x)f(x) - \int_1^x U(t)f'(t)dt = U(x)f(x) - \int_1^x U(t)f'(t)dt.$$

□

Teorema 1.8 (Costante di Eulero) *Definiamo la costante di Eulero come*

$$\gamma = 1 - \int_1^{\infty} \frac{\{t\}}{t^2} dt$$

dove $\{t\}$ *indica la parte frazionaria di* t*. Allora* $0 < \gamma < 1$ *e inoltre*

$$\sum_{n\leq x} \frac{1}{n} = \log x + \gamma + \mathcal{O}\left(\frac{1}{x}\right)$$

Dimostrazione: Dato che per ogni t $0 \leq \{t\} < 1$, abbiamo

$$0 < \int_1^{\infty} \frac{\{t\}}{t^2} dt < \int_1^{\infty} \frac{1}{t^2} dt = 1$$

e quindi $0 < \gamma < 1$. Ponendo $u(n) = 1$ e $f(t) = 1/t$ abbiamo $U(t) = [t] = t - \{t\}$. Applicando il Teorema 1.7 (terza parte, grazie alla regolarità di $1/t$ su $[1,x]$) otteniamo allora

$$\sum_{n\leq x} \frac{1}{n} = \sum_{n\leq x} u(n)f(n) = \frac{[x]}{x} + \int_1^x \frac{[t]}{t^2} dt =$$

$$= 1 - \frac{\{x\}}{x} + \int_1^x \frac{1}{t} dt - \int_1^x \frac{\{t\}}{t^2} dt =$$

$$\log x + 1 - \int_1^{\infty} \frac{\{t\}}{t^2} dt + \int_x^{\infty} \{t\} t^{-2} dt - \frac{\{x\}}{x} = \log x + \gamma + \mathcal{O}\left(\frac{1}{x}\right).$$

□

1.2 Funzioni moltiplicative

Definizione 1.9 *Una funzione aritmetica* $f(n)$ *si dice moltiplicativa se*

$$f(mn) = f(m)f(n)$$

per m, n *coprimi e totalmente (completamente) moltiplicativa se l'uguaglianza vale per ogni coppia di* m, n*.*

Osservazione 1.10 *Sia* f *moltiplicativa. Se* $f(1) = 0$ *allora* $f(n) = f(n \cdot 1) = f(n)f(1) = 0$ *e* f *è identicamente nulla. Altrimenti* $f(1) = f(1)^2$ *e quindi* $f(1) = 1$*.*

Teorema 1.11 *Sia f moltiplicativa. Allora*

$$f([m,n])f((m,n)) = f(m)f(n).$$

Dimostrazione: Posto $m = \prod_{i=1}^{r} p_i^{r_i}$ e $n = \prod_{i=1}^{r} p_i^{s_i}$ abbiamo, operando sui singoli fattori primi,

$$f([m,n])f((m,n)) = \prod_{i=1}^{r} f(p_i^{max(r_i,s_i)}) \prod_{i=1}^{r} f(p_i^{min(r_i,s_i)}) = \prod_{i=1}^{r} f(p_i^{r_i}) \prod_{i=1}^{r} f(p_i^{s_i}) = f(m)f(n)$$

per moltiplicatività di f. □

Teorema 1.12 *Sia f moltiplicativa. Se*

$$\lim_{p^k \to \infty} f(p^k) = 0,$$

dove p^k assume come valori tutte le potenze esatte dei primi, allora

$$\lim_{n \to \infty} f(n) = 0.$$

Dimostrazione: Per ipotesi esiste soltanto un numero finito di potenze di primi p^k tali che $|f(p^k)| \geq 1$. Allora

$$A = \prod_{|f(p^k)| \geq 1} |f(p^k)|$$

è una quantità finita e certamente ≥ 1. Prendiamo $0 < \epsilon < A$. Di nuovo, esistono un numero finito di potenze di primi p^k tali che $|f(p^k)| \geq \epsilon/A$. Quindi anche le combinazioni di queste potenze saranno in numero finito, e pertanto solo un numero finito di interi n godrà della proprietà che

$$|f(p^k)| \geq \epsilon/A$$

per ogni potenza di primo p^k che divide esattamente n (ovvero tale che p^{k+1} non divide n). Quindi, per n sufficientemente grande, ogni n sarà divisibile per almeno una potenza di un primo p^k tale che $|f(p^k)| < \epsilon/A$. Possiamo quindi scrivere n come

$$n = \prod_{i=1}^{r} p_i^{k_i} \prod_{i=r+1}^{r+s} p_i^{k_i} \prod_{i=r+s+1}^{r+s+t} p_i^{k_i}$$

dove i p_i sono primi distinti e vale

$$1 \leq |f(p_i^{k_i})| \text{ per } i = 1, ..., r$$
$$\epsilon/A \leq |f(p_i^{k_i})| < 1 \text{ per } i = r+1, ..., r+s$$
$$|f(p_i^{k_i})| < \epsilon/A \text{ per } i = r+s+1, ..., r+s+t$$

con $t \geq 1$. Allora, ricordando la definizione di A,

$$|f(n)| = \prod_{i=1}^{r} |f(p_i^{k_i})| \prod_{i=r+1}^{r+s} |f(p_i^{k_i})| \prod_{i=r+s+1}^{r+s+t} |f(p_i^{k_i})| < A(\epsilon/A)^t \leq \epsilon$$

per ogni ϵ e n sufficientemente grande. □

Definizione 1.13 (Funzione divisore) *Indichiamo con $d(n)$ il numero dei divisori di n.*

Teorema 1.14 *Sia $m = p_1^{k_1} \cdots p_r^{k_r}$, dove $p_1, ..., p_r$ sono primi distinti e $k_1, ..., k_r$ sono interi positivi. Allora*

$$d(m) = \prod_{i=1}^{r} (k_i + 1).$$

Inoltre $d(mn) \leq d(m)d(n)$ e $d(mn) = d(m)d(n)$ se $(m,n) = 1$, ovvero d è moltiplicativa.

Dimostrazione: Ogni divisore può essere scritto nella forma $d = p_1^{j_1} \cdots p_r^{j_r}$ con $0 \leq j_i \leq k_i$ per ogni i. Ci sono quindi $k_i + 1$ scelte per ogni j_i, da cui

$$d(m) = \prod_{i=1}^{r} (k_i + 1).$$

Prendiamo $n = p_1^{l_1} \cdots p_r^{l_r}$. Allora

$$d(n) = \prod_{i=1}^{r} (l_i + 1).$$

Inoltre $nm = p_1^{k_1+l_1} \cdots p_r^{k_r+l_r}$ e dato che $k_i + l_i + 1 \leq (k_i + 1)(l_i + 1)$ per ogni i, segue

$$d(mn) = \prod_{i=1}^{r} (k_i + l_i + 1) \leq \prod_{i=1}^{r} (k_i + 1)(l_i + 1) = d(m)d(n).$$

Se $(m, n) = 1$ si ha l'uguaglianza in quanto per ogni i uno tra k_i e l_i è zero. □

Teorema 1.15

$$D(x) = \sum_{n \leq x} d(n) = x \log x + (2\gamma - 1)x + \mathcal{O}(\sqrt{x})$$

Dimostrazione: Possiamo interpretare la funzione $d(n)$ come il numero di modi di scrivere $n = uv$, o equivalentemente come il numero di punti interi toccati dall'iperbole $uv = n$ nel quadrante $u > 0, v > 0$ del piano (u, v). Geometricamente la funzione $D(x)$ conterà allora i punti interi giacenti sull'iperbole $uv = x$ oppure al di sotto di essa. A partire da u possiamo considerare questi punti come i punti interi (u, v) tali che $1 \leq u \leq x$ e $1 \leq v \leq x/u$. Possiamo dividere questi punti in tre gruppi disgiunti:

1. $1 \leq u \leq \sqrt{x}$ e $1 \leq v \leq \sqrt{x}$. Questi punti corrispondono al quadrato con vertici l'origine e il fuoco dell'iperbole. Sono in totale $[\sqrt{x}]^2$.

2. $1 \leq u \leq \sqrt{x}$ e $\sqrt{x} < v \leq x/u$. Richiediamo in particolare $\sqrt{x} < v$ perchè questo insieme di punti sia disgiunto dal precedente. Considerando l'asse u come asse orizzontale, stiamo prendendo i punti che si trovano sopra il quadrato trovato prima e sotto l'iperbole. Il totale di questi punti sarà

   $$\sum_{1 \leq u \leq \sqrt{x}} \left(\left[\frac{x}{u} \right] - [\sqrt{x}] \right),$$

   ottenuto contando per ogni $u \geq \sqrt{x}$ i punti nella sua 'colonna', che sono i punti interi da 1 a $v = [x/u]$, e sottraendo i $[\sqrt{x}]$ punti già contati in (1).

3. $\sqrt{x} < u \leq x$ e $1 \leq v \leq x/u$. Questi punti sono i simmetrici ai precedenti. Possiamo infatti identificarli con i punti tali che $1 \leq v \leq \sqrt{x}$ e $\sqrt{x} < u \leq x/v$. Per quanto visto prima, il totale di questi punti sarà

   $$\sum_{1 \leq v \leq \sqrt{x}} \left(\left[\frac{x}{v} \right] - [\sqrt{x}] \right) = \sum_{1 \leq u \leq \sqrt{x}} \left(\left[\frac{x}{u} \right] - [\sqrt{x}] \right)$$

   per simmetria.

Sommando i tre contributi otteniamo

$$\begin{aligned}
D(x) &= [\sqrt{x}]^2 + \sum_{1 \leq u \leq \sqrt{x}} \left(\left[\frac{x}{u} \right] - [\sqrt{x}] \right) + \sum_{1 \leq v \leq \sqrt{x}} \left(\left[\frac{x}{v} \right] - [\sqrt{x}] \right) = \\
&= [\sqrt{x}]^2 + 2 \sum_{1 \leq u \leq \sqrt{x}} \left(\left[\frac{x}{u} \right] - [\sqrt{x}] \right) = -[\sqrt{x}]^2 + 2 \sum_{1 \leq u \leq \sqrt{x}} \left[\frac{x}{u} \right] = \\
&= -(\sqrt{x} - \{\sqrt{x}\})^2 + 2 \sum_{1 \leq u \leq \sqrt{x}} \left(\frac{x}{u} - \left\{ \frac{x}{u} \right\} \right) = \\
&= 2x \sum_{1 \leq u \leq \sqrt{x}} \frac{1}{u} - 2 \sum_{1 \leq u \leq \sqrt{x}} \left\{ \frac{x}{u} \right\} - x + \mathcal{O}(\sqrt{x}) = \\
&2x \left(\log \sqrt{x} + \gamma + \mathcal{O}\left(\frac{1}{\sqrt{x}} \right) \right) - x + \mathcal{O}(\sqrt{x}) = \\
&= x \log x + (2\gamma - 1)x + \mathcal{O}(\sqrt{x}),
\end{aligned}$$

dove abbiamo usato nel penultimo passaggio il Teorema 1.8 □

Teorema 1.16

$$\sum_{n \leq x} \frac{d(n)}{n} = \frac{1}{2} (\log x)^2 + \mathcal{O}(\log x).$$

Dimostrazione: Grazie al Teorema 1.15 abbiamo

$$D(x) = \sum_{n \le x} d(n) = x \log x + (2\gamma - 1)x + \mathcal{O}(\sqrt{x}).$$

Applicando il Teorema 1.7 con $u(n) = d(n)$ e $f(t) = 1/t$ abbiamo

$$\sum_{n \le x} \frac{d(n)}{n} = \frac{D(x)}{x} + \int_1^x \frac{D(t)}{t^2} dt = \frac{x \log x + \mathcal{O}(x)}{x} + \int_1^x \frac{t \log t + \mathcal{O}(t)}{t^2} dt =$$
$$= \log x + \mathcal{O}(1) + \int_1^x \frac{\log t}{t} dt + \mathcal{O}\left(\int_1^x \frac{1}{t} dt \right) = \frac{1}{2} (\log x)^2 + \mathcal{O}(\log x).$$

□

Teorema 1.17

$$\sum_{n \le x} d(n)^2 \ll x (\log x)^3.$$

Dimostrazione: Per il Teorema 1.14, $d(ab) \le d(a)d(b)$ per ogni a, b. Abbiamo quindi

$$\sum_{n \le x} d(n)^2 = \sum_{n \le x} d(n) \sum_{n = ab} 1 = \sum_{ab \le x} d(ab) \le \sum_{ab \le x} d(a)d(b) = \sum_{a \le x} d(a) \sum_{b \le x/a} d(b).$$

Ora applicando il Teorema 1.15 otteniamo

$$\sum_{a \le x} d(a) \sum_{b \le x/a} d(b) = \sum_{a \le x} d(a) \left(\left(\frac{x}{a} \right) \log \frac{x}{a} + \mathcal{O}\left(\frac{x}{a} \right) \right) \le$$
$$\le x \log x \sum_{a \le x} \frac{d(a)}{a} + \mathcal{O}\left(x \sum_{a \le x} \frac{d(a)}{a} \right) \ll x (\log x)^3$$

utilizzando il Teorema 1.16 nell'ultima stima. □

Definizione 1.18 (Square-free) *Diciamo che un numero intero n è square-free se vale*

$$n = \prod_{p \mid n} p,$$

ovvero se non compaiono potenze di primi nella decomposizione di n.

Definizione 1.19 (Funzione di Möbius) *La funzione di Möbius $\mu(n)$ è definita come*

$$\mu(n) = \begin{cases} 1 \text{ se } n = 1, \\ 0 \text{ se } n \text{ è divisibile per il quadrato di un primo}, \\ (-1)^r \text{ se } n \text{ è il prodotto di } r \text{ primi distinti}. \end{cases}$$

Osservazione 1.20 *$\mu(n) \neq 0$ se e solo se n è square-free. Inoltre μ è moltiplicativa ma non totalmente, perchè si annulla sul prodotto di numeri non coprimi tra loro.*

Teorema 1.21 *Sia f una funzione moltiplicativa con $f(1) = 1$. Allora*

$$\sum_{d \mid n} \mu(d) f(d) = \prod_{p \mid n} (1 - f(p)).$$

Dimostrazione: L'uguaglianza è vera per $n = 1$, dato che per convenzione il prodotto vuoto vale 1. Per $n > 1$, indichiamo con n^* il prodotto dei divisori primi distinti di n. Dato che $\mu(d) = 0$ se d non è square-free, possiamo limitarci a considerare i divisori square-free di n. Ma questi saranno tutti e soli i divisori di n^*. Abbiamo quindi

$$\sum_{d \mid n} \mu(d) f(d) = \sum_{d \mid n^*} \mu(d) f(d) = \prod_{p \mid n} (1 - f(p)),$$

infatti espandendo il prodotto a destra troviamo f applicato a tutti i divisori di n^* espressi come combinazione di primi (per moltiplicatività di f), con segno determinato dalla parità del numero di primi coinvolti. □

Teorema 1.22

$$\sum_{d|n} \mu(d) = \delta(n)$$

dove $\delta(n)$ è la funzione definita nel Teorema 1.4. Indicando con $1(n) = 1$ la funzione identicamente 1, possiamo formulare equivalentemente la tesi come

$$\mu * 1 = \delta.$$

Dimostrazione: Per $n = 1$ il Teorema è chiaramente vero. Se $n \geq 2$ scriviamo $n = \prod_{i=1}^{k} p_i^{r_i}$. Indicando con $\sum^*$ la somma ristretta agli elementi square-free, e ricordando che per tutti gli altri interi n vale $\mu(n) = 0$, abbiamo

$$\sum_{d|n} \mu(d) = \sum_{d|n}^{*} \mu(d) = \sum_{d|p_1 \cdots p_k} \mu(d) = \sum_{d|p_1 \cdots p_k} (-1)^{\omega(d)} = \sum_{l=0}^{k} \binom{k}{l} (-1)^l = (1-1)^k = 0,$$

dove $\omega(d)$ è il numero di divisori primi distinti di d. Il terzultimo passaggio segue dal fatto che su k primi i sottoinsiemi formati da l di essi sono $\binom{k}{l}$. □

Definizione 1.23 *Un insieme non vuoto $\mathcal{D}$ è detto chiuso per divisori se, per ogni $n \in \mathcal{D}$ e ogni $d|n$, allora $d \in \mathcal{D}$.*

Osservazione 1.24 *Se f, g sono funzioni aritmetiche definite su un insieme $\mathcal{D}$ chiuso per divisori anche la loro convoluzione $f * g$ sarà definita su $\mathcal{D}$*

Teorema 1.25 (Inversione di Möbius) *Sia $\mathcal{D}$ un insieme chiuso per divisori, e $f(n)$ una funzione definita su $\mathcal{D}$. Allora se g è definita su $\mathcal{D}$ come*

$$g(n) = \sum_{d|n} f(d)$$

vale

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

per ogni $n \in \mathcal{D}$. Viceversa sia g definita su $\mathcal{D}$. Se

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

su $\mathcal{D}$ allora

$$g(n) = \sum_{d|n} f(d).$$

Dimostrazione: Osserviamo intanto che se $n \in \mathcal{D}$ allora $d \in \mathcal{D}$. Se

$$g(n) = \sum_{d|n} f(d) = (f * 1)(n)$$

abbiamo

$$\sum_{d|n} \mu\left(\frac{d}{n}\right) g(d) = (g * \mu)(n) = ((f * 1) * \mu)(n) = (f * (1 * \mu))(n) =$$

$$(f * \delta)(n) = f(n)$$

Analogamente se

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = (g * \mu)(n)$$

otteniamo

$$\sum_{d|n} f(d) = (f * 1)(n) = ((g * \mu) * 1)(n) = (g * (\mu * 1))(n) =$$

$$(g * \delta)(n) = g(n).$$

□

Teorema 1.26 *Sia $\mathcal{D}$ un insieme finito chiuso per divisori, e f, g funzioni definite su $\mathcal{D}$. Allora*

$$g(n) = \sum_{\substack{d\in\mathcal{D}\\ n|d}} f(d)$$

se e solo se

$$f(n) = \sum_{\substack{d\in\mathcal{D}\\ n|d}} \mu\left(\frac{d}{n}\right) g(d).$$

Dimostrazione: Supponiamo

$$g(n) = \sum_{\substack{d\in\mathcal{D}\\ n|d}} f(d).$$

Procedendo per calcolo diretto abbiamo

$$\sum_{\substack{d\in\mathcal{D}\\ n|d}} \mu\left(\frac{d}{n}\right) g(d) = \sum_{\substack{d\in\mathcal{D}\\ n|d}} \mu\left(\frac{d}{n}\right) \sum_{\substack{k\in\mathcal{D}\\ d|k}} f(k) = \sum_{nh\in\mathcal{D}} \mu(h) \sum_{\substack{k\in\mathcal{D}\\ nh|k}} f(k) = \sum_{nh\in\mathcal{D}} \mu(h) \sum_{nhl\in\mathcal{D}} f(nhl) =$$
$$\sum_{nr\in\mathcal{D}} f(nr) \sum_{\substack{h\in\mathcal{D}\\ h|r}} \mu(h) = \sum_{nr\in\mathcal{D}} f(nr) \sum_{h|r} \mu(h) = f(n)$$

grazie al Teorema 1.22. Seguendo i passaggi in direzione opposta (e assumendo l'altra uguaglianza) si ottiene il viceversa. □

Definizione 1.27 (φ di Eulero) *Indichiamo con $\varphi(n)$ il numero di interi positivi $a \leq n$ tali che $(a, n) = 1$, o equivalentemente il numero di classi di congruenza modulo n coprime ad n.*

Teorema 1.28 *$\varphi(n)$ è moltiplicativa, e vale*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = \prod_{p^k||n} p^{k-1}(p-1).$$

Dimostrazione: Prendiamo una coppia di interi m, n tali che $(m, n) = 1$, e poniamo $\varphi(m) = r$ e $\varphi(n) = s$. Siano allora $a_1, ..., a_r$ rappresentanti delle r classi di congruenza modulo m coprime ad m, e $b_1, ..., b_s$ la stessa cosa con n. Vogliamo ora dimostrare che gli rs numeri $a_i n + b_j m$, con $i = 1, ..., r$ e $j = 1, ..., s$ formano un insieme contenente i rappresentanti di tutte le classi di congruenza coprime con mn.
Iniziamo col mostrare che le classi sono disgiunte. Se vale

$$a_i n + b_j m \equiv a_k n + b_l m \pmod{mn},$$

allora

$$a_i n + b_j m \equiv a_k n + b_l m \pmod{n}$$

ovvero

$$b_j m \equiv b_l m \pmod{n}.$$

Ma dato che $(m, n) = 1$ posso dividere per m ottenendo $b_j \equiv b_l (\text{mod n})$, che per definizione dei b_i implica $j = l$. Con un ragionamento analogo abbiamo anche $i = k$.
Mostriamo ora che tutte le classi nella forma $a_i n + b_j m$ sono coprime ad mn. Se valesse $(a_i n + b_j m, mn) > 1$ per qualche i, j, ci sarebbe un primo p che divide sia mn che $a_i n + b_j m$. Dato che $(m, n) = 1$, p divide esattamente uno tra m ed n. Ma allora, se $p|m$, deve valere $p|a_i n$, e quindi non dividendo n $p|a_i$. Ma questo implica $(m, a_i) \geq p$ contraddicendo la definizione di a_i. Lo stesso risultato si ottiene se $p|n$. Quindi, $(a_i n + b_j m, mn) = 1$ per ogni i, j.
Mostriamo ora che ogni classe di congruenza coprima a mn è esprimibile in questa forma. Sia $(c, mn) = 1$. Allora $(c, m) = 1$ e quindi $c \equiv a_i n \pmod{m}$ per qualche i. Inoltre $(c, n) = (c - a_i n, n) = 1$ e quindi $c - a_i n \equiv b_j m \pmod{n}$ per qualche j. Abbiamo quindi

$$\begin{cases} c \equiv a_i n + b_j m \pmod{n} \\ c \equiv a_i n + b_j m \pmod{m} \end{cases}$$

da cui segue

$$c \equiv a_i n + b_j m \pmod{mn}$$

e in conclusione

$$\varphi(mn) = rs = \varphi(m)\varphi(n),$$

ovvero φ è moltiplicativa. Per p primo e $k \geq 1$, gli unici interi non coprimi con p^k sono i multipli di p, e quindi vale

$$\varphi(p^k) = p^k - p^{k-1} = (p^k - 1)(p-1) = p^k\left(1 - \frac{1}{p}\right).$$

Scomponendo n in fattori primi otteniamo quindi

$$\varphi(n) = \prod_{\substack{p^k||n \\ k\geq 1}} \varphi(p^k) = \prod_{\substack{p^k||n \\ k\geq 1}} p^k\left(1 - \frac{1}{p}\right) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$$

dato che $n = \prod_{p^k||n} p^k$. □

Teorema 1.29 *Fissato $\epsilon > 0$ vale*

$$n^{1-\epsilon} < \varphi(n) < n$$

per ogni n sufficientemente grande.

Dimostrazione: La seconda disuguaglianza, $\varphi(n) < n$, vale per ogni $n > 1$. Per quanto riguarda la prima vogliamo dimostrare che

$$\lim_{n\to\infty} \frac{n^{1-\epsilon}}{\varphi(n)} = 0.$$

Sfruttando il fatto che $p/(p-1) \leq 2$ per ogni $p \geq 2$ e quindi per ogni primo p, abbiamo

$$\frac{p^{m(1-\epsilon)}}{\varphi(p^m)} = \frac{p^{m(1-\epsilon)}}{p^m - p^{m-1}} = \frac{p}{p-1}\frac{p^{m(1-\epsilon)}}{p^m} \leq \frac{2}{p^{m\epsilon}},$$

da cui

$$\lim_{p^m\to\infty} \frac{p^{m(1-\epsilon)}}{\varphi(p^m)} = 0.$$

Dal momento che $\varphi(n)$ è moltiplicativa, lo è anche $n^{1-\epsilon}/\varphi(n)$ e quindi la tesi segue dal Teorema 1.12. □

1.3 Somme di Ramanujan

In questa sezione e in seguito indichiamo con

$$e(x) = e^{2\pi i x}.$$

Definizione 1.30 *La somma*

$$c_q(n) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e\left(\frac{an}{q}\right)$$

è detta somma di Ramanujan.

Teorema 1.31 *La somma di Ramanujan $c_q(n)$ è una funzione moltiplicativa in q, ovvero dati q e q' tali che $(q,q') = 1$ abbiamo*

$$c_{qq'}(n) = c_q(n)c_{q'}(n).$$

Dimostrazione: Seguendo la dimostrazione del Teorema 1.28, possiamo scrivere i rappresentanti di ogni classe di congruenza modulo qq' coprima a qq' in modo unico come $x = aq' + a'q$ con $1 \leq a \leq q$ e $1 \leq a' \leq q'$. Inoltre notiamo che se fosse $(a,q) \neq 1$ allora $(aq' + a'q, qq') \geq (a,q) > 1$, e lo stesso discorso vale per (a',q'). Per le classi di resto coprime a qq' avremo quindi $(a,q) = (a',q') = 1$. Abbiamo allora

$$c_q(n)c_{q'}(n) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e\left(\frac{an}{q}\right) \sum_{\substack{a'=1 \\ (a',q')=1}}^{q'} e\left(\frac{a'n}{q'}\right) =$$

$$= \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{a'=1 \\ (a',q')=1}}^{q'} e\left(\frac{(aq'+a'q)n}{qq'}\right) = \sum_{\substack{a''=1 \\ (a'',qq')=1}}^{qq'} e\left(\frac{a''n}{qq'}\right) = c_{qq'}(n).$$

□

Teorema 1.32 *Vale*

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

In particolare se $(q,n) = 1$ *abbiamo*

$$c_q(n) = \mu(q).$$

Dimostrazione: Definiamo

$$f_d(n) = \sum_{l=1}^{d} e\left(\frac{ln}{d}\right).$$

Ora se $d|n$ abbiamo, ricordando che $e(x) = \exp(2\pi i x) = \cos 2\pi x + i \sin 2\pi x$,

$$e\left(\frac{ln}{d}\right) = e(lk) = 1$$

e quindi $f_d(n) = d$. Se invece $d \nmid n$ la somma si annulla sempre grazie all'identità $x^d - 1 = (x-1)(x^{d-1} + x^{d-2} + \cdots + x + 1)$ con $x = e(n/d)$. Riassumendo

$$f_d(n) = \begin{cases} d \text{ se } d|n \\ 0 \text{ se } d \nmid n. \end{cases}$$

Abbiamo quindi

$$c_q(n) = \sum_{\substack{k=1 \\ (k,q)=1}}^{q} e\left(\frac{kn}{q}\right) = \sum_{k=1}^{q} e\left(\frac{kn}{q}\right) \sum_{d|(k,q)} \mu(d)$$

dato che $\sum_{d|(k,q)} \mu(d) = \delta((k,q))$ grazie al Teorema 1.22. Allora riordinando le somme

$$\sum_{k=1}^{q} e\left(\frac{kn}{q}\right) \sum_{d|(k,q)} \mu(d) = \sum_{d|q} \mu(d) \sum_{\substack{k=1 \\ d|k}}^{q} e\left(\frac{kn}{q}\right)$$

e ponendo $k = ld$ otteniamo infine

$$\sum_{d|q} \mu(d) \sum_{\substack{k=1 \\ d|k}}^{q} e\left(\frac{kn}{q}\right) = \sum_{d|q} \mu(d) \sum_{l=1}^{q/d} e\left(\frac{ln}{q/d}\right) = \sum_{d|q} \mu(d) f_{q/d}(n) \overset{(A)}{=}$$

$$\sum_{d|q} \mu(q/d) f_d(n) = \sum_{\substack{d|q \\ d|n}} \mu(q/d) d = \sum_{d|(n,q)} \mu(q/d) d,$$

dove in (A) sfruttiamo la commutatività della convoluzione. □

1.4 Prodotti infiniti

Sia $\alpha_1, \alpha_2, \ldots$ una successione di numeri complessi. Indichiamo con p_n l'n-esimo prodotto parziale, ovvero

$$p_n = \prod_{k=1}^{n} \alpha_i = \alpha_1 \cdots \alpha_n$$

Definizione 1.33 *Se, facendo tendere n ad infinito,* p_n *converge ad un limite* $\alpha \neq 0$*, diciamo che il prodotto infinito degli* α_n *converge, e vale*

$$\prod_{i=k}^{\infty} \alpha_i = \lim_{n\to\infty} p_n = \lim_{n\to\infty} \prod_{i=k}^{n} \alpha_k = \alpha$$

Se il limite non esiste diciamo che il prodotto infinito diverge, mentre se il limite esiste e vale zero diciamo che la serie diverge a zero.

Osservazione 1.34 *Se, data una successione $\{a_k\}$, prendiamo $\alpha_k = 1+a_k$ e il prodotto infinito $\prod \alpha_k$ converge secondo la nostra definizione, possiamo affermare che $a_k \neq -1$ per ogni k. Inoltre possiamo scrivere $a_k + 1 = p_{k+1}/p_k$, e di nuovo grazie alla convergenza dei p_n abbiamo*

$$\lim_{k\to\infty}(a_k+1) = \lim_{k\to\infty}\frac{p_{k+1}}{p_k} = 1$$

da cui si vede che $a_k \to 0$. Possiamo però ottenere un risultato ancora più preciso.

Teorema 1.35 *Sia $a_k \geq 0$ per ogni $k \geq 1$. Allora il prodotto infinito $\prod_{k=1}^{\infty}(1+a_k)$ converge se e solo se converge la serie $\sum_{k=1}^{\infty} a_k$*

Dimostrazione: Indichiamo con s_n l'n-esima somma parziale, ovvero $\sum_{k=1}^{n} a_k$, mentre p_n indica come sopra l'n-esimo prodotto parziale. Grazie all'ipotesi $a_k \geq 0$, sia p_n che s_n sono successioni monotone non decrescenti. Inoltre $p_n \geq 1$. Abbiamo quindi

$$0 \leq s_n = \sum_{k=1}^{n} a_k < \prod_{k=1}^{n}(1+a_k) = p_n$$

Infatti ogni termine della somma compare nel prodotto, moltiplicato per l'1 che viene sommato a tutti gli altri termini. Inoltre nel prodotto compaiono anche altri termini positivi. Tenendo presente che $1 + x \leq e^x$ per ogni x, vale anche

$$p_n = \prod_{k=1}^{n}(1+a_k) \leq \prod_{k=1}^{n}(e^{a_k}) = e^{\sum_{k=1}^{n} a_k} = e^{s_n}$$

Mettendo insieme le due disuguaglianze otteniamo

$$0 \leq s_n < p_n \leq e^{s_n}$$

che implica che p_n converge se e solo se converge s_n. Notiamo che il minore stretto tra s_n e p_n garantisce che p_n non possa essere zero. □

Definizione 1.36 *Diciamo che il prodotto infinito $\prod_{k=1}^{\infty}(1+a_k)$ converge assolutamente se converge il prodotto infinito $\prod_{k=1}^{\infty}(1+|a_k|)$*

Teorema 1.37 *Se il prodotto infinito $\prod_{k=1}^{\infty}(1+a_k)$ converge assolutamente, e $a_k \neq -1$ per ogni k, allora converge.*

Dimostrazione: Poniamo $P_n = \prod_{k=1}^{n}(1+|a_k|)$. Se $p_n = \prod_{k=1}^{n}(1+a_k)$ converge assolutamente la successione dei P_n converge, e quindi converge anche la serie telescopica $\sum_{n=2}^{\infty}(P_n - P_{n-1})$. Sfruttando il fatto che $p_n = (1+a_n)p_{n-1}$, e analogamente $P_n = (1+|a_n|)P_{n-1}$ otteniamo

$$0 \leq |p_n - p_{n-1}| = |a_n p_{n-1}| = |a_n \prod_{k=1}^{n-1}(1+a_k)| \leq$$

$$\leq |a_n| \prod_{k=1}^{n-1}(1+|a_k|) = |a_n| P_{n-1} = P_n - P_{n-1}$$

Quindi anche $\sum_{n=2}^{\infty}|p_n - p_{n-1}|$ converge, ma questo implica la convergenza della serie

$$\sum_{n=2}^{\infty}(p_n - p_{n-1}) = \lim_{n\to\infty} p_n - p_1$$

Quindi la successione dei prodotti parziali $\{p_n\}$ converge ad un limite finito. Dobbiamo ora mostrare che questo limite è diverso da zero.
La convergenza dei $\{P_n\}$, grazie al Teorema 1.35, implica la convergenza della serie $\sum_{k=0}^{\infty}|a_k|$. Questo significa che a_k tende a zero al crescere di k, e in particolare per tutti i k sufficientemente grandi $|a_k| \leq 1/2$, da cui $|1+a_k| \geq 1/2$. Prendendo i reciproci da entrambi i lati e moltiplicando per $|a_k|$ otteniamo che la serie

$$\sum_{k=1}^{\infty}\left|\frac{-a_k}{1+a_k}\right| \leq 2\sum_{k=1}^{\infty}|a_k|$$

converge, essendo maggiorata in modulo da una serie convergente. Applicando nuovamente il Teorema 1.35 otteniamo che il prodotto infinito

$$\prod_{k=1}^{\infty}\left(1 - \frac{a_k}{1+a_k}\right)$$

converge assolutamente, e che quindi i suoi prodotti parziali

$$\prod_{k=1}^{n}\left(1-\frac{a_k}{1+a_k}\right)=\prod_{k=1}^{n}\left(\frac{1}{1+a_k}\right)=\frac{1}{\prod_{k=1}^{n}(1+a_k)}=\frac{1}{p_n}$$

convergono ad un limite finito. Ma questo implica che il limite della successione $\{p_n\}$ è diverso da zero, completando la dimostrazione. □

Definizione 1.38 *Un prodotto di Eulero è un prodotto infinito calcolato sui numeri primi. Può essere indicato come $\prod_p$, mentre una somma infinita sui primi può essere indicata con $\sum_p$.*

Teorema 1.39 *Sia $f(n)$ una funzione moltiplicativa non identicamente nulla. Se la serie $\sum_{n=1}^{\infty} f(n)$ converge assolutamente, allora vale*

$$\sum_{n=1}^{\infty} f(n)=\prod_p(1+f(p)+f(p^2)+\dots)=\prod_p(1+\sum_{k=1}^{\infty} f(p^k))$$

Inoltre, se f è completamente moltiplicativa vale anche

$$\sum_{n=1}^{\infty} f(n)=\prod_p\frac{1}{1-f(p)}$$

Dimostrazione: Se la serie $\sum_{n=1}^{\infty} f(n)$ converge assolutamente, allora per ogni primo p converge assolutamente la serie $a_p=\sum_{k=1}^{\infty} f(p^k)$, e quindi anche

$$\sum_p |a_p|=\sum_p\left|\sum_{k=1}^{\infty} f(p^k)\right|\le\sum_p\sum_{k=1}^{\infty}|f(p^k)|<\sum_{n=1}^{\infty}|f(n)|$$

converge, grazie alla possibilità di cambiare l'ordine nella sommatoria. Ma allora il prodotto infinito

$$\prod_p(1+a_p)=\prod_p\left(1+\sum_{k=1}^{\infty} f(p^k)\right)$$

converge assolutamente grazie al Teorema 1.35 e quindi converge per il teorema 1.37.
Dato $\epsilon>0$, possiamo scegliere N_0 tale che $\sum_{n>N_0}|f(n)|<\epsilon$. Per ogni intero positivo n, indichiamo con $P(n)$ il più grande fattore primo di n. Indichiamo allora con $\sum_{P(n)\le N}$ la somma su tutti i numeri il cui maggior fattore primo (e di conseguenza tutti gli altri) è minore o uguale a N. Al contrario, $\sum_{P(n)>N}$ indica la somma su tutti i numeri che hanno almeno un fattore primo maggiore di N. Prendiamo $N>N_0$. Osserviamo che, grazie al teorema fondamentale dell'aritmetica, ogni n tale che $P(n)<N$ si scrive in modo unico come prodotto di potenze di primi minori di N, e ovviamente ogni prodotto di questa forma è un numero n tale che $P(n)<N$; otteniamo quindi

$$\prod_{p\le N}\left(1+\sum_{k=1}^{\infty} f(p^k)\right)=\sum_{P(n)\le N} f(n)$$

da cui

$$\left|\sum_{n=1}^{\infty} f(n)-\prod_{p\le N}\left(1+\sum_{k=1}^{\infty} f(p^k)\right)\right|=\left|\sum_{n=1}^{\infty} f(n)-\sum_{P(n)\le N} f(n)\right|=$$

$$=\left|\sum_{P(n)>N} f(n)\right|\le\sum_{P(n)>N}|f(n)|\le\sum_{n>N}|f(n)|\le\sum_{n>N_0}|f(n)|<\epsilon$$

Ne segue che

$$\sum_{n=1}^{\infty} f(n)=\lim_{N\to\infty}\prod_{p\le N}\left(1+\sum_{k=1}^{\infty} f(p^k)\right)=\prod_p\left(1+\sum_{k=1}^{\infty} f(p^k)\right)$$

e questo dimostra la prima parte della tesi.
Se $f(n)$ è completamente moltiplicativa, $f(p^k)=f(p)^k$ per ogni p e k. Dato che la somma degli $f(n)$ converge, $f(p)^k$ deve tendere a zero, ma questo implica $|f(p)|<1$. Otteniamo quindi la progressione geometrica

$$1+\sum_{k=1}^{\infty} f(p^k)=1+\sum_{k=1}^{\infty} f(p)^k=\frac{1}{1-f(p)}$$

da cui

$$\prod_p \left(1 + \sum_{k=1}^{\infty} f(p^k)\right) = \prod_p \left(\frac{1}{1 - f(p)}\right)$$

□

1.5 Parte intera e parte frazionaria

Definizione 1.40 *Indichiamo con*

$$||\alpha|| = \min(|n - \alpha| : n \in \mathbb{Z}) = \inf(\{\alpha\}, 1 - \{\alpha\})$$

la distanza di un numero reale α dall'intero più vicino.

Osservazione 1.41 *Per la disparità del seno attorno ai multipli di π abbiamo $|\sin \pi\alpha| = \sin \pi||\alpha||$.*

Proposizione 1.42 *Per ogni coppia di reali α, β vale la disuguaglianza triangolare*

$$\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\|.$$

Dimostrazione:

$$\min(\{\alpha + \beta\}, 1 - \{\alpha + \beta\}) \leq \min(\{\alpha\}, 1 - \{\alpha\}) + \min(\{\beta\}, 1 - \{\beta\}).$$

□

Teorema 1.43 (Dirichlet) *Siano α, Q reali con $Q \geq 1$. Esistono allora due interi a, q tali che $1 \leq q \leq Q$,*

$$(a, q) = 1$$

e

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{qQ}.$$

Inoltre se $\alpha \in [0, 1]$ possiamo prendere $q \geq a$.

Dimostrazione: Sia $N = [Q]$. Supponiamo che $\{q\alpha\} \in [0, 1/(N+1))$ per qualche intero positivo $q \leq N$. Posto $a = [q\alpha]$, abbiamo

$$0 \leq \{q\alpha\} = q\alpha - [q\alpha] = q\alpha - a < \frac{1}{N+1}$$

e dividendo per q

$$\left|\alpha - \frac{a}{q}\right| < \frac{1}{q(N+1)} < \frac{1}{qQ}.$$

Se invece $\{q\alpha\} \in [N/(N+1), 1)$ per qualche $q \leq N$, per $a = [q\alpha] + 1$ otteniamo

$$\frac{N}{N+1} \leq \{q\alpha\} = q\alpha - a + 1 < 1$$

da cui sottraendo 1 ad entrambi i lati ricaviamo $|q\alpha - a| \leq \frac{1}{N+1}$ che implica

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q(N+1)} < \frac{1}{qQ}.$$

Se invece

$$\{q\alpha\} \in \left[\frac{1}{N+1}, \frac{N}{N+1}\right)$$

per ogni $q = 1, ..., N$, allora tutti gli N numeri reali $\{q\alpha\}$ stanno in uno degli $N - 1$ intervalli

$$\left[\frac{i}{N+1}, \frac{i+1}{N+1}\right)$$

con $i = 1, ..., N - 1$. Ma allora per il principio della piccionaia devono esistere due interi $1 \leq q_1 < q_2 \leq N$ e un terzo intero $i \in [1, N - 1]$ tali che

$$\{q_1\alpha\}, \{q_2\alpha\} \in \left[\frac{i}{N+1}, \frac{i+1}{N+1}\right).$$

Poniamo allora $q = q_2 - q_1 \in [1, N-1]$, dato che i due interi sono distinti, e $a = [q_2\alpha] - [q_1\alpha]$. In questo modo, dato che $\{q_1\alpha\}$ e $\{q_2\alpha\}$ stanno nello stesso intervallo di lunghezza $1/(N+1)$

$$|q\alpha - a| = |(q_2\alpha - [q_2\alpha]) - (q_1\alpha - [q_1\alpha])| = |\{q_2\alpha\} - \{q_1\alpha\}| < \frac{1}{N+1} < \frac{1}{Q}$$

e dividendo per q come sopra abbiamo la prima parte della tesi. Per averli coprimi è sufficiente ridurre la frazione a/q ai minimi termini, dato che questo lascia inalterato il termine a sinistra e aumenta quello a destra nella disuguaglianza.
Per costruzione, è chiaro che nel primo caso se $\alpha \leq 1$ allora $a = [q\alpha] \leq q$. Nel secondo caso $\{q\alpha\} > 0$ esclude la possibilità $\alpha = 1$, e quindi ancora $q \leq a$. Infine anche nel terzo caso la disuguaglianza segue immediatamente dalla definizione di a. □

Lemma 1.44 *Per $0 < \alpha < 1/2$ vale*

$$2\alpha < \sin \pi\alpha < \pi\alpha.$$

Dimostrazione: Indichiamo con $s(\alpha) = \sin \pi\alpha - 2\alpha$. Allora $s(0) = s(1/2) = 0$. Se $s(\alpha) = 0$ per qualche $0 < \alpha < 1/2$, allora $s'(\alpha) = \pi \cos \pi\alpha - 2$ dovrebbe, per il Teorema di Rolle, avere almeno due zeri in $(0, 1/2)$. Ma questo è impossibile perchè in tale intervallo $s'(\alpha)$ è monotona decrescente. Dato che ad esempio $s(1/4) = (\sqrt{2}-1)/2 > 0$, $s(\alpha) > 0$ per ogni $\alpha \in (0, 1/2)$, che dimostra la prima disuguaglianza. Ripetendo il ragionamento con $s(\alpha) = \pi\alpha - \sin \pi\alpha$ abbiamo anche la seconda disuguaglianza. □

Lemma 1.45 *Per ogni reale α e ogni coppia di interi $N_1 < N_2$ vale*

$$\sum_{n=N_1+1}^{N_2} e(\alpha n) \ll \min(N_2 - N_1, \|\alpha\|^{-1}).$$

Dimostrazione: Dato che $|e(\alpha n)| = |\cos 2\pi\alpha nx + i \sin 2\pi\alpha nx| = 1$ abbiamo

$$\left| \sum_{n=N_1+1}^{N_2} e(\alpha n) \right| \leq \sum_{n=N_1+1}^{N_2} 1 = N_2 - N_1.$$

Se $\alpha \notin \mathbb{Z}$, allora $\|\alpha\| > 0$ e possiamo studiare anche il termine $\|\alpha\|^{-1}$. In questo caso $e(\alpha) \neq 1$. Dato che $e(\alpha n) = e(\alpha)^n$, possiamo vedere la somma come progressione geometrica, e raccogliendo il primo termine $e(\alpha(N_1+1))$ abbiamo

$$\left| \sum_{n=N_1+1}^{N_2} e(\alpha n) \right| = \left| e(\alpha(N_1+1)) \sum_{n=0}^{N_2-N_1-1} e(\alpha)^n \right| = \left| e(\alpha(N_1+1)) \left(\frac{e(\alpha(N_2-N_1)) - 1}{e(\alpha) - 1} \right) \right| \leq$$
$$\frac{2}{|e(\alpha) - 1|} = \frac{2}{|e(\alpha) - 1|} \frac{1}{|e(\alpha/2)|} = \frac{2}{|e(\alpha/2) - e(-\alpha/2)|} = \frac{2}{|2i \sin \pi\alpha|} =$$
$$= \frac{1}{|\sin \pi\alpha|} = \frac{1}{\sin(\pi\|\alpha\|)} \leq \frac{1}{2\|\alpha\|},$$

sfruttando nel penultimo passaggio la simmetria del seno attorno ai multipli di π e nell'ultimo il Lemma 1.44. □

Lemma 1.46 *Siano α reale, q, a interi tali che $q \geq 1$ e $(a, q) = 1$. Se*

$$\left| \alpha - \frac{a}{q} \right| \leq \frac{1}{q^2},$$

allora

$$\sum_{1 \leq r \leq q/2} \frac{1}{\|\alpha r\|} \ll q \log q.$$

Dimostrazione: Il lemma vale sempre per $q = 1$, dato che la somma a sinistra risulta vuota. Assumiamo quindi $q \geq 2$. Per ogni intero r, ad a fissato, esistono due interi $s(r) \in [0, q/2]$ e $m(r)$ tali che

$$\frac{s(r)}{q} = \left\| \frac{ar}{q} \right\| = \pm \left(\frac{ar}{q} - m(r) \right)$$

grazie alla definizione di $\|\cdot\|$. Dato che $(a,q)=1$, $s(r)=0$ se e solo se $r\equiv 0\ (\mathrm{mod} q)$. Questo non è possibile se $r\in[1,q/2]$ e quindi in tal caso anche $s(r)\in[1,q/2]$. Poniamo

$$\alpha-\frac{a}{q}=\frac{\theta}{q^2}$$

dove $-1\le\theta\le 1$ per ipotesi. Abbiamo allora

$$\alpha r=\frac{ar}{q}+\frac{\theta r}{q^2}=\frac{ar}{q}+\frac{\theta'}{2q},$$

dove

$$|\theta'|=\left|\frac{2\theta r}{q}\right|\le|\theta|\le 1.$$

Segue allora dalla Proposizione 1.42 che

$$\|\alpha r\|=\left\|\frac{ar}{q}+\frac{\theta'}{2q}\right\|=\left\|m(r)\pm\frac{s(r)}{q}+\frac{\theta'}{2q}\right\|=\left\|\frac{s(r)}{q}\pm\frac{\theta'}{2q}\right\|\ge$$
$$\ge\left\|\frac{s(r)}{q}\right\|-\left\|\frac{\theta'}{2q}\right\|\ge\frac{s(r)}{q}-\frac{1}{2q}$$

sfruttando nell'ultimo passaggio il fatto che il primo termine è positivo e minore o uguale a un mezzo, mentre il secondo è maggiorato da $1/2q$.
Prendiamo ora $1\le r_1\le r_2\le q/2$ e supponiamo $s(r_1)=s(r_2)$. Avremo

$$\pm\left(\frac{ar_1}{q}-m(r_1)\right)=\pm\left(\frac{ar_2}{q}-m(r_2)\right)$$

da cui $ar_1\equiv\pm ar_2\ (mod\ q)$. Dato che $(a,q)=1$ questo equivale a dire $r_1\equiv\pm r_2\ (mod\ q)$, e quindi, avendo preso $1\le r_1\le r_2\le q/2$, $r_1=r_2$. Ne consegue una corrispondenza biunivoca tra gli $r\in[1,q/2]$ e gli $s(r)$ nello stesso intervallo. Ma dato che gli r coprono tutto l'intervallo (intersecato con $\mathbb{N}$) lo stesso faranno gli s. Mettendo insieme la stima per $\|\alpha r\|$ e questa osservazione otteniamo quindi

$$\sum_{1\le r\le q/2}\frac{1}{\|\alpha r\|}\le\sum_{1\le r\le q/2}\frac{1}{s(r)/q-1/2q}=\sum_{1\le s\le q/2}\frac{1}{s/q-1/2q}=$$
$$=2q\sum_{1\le s\le q/2}\frac{1}{2s-1}\le 2q\sum_{1\le s\le q/2}\frac{1}{s}\ll q\log q$$

grazie al Teorema 1.8. □

Lemma 1.47 *Siano α reale, q,a interi tali che $q\ge 1$ e $(a,q)=1$. Se*

$$\left|\alpha-\frac{a}{q}\right|\le\frac{1}{q^2},$$

allora per ogni V e h non negativi, con h intero, abbiamo

$$\sum_{r=1}^{q}\min\left(V,\frac{1}{\|\alpha(hq+r)\|}\right)\ll V+q\log q.$$

Dimostrazione: Poniamo

$$\alpha=\frac{a}{q}+\frac{\theta}{q^2}$$

con $-1\le\theta\le 1$ per ipotesi. Allora per ogni intero $1\le r\le q$ abbiamo

$$\alpha(hq+r)=ah+\frac{ar}{q}+\frac{\theta h}{q}+\frac{\theta r}{q^2}=$$
$$ah+\frac{ar}{q}+\frac{[\theta h]+\{\theta h\}}{q}+\frac{\theta r}{q^2}=ah+\frac{ar+[\theta h]+\delta(r)}{q}$$

dove

$$-1\le\delta(r)=\{\theta h\}+\frac{\theta r}{q}<2.$$

grazie alle ipotesi su r e θ. Allora per ogni r esiste unico r' tale che

$$\{\alpha(hq+r)\} = \frac{ar + [\theta h] + \delta(r)}{q} - r'.$$

Prendiamo allora $0 \le t \le 1 - 1/q$. Se

$$t \le \{\alpha(hq+r)\} \le t + \frac{1}{q}$$

allora moltiplicando per q otteniamo

$$qt \le ar - qr' + [\theta h] + \delta(r) \le qt + 1$$

da cui

$$\begin{cases} ar - qr' \le qt - [\theta h] + 1 - \delta(r) \le qt - [\theta h] + 2 \\ ar - qr' \ge qt - [\theta h] - \delta(r) > qt - [\theta h] - 2 \end{cases}$$

ovvero $ar - qr' \in J$ dove J è l'intervallo

$$J = (qt - [\theta h] - 2, qt - [\theta h] + 2].$$

L'intervallo J contiene esattamente 4 interi. Ragionando come nella dimostrazione precedente (il termine qr' non influisce) abbiamo che se $1 \le r_1 \le r_2 \le q$ e $ar_1 - qr_1' = ar_2 - qr_2'$ allora $r_1 = r_2$. Quindi per ogni $t \in [0, 1 - 1/q]$ fissato esistono al più 4 interi distinti $r \in [1, q]$ tali che $\{\alpha(hq+r)\} \in [t, t + (1/q)] = T(t)$. Osserviamo però che $\|\alpha(hq+r)\| \in T(t)$ se e solo se uno tra $\{\alpha(hq+r)\}$ e $1 - \{\alpha(hq+r)\}$ vi appartiene. La seconda inclusione può essere poi riscritta come

$$\{\alpha(hq+r)\} \in T(t')$$

dove $0 \le t' = 1 - 1/q - t \le 1 - 1/q$. $T(t')$ è quindi un intervallo che coprirà a sua volta al più 4 valori di r. Quindi ricapitolando per ogni $t \in [0, (q-1)/q]$ ci sono al più 8 interi $r \in [1, q]$ tali che $\|\alpha(hq+r)\| \in T(t)$. Indichiamo allora con $J(s) = T(s/q) = [s/q, (s+1)/q]$. Per ottenere la tesi vogliamo stimare

$$\sum_{r=1}^{q} \min\left(V, \frac{1}{\|\alpha(hq+r)\|}\right)$$

Se $\|\alpha(hq+r)\| \in J(0)$ usiamo il fatto che

$$\min\left(V, \frac{1}{\|\alpha(hq+r)\|}\right) \le V,$$

se invece $\|\alpha(hq+r)\| \in J(s)$ per $s \ge 1$ vale comunque

$$\min\left(V, \frac{1}{\|\alpha(hq+r)\|}\right) \le \frac{1}{\|\alpha(hq+r)\|} \le \frac{q}{s}$$

per definizione di $J(s)$. Dato che per definizione $\|\alpha(hq+r)\| \le 1/2 \le q/2$, possiamo prendere per ogni r $s < q/2$. Otteniamo allora

$$\sum_{r=1}^{q} \min\left(V, \frac{1}{\|\alpha(hq+r)\|}\right) \le 8V + 8 \sum_{1 \le s < q/2} \frac{q}{s} \ll V + q \log q$$

sempre per il Teorema 1.8. □

Lemma 1.48 *Siano α reale, q, a interi tali che $q \ge 1$ e $(a, q) = 1$. Se*

$$\left|\alpha - \frac{a}{q}\right| \le \frac{1}{q^2},$$

allora per ogni reale $U \ge 1$ e ogni n intero positivo vale

$$\sum_{1 \le k \le U} \min\left(\frac{n}{k}, \frac{1}{\|ak\|}\right) \ll \left(\frac{n}{q} + U + q\right) \log 2qU.$$

Dimostrazione: Possiamo scrivere ogni k nella forma

$$k = hq + r,$$

con $1 \leq r \leq q$ e $0 \leq h \leq U/q$. Allora

$$S = \sum_{1 \leq k \leq U} \min\left(\frac{n}{k}, \frac{1}{\|\alpha k\|}\right) \leq \sum_{0 \leq h \leq U/q} \sum_{1 \leq r \leq q} \min\left(\frac{n}{hq+r}, \frac{1}{\|\alpha(hq+r)\|}\right).$$

Per $h = 0$ e $1 \leq r \leq q/2$ possiamo applicare il Lemma 1.46 e ottenere

$$\sum_{1 \leq r \leq q/2} \min\left(\frac{n}{r}, \frac{1}{\|\alpha r\|}\right) \leq \sum_{1 \leq r \leq q/2} \frac{1}{\|\alpha r\|} \ll q \log q.$$

Altrimenti, o $h \geq 1$ e allora

$$hq + r > hq \geq \frac{(h+1)q}{2}$$

oppure se $h = 0$ abbiamo anche $q/2 < r \leq q$ e quindi

$$hq + r = r > \frac{q}{2} = \frac{(h+1)q}{2}.$$

In entrambi i casi

$$\frac{1}{hq+r} < \frac{2}{(h+1)q}$$

da cui

$$S \ll q \log q + \sum_{0 \leq h \leq U/q} \sum_{1 \leq r \leq q} \min\left(\frac{n}{(h+1)q}, \frac{1}{\|\alpha(hq+r)\|}\right).$$

Applicando allora il Lemma 1.47 con $V = n/(h+1)q$ per stimare la somma interna, e in seguito ancora il Teorema 1.8 otteniamo

$$\begin{aligned}
q \log q + \sum_{0 \leq h \leq U/q} \sum_{1 \leq r \leq q} \min\left(\frac{n}{(h+1)q}, \frac{1}{\|\alpha(hq+r)\|}\right) &\ll \\
\ll q \log q + \sum_{0 \leq h < U/q} \left(\frac{n}{(h+1)q} + q \log q\right) &= \\
= q \log q + \frac{n}{q} \sum_{0 \leq h < U/q} \frac{1}{h+1} + \left(\frac{U}{q} + 1\right) q \log q &\ll \\
\ll q \log q + \frac{n}{q} \log\left(\frac{U}{q} + 1\right) + U \log q + q \log q &\ll \\
\ll \left(\frac{n}{q} + U + q\right) \log 2qU &
\end{aligned}$$

grazie al fatto che $2qU \geq 2\max(q, U) \geq U + q \geq U/q + 1$ dato che $q \geq 1$ per ipotesi. □

2 Distribuzione dei numeri primi

In questa sezione introduciamo alcuni risultati sulla distribuzione dei numeri primi, che risulteranno utili in seguito.

Definizione 2.1 (Serie di Dirichlet) *Sia $s = \sigma + it$ un numero complesso. Ad ogni successione di numeri complessi $a_1, a_2, \dots$ associamo la sua serie di Dirichlet definita come*

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

Osservazione 2.2 *Se la serie $F(s)$ converge assolutamente per $s_0 = \sigma_0 + it_0$, allora converge assolutamente per tutti gli $s = \sigma + it$ tali che $\sigma \geq \sigma_0$, dato che $|n^s| = n^\sigma$ e quindi*

$$\left|\frac{a_n}{n^s}\right| = \frac{|a_n|}{n^\sigma} \leq \frac{|a_n|}{n^{\sigma_0}} = \left|\frac{a_n}{n^{s_0}}\right|$$

che converge.

Definizione 2.3 *Prendendo $a_n = 1$ per ogni n otteniamo la funzione Zeta di Riemann, definita come*

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

Questa serie di Dirichlet converge assolutamente per ogni s con $\Re(s) > 1$.

Teorema 2.4 *Sia $f(n)$ una funzione moltiplicativa. Se la serie di Dirichlet*

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

converge assolutamente per tutti i numeri complessi s tali che $\Re(s) > \sigma_0$, allora $F(s)$ può essere espressa come prodotto infinito

$$F(s) = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} \dots\right)$$

Se inoltre f è totalmente moltiplicativa

$$F(s) = \prod_p \left(1 - \frac{f(p)}{p^s}\right)^{-1}$$

Questa espressione è detta prodotto di Eulero di $F(s)$.

Dimostrazione: Basta notare che se $f(n)$ è (totalmente) moltiplicativa, allora lo è anche $f(n)/n^s$. La tesi segue direttamente dal Teorema 1.39. □

Osservazione 2.5 *Dato che la Zeta di Riemann converge sul semipiano complesso $\Re(s) > 1$, segue dal Teorema 2.4 che il suo prodotto di Eulero in tale regione vale*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

Teorema 2.6 (Euclide) *Esistono infiniti numeri primi.*

Dimostrazione: Per $0 < x < 1$ la serie di Taylor del logaritmo vale

$$\log(1-x) = -\sum_{n=1}^{\infty} \frac{x^n}{n}$$

Per $\sigma > 0$, $\zeta(1+\sigma) > 1$ e vale

$$\log \zeta(1+\sigma) = \log \prod_p \left(1 - \frac{1}{p^{1+\sigma}}\right)^{-1} = -\sum_p \log\left(1 - \frac{1}{p^{1+\sigma}}\right) =$$

$$= \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{n(1+\sigma)}} = \sum_p \frac{1}{p^{1+\sigma}} + \sum_p \sum_{n=2}^{\infty} \frac{1}{np^{n(1+\sigma)}}$$

Dato che

$$0 < \sum_p \sum_{n=2}^{\infty} \frac{1}{np^{n(1+\sigma)}} < \sum_p \sum_{n=2}^{\infty} \frac{1}{p^n} = \sum_p \frac{1}{p(p-1)} < \infty$$

segue che

$$\log \zeta(1+\sigma) = \sum_p \frac{1}{p^{1+\sigma}} + \mathcal{O}(1) \tag{1}$$

Se prendiamo $0 < \sigma < 1$ abbiamo

$$1 < \frac{1}{\sigma} = \int_1^{\infty} \frac{1}{x^{1+\sigma}} dx < \zeta(1+\sigma) < 1 + \int_1^{\infty} \frac{1}{x^{1+\sigma}} = 1 + \frac{1}{\sigma}$$

sfruttando il fatto che $\zeta(1+\sigma) = \sum_{n=1}^{\infty} \frac{1}{n^{1+\sigma}}$ corrisponde alle somme superiori nel primo integrale, e alle somme inferiori nel secondo. Sfruttando poi la monotonia del logaritmo otteniamo

$$0 < \log \frac{1}{\sigma} < \log \zeta(1+\sigma) < \log \left(1 + \frac{1}{\sigma}\right) = \log \left(\frac{1}{\sigma}(1+\sigma)\right) =$$
$$= \log \frac{1}{\sigma} + \log(1+\sigma) < \log \frac{1}{\sigma} + \sigma$$

da cui ricaviamo

$$\log \zeta(1+\sigma) = \log \frac{1}{\sigma} + \mathcal{O}(\sigma) = \log \frac{1}{\sigma} + \mathcal{O}(1) \tag{2}$$

Combinando le espressioni contenute in (1) e (2) otteniamo

$$\log \frac{1}{\sigma} = \sum_p \frac{1}{p^{1+\sigma}} + \mathcal{O}(1)$$

dove abbiamo preso $0 < \sigma < 1$. Se esistesse solo un numero finito di primi, il lato destro dell'uguaglianza resterebbe limitato al tendere di σ a zero, ma il lato sinistro tende ad infinito e questo è impossibile. Devono quindi esistere infiniti primi. □

2.1 Teorema di Chebychev

Definizione 2.7 *Definiamo ora tre importanti funzioni sui primi:*

$$\pi(x) = \sum_{p \le x} 1$$

$$\vartheta(x) = \sum_{p \le x} \log p$$

$$\psi(x) = \sum_{p^k \le x} \log p$$

$\vartheta(x)$ e $\psi(x)$ sono dette funzioni di Chebyshev.

Lemma 2.8 *Per $n \ge 1$ e $1 \le k \le n$ vale*

$$\binom{n}{k-1} < \binom{n}{k} \iff k < \frac{n+1}{2},$$

$$\binom{n}{k-1} > \binom{n}{k} \iff k > \frac{n+1}{2},$$

$$\binom{n}{k-1} = \binom{n}{k} \iff n \text{ dispari e } k = \frac{n+1}{2}.$$

Questo in particolare implica che il massimo coefficiente binomiale è quello centrale per n pari, e i due centrali per n dispari.

Dimostrazione: È sufficiente notare che il rapporto tra i due coefficienti binomiali vale

$$\binom{n}{k}\binom{n}{k-1}^{-1} = \frac{(k-1)!(n-k+1)!}{k!(n-k)!} = \frac{n+1}{k} - 1$$

□

Lemma 2.9 *Sia $n \geq 1$ e $N = \binom{2n}{n}$. Allora*

$$N < 2^{2n} \leq 2nN$$

Dimostrazione: Grazie al Lemma 2.8 sappiamo che N è il coefficiente maggiore nell'espansione di $(1+1)^n$. Otteniamo quindi

$$N = \binom{2n}{n} < \sum_{k=0}^{2n} \binom{2n}{k} = (1+1)^{2n} = 2^{2n}$$

$$2^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} = 1 + \sum_{k=1}^{2n-1} +1 \leq 2 + (2n-1)\binom{2n}{n} \leq 2n\binom{2n}{n} \leq 2nN$$

□

Definizione 2.10 *Per ogni intero n e ogni primo p, indichiamo con $v_p(n)$ la più grande potenza di p che divide n. Diciamo inoltre che $p^k || n$ se $p^k | n$ e $p^{k+1} \nmid n$. È chiaro che $p^k || n$ se e solo se $v_p(n) = k$.*

Lemma 2.11 *Per ogni intero positivo n vale $v_p(n) \leq \log n / \log p$, e inoltre*

$$v_p(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right] = \sum_{k=1}^{[\log n/\log p]} \left[\frac{n}{p^k}\right].$$

Dimostrazione: Osserviamo che se $v_p(n) = k$ allora $p^k || n \Rightarrow p^k \leq n \Rightarrow v_p(n) \leq \log n / \log p$. Inoltre $v_p(mn) = v_p(m) + v_p(n)$, per l'unicità della fattorizzazione come prodotto di potenze di primi. Abbiamo allora, semplicemente riordinando le somme,

$$v_p(n!) = \sum_{m=1}^{n} v_p(m) = \sum_{m=1}^{n} \sum_{\substack{k \geq 1 \\ p^k | m}} 1 = \sum_{k=1}^{\infty} \sum_{\substack{m=1 \\ p^k = m}}^{n} 1 = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$$

dove nell'ultimo passaggio abbiamo sfruttato il fatto che, a k fissato, i numeri minori di n divisibili per p^k sono esattamente $\lfloor n/p^k \rfloor$. Questo dimostra la prima uguaglianza. Per la seconda è sufficiente notare che per ogni $k > [\log n / \log p]$ vale $n/p^k < 1$, e quindi $[n/p^k] = 0$. □

Teorema 2.12 (Chebyshev) *Esistono due costanti positive c_1, c_2 tali che*

$$c_1 x \leq \vartheta(x) \leq \psi(x) \leq \pi(x) \log x \leq c_2 x \tag{3}$$

per $x \geq 2$. Inoltre

$$\liminf_{x\to\infty} \frac{\vartheta(x)}{x} = \liminf_{x\to\infty} \frac{\psi(x)}{x} = \liminf_{x\to\infty} \frac{\pi(x)\log x}{x} \geq \log 2 \tag{4}$$

e

$$\limsup_{x\to\infty} \frac{\vartheta(x)}{x} = \limsup_{x\to\infty} \frac{\psi(x)}{x} = \limsup_{x\to\infty} \frac{\pi(x)\log x}{x} \leq 4\log 2 \tag{5}$$

Dimostrazione: Sia $x \geq 2$. Se $p^k \leq x$, allora $k \leq [\log x / \log p]$ e quindi

$$\begin{aligned} \vartheta(x) = \sum_{p\leq x} \log p \leq \psi(x) = \sum_{p^k \leq x} \log p \leq \\ \leq \sum_{p\leq x} \left[\frac{\log x}{\log p}\right] \log p \leq \sum_{p\leq x} \log x = \pi(x)\log x. \end{aligned} \tag{6}$$

Ovviamente queste disuguaglianze si mantengono anche dividendo per x e prendendo lim sup e lim inf. Prendiamo ora $0 < \delta < 1$. Abbiamo

$$\begin{aligned} \vartheta(x) = \sum_{p\leq x} \log p \geq \sum_{x^{1-\delta} < p \leq x} \log p \geq \sum_{x^{1-\delta} < p \leq x} \log x^{1-\delta} = \\ = \sum_{x^{1-\delta} < p \leq x} (1-\delta)\log x = (1-\delta)(\pi(x) - \pi(x^{1-\delta}))\log x \geq \\ \geq (1-\delta)\pi(x)\log x - x^{1-\delta}\log x, \end{aligned}$$

essendo $x \geq \pi(x)$ per ogni x. Otteniamo quindi

$$\frac{\vartheta(x)}{x} \geq \frac{(1-\delta)\pi(x)\log x}{x} - \frac{\log x}{x^\delta}$$

Passando ai limiti

$$\liminf_{x\to\infty} \frac{\vartheta(x)}{x} \geq (1-\delta) \liminf_{x\to\infty} \frac{\pi(x)\log x}{x},$$

ma questo deve valere per ogni δ, e abbiamo quindi

$$\liminf_{x\to\infty} \frac{\vartheta(x)}{x} \geq \liminf_{x\to\infty} \frac{\pi(x)\log x}{x}.$$

Lo stesso procedimento ci permette di ottenere un risultato analogo per il lim sup, e queste disuguaglianze assieme alla (6) permettono di dimostrare le uguaglianze in (4) e (5).
Sia ora $n \geq 1$, e

$$N = \binom{2n}{n} = \frac{2n(2n-1)\cdots(n+1)}{n!}.$$

Grazie al Lemma 2.9 abbiamo

$$\frac{2^{2n}}{2n} \leq N < 2^{2n}.$$

Se prendiamo p primo tale che $n < p \leq 2n$, notiamo che p divide il numeratore di N, che contiene nel suo prodotto tutti i p di questa forma ma non il suo denominatore, prodotto di numeri minori di p. Questo implica che, per ognuno di questi p, $p|N$. Ma essendo primi, da questo segue che il loro prodotto divide N, e quindi che

$$\prod_{n<p\leq 2n} p \leq N \leq 2^{2n}.$$

Prendendo $n = 2^{r-1}$, con $r \geq 1$, abbiamo

$$\prod_{2^{r-1}<p\leq 2^r} p \leq N \leq 2^{2^r}.$$

Segue che, per ogni $R \geq 1$,

$$\prod_{p\leq 2^R} p = \prod_{r=1}^{R} \prod_{2^{r-1}<p\leq 2^r} p < \prod_{r=1}^{R} 2^{2^R} < 2^{2^{R+1}}.$$

Per ogni $x \geq 2$ possiamo trovare $R \geq 1$ tale che $2^{R-1} < x \leq 2^R$. Otteniamo allora

$$\prod_{p\leq x} p \leq \prod_{p\leq 2^R} p < 2^{2^{R+1}} < 2^{4x},$$

da cui segue

$$\vartheta(x) = \sum_{p\leq x} \log(p) = \log\left(\prod_{p\leq x} p\right) < (4\log 2)x$$

e quindi

$$\limsup_{x\to\infty} \frac{\vartheta(x)}{x} \leq 4\log 2.$$

Ci manca ora il limite inferiore. Iniziamo ad osservare che, grazie alla definizione di $v_p(n)$, abbiamo

$$(2n)! = \prod_{p\leq 2n} p^{v_p(2n!)}$$

mentre

$$(n!)^2 = \prod_{p\leq n} p^{2v_p(n!)}.$$

Possiamo quindi scrivere

$$N = \binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \prod_{p\leq 2n} p^{v_p(2n!)-2v_p(n!)}.$$

Grazie al Lemma 2.11, e osservando che $[2t] - 2[t]$ può valere solo 0 o 1,

$$v_p(2n!) - 2v_p(n!) = \sum_{k=1}^{[\log 2n/\log p]} \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right) \leq \frac{\log 2n}{\log p}.$$

Sfruttando ora la stima data dal Lemma 2.9 abbiamo

$$\frac{2^{2n}}{2n} \leq N = \prod_{p \leq 2n} p^{v_p(2n!) - 2v_p(n!)} \leq \prod_{p \leq 2n} p^{\frac{\log 2n}{\log p}} = \prod_{p \leq 2n} 2n = (2n)^{\pi(2n)},$$

da cui otteniamo

$$\pi(2n) \log 2n \geq 2n \log 2 - \log 2n.$$

Se ora prendiamo $n = [x/2]$, abbiamo $2n \leq x < 2n + 2$ e quindi

$$\pi(x) \log x \geq \pi(2n) \log 2n \geq 2n \log 2 - \log 2n > (x-2) \log 2 - \log x = \\ = x \log 2 - \log x - 2 \log 2.$$

Dividendo per x otteniamo

$$\frac{\pi(x) \log x}{x} > \log 2 - \frac{\log x + 2 \log 2}{x}$$

e quindi

$$\liminf_{x \to \infty} \frac{\pi(x) \log x}{x} \geq \log 2.$$

Questo dimostra che anche il rapporto $\frac{\vartheta(x)}{x}$ è limitato dal basso, e, dato che $\vartheta(2) > 0$, concludiamo che $\vartheta(x) \geq c_1 x$ per ogni $x \geq 2$, con $c_1 > 0$. □

Teorema 2.13 *Indichiamo con p_n l'n-esimo numero primo. Esistono allora due costanti positive, c_3 e c_4 tali che*

$$c_3 n \log n \leq p_n \leq c_4 n \log n$$

per ogni $n \geq 2$.

Dimostrazione: Grazie al Teorema 2.12 sappiamo che

$$\frac{c_1 p_n}{\log p_n} \leq \pi(p_n) = n \leq \frac{c_2 p_n}{\log p_n}$$

da cui segue, passando ai reciproci

$$c_2^{-1} n \log p_n \leq p_n \leq c_1^{-1} n \log p_n. \tag{7}$$

Dato che $n \leq p_n$, $\log n \leq \log p_n$, e quindi

$$p_n \geq c_2^{-1} n \log n = c_3 n \log n,$$

che dimostra la prima disuguaglianza.
Passando ai logaritmi nel lato destro della (7) otteniamo

$$\log p_n \leq \log n + \log \log p_n + \log c_1^{-1} \leq \log n + 2 \log \log p_n$$

per n sufficientemente grande, essendo c_1 fissato. Inoltre, sempre per n grande, abbiamo $2 \log \log p_n \leq \frac{1}{2} \log p_n$ da cui

$$\log p_n \leq \log n + 2 \log \log p_n \leq \log n + \frac{1}{2} \log p_n$$

che implica

$$\log p_n \leq 2 \log n.$$

Inserendo nuovamente questo risultato in (7) otteniamo

$$p_n \leq c_1^{-1} n \log p_n \leq 2 c_1^{-1} n \log n$$

per ogni $n > \bar{n}$, con $\bar{n}$ fissato in modo da rispettare entrambe le condizioni precedenti. Esiste quindi una costante c_4 tale che

$$p_n \leq c_4 n \log n.$$

□

2.2 Teoremi di Mertens

Lemma 2.14 *Per ogni $x \geq 1$ abbiamo*

$$0 \leq \sum_{n \leq x} \log\left(\frac{x}{n}\right) < x.$$

Dimostrazione: Dato che la funzione $h(t) = \log\left(\frac{x}{t}\right)$ è monotona decrescente su $[1, x]$, possiamo considerare le sue somme inferiori

$$\sum_{n=2}^{x} \log\left(\frac{x}{n}\right) = \sum_{n=1}^{x} \log\left(\frac{x}{n}\right) - \log x.$$

Abbiamo quindi

$$\sum_{n \leq x} \log\left(\frac{x}{n}\right) < \log x + \int_1^x \log\left(\frac{x}{t}\right) dt = \log x + \int_1^x (\log x - \log t)\, dt =$$

$$= x \log x - \int_1^x \log t dt = x \log x - (x \log x - x + 1) = x - 1 < x$$

□

Definizione 2.15 *Introduciamo la funzione $\Lambda(n)$, detta funzione di von Mangoldt, definita come*

$$\Lambda(n) = \begin{cases} \log p & \text{se } n = p^m \text{ è potenza di un primo} \\ 0 & \text{altrimenti} \end{cases}$$

Osservazione 2.16 *Abbiamo*

$$\psi(x) = \sum_{p^k \leq x} \log p = \sum_{m=1}^{x} \Lambda(m)$$

Teorema 2.17 (Mertens) *Per ogni $x \geq 1$ vale*

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + \mathcal{O}(1)$$

Dimostrazione: Prendiamo $N = [x]$. Grazie al Lemma 2.14 abbiamo

$$0 \leq \sum_{n \leq x} \log\left(\frac{x}{n}\right) = \sum_{n \leq x} (\log x - \log n) = N \log x - \sum_{n=1}^{N} \log n =$$

$$= x \log x - \log N! + \mathcal{O}(\log x) < x$$

e quindi

$$\log N! = x \log x + \mathcal{O}(x).$$

D'altra parte, grazie al Lemma 2.11 otteniamo

$$\log N! = \log\left(\prod_{p \leq N} p^{v_p(N!)}\right) = \sum_{p \leq N} \log p^{v_p(N!)} = \sum_{p \leq N} v_p(N!) \log p =$$

$$= \sum_{p \leq N} \sum_{k=1}^{[\log N / \log p]} \left[\frac{N}{p^k}\right] \log p = \sum_{p^k \leq N} \left[\frac{N}{p^k}\right] \log p =$$

$$\sum_{p^k \leq x} \left[\frac{x}{p^k}\right] \log p = \sum_{n \leq x} \left[\frac{x}{n}\right] \Lambda(n) = \sum_{n \leq x} \left(\frac{x}{n} + \mathcal{O}(1)\right) \Lambda(n) =$$

$$= x \sum_{n \leq x} \frac{\Lambda(n)}{n} + \mathcal{O}\left(\sum_{n \leq x} \Lambda(n)\right) = x \sum_{n \leq x} \frac{\Lambda(n)}{n} + \mathcal{O}(\psi(x)) =$$

$$= x \sum_{n \leq x} \frac{\Lambda(n)}{n} + \mathcal{O}(x)$$

dove nell'ultima uguaglianza abbiamo sfruttato il Teorema 2.12. Unendo le due uguaglianze otteniamo

$$x \sum_{n \leq x} \frac{\Lambda(n)}{n} + \mathcal{O}(x) = x \log x + \mathcal{O}(x)$$

e quindi

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} + \mathcal{O}(1) = \log x + \mathcal{O}(1)$$

da cui la tesi. □

Teorema 2.18 (Mertens) *Per ogni $x \geq 1$ vale*

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + \mathcal{O}(1)$$

Dimostrazione: Per metterci nelle condizioni del Teorema 2.17, calcoliamo

$$0 \leq \sum_{n \leq x} \frac{\Lambda(n)}{n} - \sum_{p \leq x} \frac{\log p}{p} = \sum_{\substack{p^k \leq x \\ k \geq 2}} \frac{\log p}{p^k} \leq \sum_{p \leq x} \log p \sum_{k=2}^{\infty} \frac{1}{p^k} =$$

$$= \sum_{p \leq x} \log p \left(\frac{p}{p-1} - 1 - \frac{1}{p} \right) = \sum_{p \leq x} \frac{\log p}{p(p-1)} \leq 2 \sum_{p \leq x} \frac{\log p}{p^2} \leq$$

$$\leq 2 \sum_{n=1}^{\infty} \frac{\log n}{n^2} = \mathcal{O}(1).$$

Grazie al Teorema 2.17 abbiamo ora

$$\sum_{p \leq x} \frac{\log p}{p} = \sum_{n \leq x} \frac{\Lambda(n)}{n} + \mathcal{O}(1) = \log x + \mathcal{O}(1)$$

□

Teorema 2.19 *Esiste una costante $b_1 > 0$ tale che*

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + b_1 + \mathcal{O}\left(\frac{1}{\log x} \right)$$

per $x \geq 2$.

Dimostrazione: Scriviamo

$$\sum_{p \leq x} \frac{1}{p} = \sum_{p \leq x} \frac{\log p}{p} \frac{1}{\log p} = \sum_{n \leq x} u(n) f(n),$$

dove abbiamo posto

$$u(n) = \begin{cases} \frac{\log p}{p} & \text{se } n = p \\ 0 & \text{altrimenti} \end{cases}$$

e

$$f(n) = \frac{1}{\log n}.$$

Definiamo quindi $U(t)$ e $g(t)$ in modo che valga

$$U(t) = \sum_{n \leq t} u(n) = \sum_{p \leq t} \frac{\log p}{p} = \log t + g(t).$$

Allora grazie al Teorema 2.18 $g(t) = \mathcal{O}(1)$, e inoltre $U(t) = 0$ per $t < 2$. Questo implica che

$$\int_2^{\infty} \frac{g(t)}{t(\log t)^2} dt$$

converge assolutamente e

$$\int_x^\infty \frac{g(t)}{t(\log t)^2}dt = \mathcal{O}\left(\int_x^\infty \frac{dt}{t(\log t)^2}\right) = \mathcal{O}\left(\frac{1}{\log x}\right).$$

Grazie al Teorema 1.7 otteniamo quindi

$$\begin{aligned}\sum_{p\le x}\frac{1}{p} = \sum_{n\le x} u(n)f(n) = f(x)U(x) - \int_2^x U(t)f'(t)dt = \\ = \frac{\log x + g(x)}{\log x} + \int_2^x \frac{\log t + g(t)}{t(\log t)^2}dt = \\ = 1 + \mathcal{O}\left(\frac{1}{\log x}\right) + \int_2^x \frac{1}{t\log t}dx + \int_2^\infty \frac{g(t)}{t(\log t)^2}dt - \int_x^\infty \frac{g(t)}{t(\log t)^2}dt = \\ = \log\log x - \log\log 2 + \int_2^\infty \frac{g(t)}{t(\log t)^2}dt + 1 + \mathcal{O}\left(\frac{1}{\log x}\right) = \\ = \log\log x + b_1 + \mathcal{O}\left(\frac{1}{\log x}\right)\end{aligned}$$

dove abbiamo posto

$$b_1 = 1 - \log\log 2 + \int_2^\infty \frac{g(t)}{t(\log t)^2}dt \tag{8}$$

□

Osservazione 2.20 *Espandendo in serie di Taylor* $\log(1-x)$*, come già visto nella dimostrazione del Teorema 2.6 otteniamo*

$$0 < \log\left(1-\frac{1}{p}\right)^{-1} - \frac{1}{p} = \sum_{n=2}^\infty \frac{1}{np^n} < \sum_{n=2}^\infty \frac{1}{p^n} = \frac{1}{p(p-1)}.$$

Quindi la serie

$$b_2 = \sum_p \left(\log\left(1-\frac{1}{p}\right)^{-1} - \frac{1}{p}\right) = \sum_p \sum_{k=2}^\infty \frac{1}{kp^k} \tag{9}$$

converge.

Lemma 2.21 *Siano* b_1 *e* b_2 *le costanti definite in* (8) e (9), e γ la costante di Eulero. Allora

$$b_1 + b_2 = \gamma.$$

Dimostrazione: Similmente alla dimostrazione del Teorema 2.6, prendiamo $0 < \sigma < 1$ e definiamo

$$F(\sigma) = \log\zeta(1+\sigma) - \sum_p \frac{1}{p^{1+\sigma}} = \sum_p \sum_{n=2}^\infty \frac{1}{np^{n(1+\sigma)}}.$$

Come già osservato, $F(\sigma)$ converge assolutamente per $\sigma \ge 0$ e rappresenta quindi una funzione continua. Vale allora

$$\lim_{\sigma\to 0^+} F(\sigma) = b_2. \tag{10}$$

Cerchiamo quindi ora una rappresentazione differente per $F(\sigma)$. Espandendo in serie di Taylor $e^{-\sigma}$ otteniamo

$$1 - \sigma + \frac{\sigma^2}{2e} < e^{-\sigma} < 1 - \sigma + \frac{\sigma^2}{2}.$$

Ora dato che $0 < \sigma < 1$ possiamo dividere tutto per σ, poi sottrarre $1/\sigma$ e infine cambiare i segni invertendo l'ordine. In questo modo otteniamo

$$\frac{2-\sigma}{2} < \frac{1-e^{-\sigma}}{\sigma} < \frac{2e-\sigma}{2e}$$

da cui, passando ai reciproci, segue

$$1 + \frac{\sigma}{2e} < 1 + \frac{\sigma}{2e-\sigma} < \frac{\sigma}{1-e^{-\sigma}} < 1 + \frac{\sigma}{2-\sigma} < 1 + \sigma.$$

Abbiamo quindi

$$0 < \log\sigma + \log(1-e^{-\sigma})^{-1} = \log\left(\frac{\sigma}{1-e^{-\sigma}}\right) < \log(1+\sigma) < \sigma$$

da cui segue

$$\log\frac{1}{\sigma} = -\log\sigma = \log(1-e^{-\sigma})^{-1} + \mathcal{O}(\sigma).$$

Sfruttando l'equazione (2) otteniamo allora

$$\log\zeta(1+\sigma) = \log\frac{1}{\sigma} + \mathcal{O}(\sigma) = \log(1-e^{-\sigma})^{-1} + \mathcal{O}(\sigma) = \sum_{n=1}^{\infty}\frac{e^{-n\sigma}}{n} + \mathcal{O}(\sigma).$$

Poniamo ora $L(x) = \sum_{n\leq x}\frac{1}{n}$. Grazie al Teorema 1.8, per $x \geq 1$

$$L(x) = \log x + \gamma + \mathcal{O}\left(\frac{1}{x}\right).$$

Poniamo quindi $f(x) = e^{-\sigma x}$. Grazie al Teorema 1.7 otteniamo

$$\log\zeta(1+\sigma) = \sum_{n=1}^{\infty}\frac{f(n)}{n} + \mathcal{O}(\sigma) = \int_0^{\infty} f(x)dL(x) + \mathcal{O}(\sigma) =$$
$$= -\int_0^{\infty} L(x)df(x) + \mathcal{O}(\sigma) = \sigma\int_0^{\infty} e^{-\sigma x}L(x)dx + \mathcal{O}(\sigma).$$

Grazie al Teorema 2.19

$$S(x) = \sum_{p\leq x}\frac{1}{p} = \log\log x + b_1 + \mathcal{O}\left(\frac{1}{\log x}\right)$$

per $x \geq 2$. Poniamo allora $g(x) = x^{-\sigma}$, e applicando nuovamente il Teorema 1.7 otteniamo

$$\sum_p \frac{1}{p^{1+\sigma}} = \sum_p \frac{g(p)}{p} = \int_1^{\infty} g(x)dS(x) = -\int_1^{\infty} S(x)dg(x) =$$
$$= \sigma\int_1^{\infty}\frac{S(x)dx}{x^{1+\sigma}} = \sigma\int_0^{\infty} e^{-\sigma x}S(e^x)dx$$

Ma

$$S(e^x) = \log x + b_1 + \mathcal{O}\left(\frac{1}{x}\right)$$

e come visto prima

$$L(x) = \log x + \gamma + \mathcal{O}\left(\frac{1}{x}\right),$$

quindi

$$L(x) - S(e^x) = \gamma - b_1 + \mathcal{O}\left(\frac{1}{x}\right) = \gamma - b_1 + \mathcal{O}\left(\frac{1}{x+1}\right)$$

per $x \geq 1$. Ovviamente lo stesso risultato in questa versione vale anche per $0 \leq x \leq 1$. Segue allora

$$F(\sigma) = \log\zeta(1+\sigma) - \sum_p\frac{1}{p^{1+\sigma}} = \sigma\int_0^{\infty} e^{-\sigma x}(L(x) - S(e^x))dx + \mathcal{O}(\sigma) =$$
$$\sigma\int_0^{\infty} e^{-\sigma x}\left(\gamma - b_1 + \mathcal{O}\left(\frac{1}{x+1}\right)\right)dx + \mathcal{O}(\sigma) =$$
$$(\gamma - b_1)\sigma\int_0^{\infty} e^{-\sigma x}dx + \mathcal{O}\left(\sigma\int_0^{\infty}\frac{e^{-\sigma x}dx}{x+1}\right) + \mathcal{O}(\sigma) =$$
$$\gamma - b_1 + \mathcal{O}\left(\sigma\int_0^{\infty}\frac{e^{-\sigma x}dx}{x+1}\right) + \mathcal{O}(\sigma).$$

Valutiamo ora l'integrale

$$\int_0^{\infty}\frac{e^{-\sigma x}dx}{x+1} < \int_0^{1/\sigma}\frac{e^{-\sigma x}dx}{x+1} + \int_{1/\sigma}^{\infty}\frac{e^{-\sigma x}dx}{x} <$$
$$\int_0^{1/\sigma}\frac{dx}{x+1} + \int_1^{\infty}\frac{e^{-y}dy}{y} = \log\left(\frac{1}{\sigma}+1\right) + \mathcal{O}(1).$$

Segue che

$$F(\sigma) = \gamma - b_1 + \mathcal{O}\left(\sigma \log\left(\frac{1}{\sigma} + 1\right)\right).$$

Grazie alla (10) abbiamo allora

$$b_2 = \lim_{\sigma \to 0^+} F(\sigma) = \gamma + b_1.$$

□

Teorema 2.22 (Formula di Mertens) *Per $x \geq 2$*

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = e^{\gamma} \log x + \mathcal{O}(1).$$

Dimostrazione: Osserviamo anzitutto che

$$\sum_{p>x} \sum_{k=2}^{\infty} \frac{1}{kp^k} = \sum_{p>x} \frac{1}{p} \sum_{k=1}^{\infty} \frac{1}{(k+1)p^k} < \sum_{p>x} \frac{1}{p} \sum_{k=1}^{\infty} \frac{1}{p^k}$$

e dato che

$$\sum_{k=1}^{\infty} \frac{1}{p^k} = \frac{1}{1 - 1/p} - 1 = \frac{p}{p-1} - 1 = \frac{1}{p-1}$$

abbiamo

$$\sum_{p>x} \frac{1}{p} \sum_{k=1}^{\infty} \frac{1}{p^k} = \sum_{p>x} \frac{1}{p(p-1)} < \sum_{n>x} \frac{1}{n(n-1)} =$$
$$= \sum_{n>x} \left(\frac{1}{n-1} - \frac{1}{n}\right) = \mathcal{O}\left(\frac{1}{x}\right) = \mathcal{O}\left(\frac{1}{\log x}\right).$$

Inoltre per t in un intervallo limitato vale $e^t = 1 + \mathcal{O}(t)$. Dato che $1/\log x$ è limitato per $x \geq 2$, possiamo scrivere

$$\exp\left(\mathcal{O}\left(\frac{1}{\log x}\right)\right) = 1 + \mathcal{O}\left(\frac{1}{\log x}\right).$$

Ricordando l'Osservazione 2.20 abbiamo quindi

$$\log \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = \sum_{p \leq x} \log\left(1 - \frac{1}{p}\right)^{-1} = \sum_{p \leq x} \left(\frac{1}{p} + \sum_{k=2}^{\infty} \frac{1}{kp^k}\right).$$

Applicando il Teorema 2.19 al primo termine e ricordando la definizione di b_2 data in (9) abbiamo

$$\sum_{p \leq x} \left(\frac{1}{p} + \sum_{k=2}^{\infty} \frac{1}{kp^k}\right) = \log\log x + b_1 + \mathcal{O}\left(\frac{1}{\log x}\right) + b_2 - \sum_{p>x} \sum_{k=2}^{\infty} \frac{1}{kp^k} = \log\log x + \gamma + \mathcal{O}\left(\frac{1}{\log x}\right)$$

dove nell'ultimo passaggio abbiamo usato il fatto che $b_1 + b_2 = \gamma$ per il Lemma 2.21 e quanto osservato in precedenza sull'ultima somma. Passando all'esponenziale abbiamo quindi

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = e^{\gamma} \log x \exp\left(\mathcal{O}\frac{1}{\log x}\right) = e^{\gamma} \log x \left(1 + \mathcal{O}\left(\frac{1}{\log x}\right)\right) = e^{\gamma} \log x + \mathcal{O}(1)$$

per la seconda osservazione preliminare. □

3 I crivelli

3.1 Metodo di Brun

Lemma 3.1 *Per $l \geq 1$ e $0 \leq m \leq l$ vale*

$$\sum_{k=0}^{m}(-1)^k\binom{l}{k} = (-1)^m\binom{l-1}{m}.$$

Dimostrazione: Se $m = 0, 1$ l'identità vale per verifica diretta. Procedendo per induzione

$$\sum_{k=0}^{m}(-1)^k\binom{l}{k} = \sum_{k=0}^{m-1}(-1)^k\binom{l}{k} + (-1)^m\binom{l}{m} = (-1)^{m-1}\binom{l-1}{m-1} + (-1)^m\binom{l}{m} =$$
$$= (-1)^m\left(\binom{l}{m} - \binom{l-1}{m-1}\right) = (-1)^m\binom{l-1}{m}$$

per la nota corrispondenza tra i coefficienti binomiali e il Triangolo di Pascal. □

Teorema 3.2 (Crivello di Brun) *Sia X un insieme di N elementi, $P_1, \ldots, P_r$ proprietà degli elementi di X, N_0 il numero di elementi di X che non godono di nessuna delle proprietà P_i. Per ogni $I = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, r\}$ indichiamo con $N(I) = N(i_1, \ldots, i_k)$ il numero di elementi che godono di ognuna delle proprietà $P_{i_1}, \ldots, P_{i_k}$ (in particolare $N(\emptyset) = |X| = N$). Allora*

$$N_0 \leq \sum_{k=0}^{m}(-1)^k \sum_{|I|=k} N(I)$$

se m è pari e

$$N_0 \geq \sum_{k=0}^{m}(-1)^k \sum_{|I|=k} N(I)$$

se m è dispari.

Dimostrazione: Per ogni elemento di X, date le sue proprietà, contiamo quante volte contribuisce ad ogni lato della sua disuguaglianza. Supponiamo che x abbia esattamente l proprietà. Se $l = 0$ x è contato una volta in N_0 e una volta in $N(\emptyset)$, mentre non compare in nessuno degli $N(I)$ con $I \neq \emptyset$, non alterando la disuguaglianza. Possiamo quindi supporre $l \geq 1$. In questo caso x non è considerato in N_0. Rinumerando le proprietà, possiamo supporre che x goda di $P_1, \ldots, P_l$. Prendiamo allora un insieme I. Se $i \in I$ per $i > l$ x non viene contato in $N(I)$, quindi consideriamo solo $I \subseteq \{1, \ldots, l\}$. Per ogni $k = 0, \ldots, l$ ci sono $\binom{l}{k}$ sottoinsiemi di $\{1, \ldots, l\}$ di cardinalità k. Se $m \geq l$, il contributo di x vale

$$\sum_{k=0}^{l}(-1)^k\binom{l}{k} = (1-1)^l = 0.$$

Se invece $m < l$, grazie al Lemma 3.1, tale contributo vale

$$\sum_{k=0}^{m}(-1)^k\binom{l}{k} = (-1)^m\binom{l-1}{m}$$

che è positivo se m è pari e negativo se m è dispari. □

Lemma 3.3 *Per $x \geq 1$, per ogni classe di congruenza a (modulo m)*

$$\#\{n \leq x,\ n \equiv a\ (mod\ m)\} = \frac{x}{m} + \theta$$

con $|\theta| < 1$.

Dimostrazione: Se $x/m = q \in \mathbb{Z}$ l'insieme $\{1, \ldots, qm = x\}$ contiene esattamente x/m elementi per ogni classe di congruenza modulo m. Prendiamo allora $[x] = qm + r$, con $0 \leq r < m$. Allora

$$qm < x = qm + r + \{x\} \leq qm + (m-1) + \{x\} < (q+1)m,$$

sfruttando $r < m$ e $\{x\} < 1$. Dividendo per m otteniamo $q < x/m < q + 1$. Possiamo allora dividere gli interi da 1 a x in $q+1$ insiemi disgiunti tali che q contengano tutte le classi di congruenza modulo m, mentre l'ultimo sia incompleto. In questo modo fissato un a la sua classe avrà o q o $q+1$ rappresentanti, e il lemma segue dall'ultima disuguaglianza. □

Lemma 3.4 *Sia $x \geq 1$ e $p_{i_1}, \ldots, p_{i_k}$ primi distinti $\neq 2$. Sia $N(i_1, \ldots, i_k)$ il numero di $n \leq x$ tali che*

$$n(n+2) \equiv 0 \ (mod\ p_{i_1} \cdots p_{i_k})$$

. Allora

$$N(i_1, \ldots, i_k) = \frac{2^k x}{p_{i_1} \cdots p_{i_k}} + 2^k \theta$$

con $|\theta| < 1$.

Dimostrazione: Se p è un primo dispari (quindi ≥ 3) e $n(n+2) \equiv 0 \pmod p$ vale $n \equiv 0$ oppure $n \equiv -2 \pmod p$. Inoltre $0 \neq -2 \pmod p$. L'ipotesi è quindi soddisfatta per gli n tali che

$$\begin{cases} n \equiv u_1 \ mod\ p_1 \\ n \equiv u_2 \ mod\ p_2 \\ \vdots \\ n \equiv u_k \ mod\ p_k \end{cases}$$

con $u_i \in \{0, -2\} \forall i$. Per ognuna delle scelte possibili degli u_i, per il Teorema Cinese del Resto esiste una soluzione α, unica mod $p_1 \cdots p_k$. Questa soluzione, grazie al Lemma 3.3, ha $x/(p_1 \cdots p_k) + \theta(\alpha)$ rappresentanti $\leq x$, con $|\theta(\alpha)| < 1$. Dato che le scelte possibili sono 2^k, le soluzioni totali sono

$$N(i_1, \ldots, i_k) = \frac{2^k x}{p_{i_1} \cdots p_{i_k}} + 2^k \theta$$

con $|\theta| < 1$. □

Teorema 3.5 (Brun) *Indichiamo con $\pi_2(x)$ il numero di primi $p \leq x$ tali che anche $p+2$ è primo. Allora*

$$\pi_2(x) \ll \frac{x(\log\log x)^2}{(\log x)^2}.$$

Dimostrazione: Prendiamo $5 \leq y < x$ e $r = \pi(y) - 1$, il numero di primi dispari non maggiori di y. Indichiamo questi primi con $p_1, \ldots, p_r$, e $\pi_2(x, y)$ il numero di primi $y < p \leq x$ tali che $p+2$ sia anch'esso primo. Ognuno di questi p sarà maggiore di tutti i p_i e inoltre

$$p(p+2) \not\equiv 0 \ (mod\ p_i)$$

per ogni i. Indichiamo con $N_0(y, x)$ il numero degli interi positivi $n \leq x$ che soddisfano quest'ultima proprietà. Allora avremo

$$\pi_2(x) \leq y + \pi_2(y, x) \leq y + N_0(y, x).$$

Sia X l'insieme degli interi positivi $\leq x$. Per ogni primo dispari $p_i \leq y$ indichiamo con P_i la proprietà che $n(n+2)$ sia divisibile per p_i. $N_0(y, x)$ sarà allora il numero degli $n \in X$ che non godono di nessuna delle proprietà P_i. Per ogni $I = \{i_1, \ldots, i_k\} \subseteq \{1, ..., r\}$ indichiamo con $N(I)$ il numero di interi $n \in X$ che godono di P_{i_j} per ogni $i_j \in I$, o equivalentemente tali che $n(n+2)$ sia divisibile per ogni p_{i_j}. Grazie al lemma 3.4

$$N(I) = N(i_1, \ldots, i_k) = \frac{2^k x}{p_{i_1} \cdots p_{i_k}} + 2^k \theta$$

Sia allora m un intero pari $1 \leq m \leq r$. Grazie al Teorema 3.2 abbiamo

$$N_0(y, x) \leq \sum_{k=0}^{m} (-1)^k \sum_{|I|=k} N(I) \leq \sum_{k=0}^{m} (-1)^k \sum_{\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, r\}} \left(\frac{2^k x}{p_{i_1} \cdots p_{i_k}} + \mathcal{O}(2^k) \right) \leq$$

$$\leq x \sum_{k=0}^{m} \sum_{\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, r\}} \frac{(-2)^k}{p_{i_1} \cdots p_{i_k}} + \sum_{k=0}^{m} (-1)^k \binom{r}{k} \mathcal{O}(2^k) \leq$$

$$\leq \overset{(A)}{x \sum_{k=0}^{r} \sum_{\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, r\}} \frac{(-2)^k}{p_{i_1} \cdots p_{i_k}}} - \overset{(B)}{x \sum_{k=m+1}^{r} \sum_{\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, r\}} \frac{(-2)^k}{p_{i_1} \cdots p_{i_k}}} + \overset{(C)}{\mathcal{O}\left(\sum_{k=0}^{m} \binom{r}{k} 2^k \right)}$$

Valutiamo il termine (A). Osservando che i termini della sommatoria hanno come denominatore tutti i possibili prodotti dei primi dispari $\leq y$, e come numeratore $x(-2)^k$ dove k è il numero di primi coinvolti, possiamo riscrivere tutto come

$$x\sum_{k=0}^{r}\sum_{\{i_1,\dots,i_k\}\subseteq\{1,\dots,r\}}\frac{(-2)^k}{p_{i_1}\cdots p_{i_k}} = x\prod_{2<p\leq y}\left(1-\frac{2}{p}\right) < x\prod_{2<p\leq y}\left(1-\frac{1}{p}\right)^2 \ll \frac{x}{(\log y)^2},$$

utilizzando nell'ultimo passaggio il Teorema 2.22.
Stimiamo ora il termine (B). Sia $s_k(x_1,...,x_r)$ il polinomio simmetrico elementare di grado k in r variabili. Abbiamo

$$s_k(x_1,...,x_r) = \sum_{\{i_1,\dots,i_k\}\subseteq\{1,\dots,r\}} x_{i_1}\cdots x_{i_k} \leq \frac{(x_1+\cdots x_r)^k}{k!}$$

come si può vedere per induzione su k ($s_{n-1}s_1 = ns_n + R$, dove R sono prodotti con termini ripetuti, certamente positivi dato che tutti gli x_i sono positivi in questo caso). Ma

$$\frac{(x_1+\cdots+x_r)^k}{k!} = \frac{(s_1(x_1,...,x_r))^k}{k!} < \left(\frac{e}{k}\right)^k s_1(x_1,...,x_r)^k$$

grazie al Teorema 1.6. Tornando a (B) abbiamo

$$\left|x\sum_{k=m+1}^{r}\sum_{\{i_1,\dots,i_k\}\subseteq\{1,\dots,r\}}\frac{(-2)^k}{p_{i_1}\cdots p_{i_k}}\right| \leq x\sum_{k=m+1}^{r}\sum_{\{i_1,\dots,i_k\}\subseteq\{1,\dots,r\}}\frac{2^k}{p_{i_1}\cdots p_{i_k}} =$$
$$= x\sum_{k=m+1}^{r}\sum_{\{i_1,\dots,i_k\}\subseteq\{1,\dots,r\}}\left(\frac{2}{p_{i_1}}\right)\cdots\left(\frac{2}{p_{i_k}}\right) = x\sum_{k=m+1}^{r}s_k\left(\frac{2}{p_1},\cdots,\frac{2}{p_r}\right) <$$
$$< x\sum_{k=m+1}^{r}\left(\frac{e}{k}\right)^k s_1\left(\frac{2}{p_1},\cdots,\frac{2}{p_r}\right)^k$$

grazie all'osservazione precedente. Ma

$$x\sum_{k=m+1}^{r}\left(\frac{e}{k}\right)^k s_1\left(\frac{2}{p_1},\cdots,\frac{2}{p_r}\right)^k = x\sum_{k=m+1}^{r}\left(\frac{e}{k}\right)^k\left(\frac{2}{p_1}+\cdots+\frac{2}{p_r}\right)^k =$$
$$= x\sum_{k=m+1}^{r}\left(\frac{2e}{k}\right)^k\left(\sum_{p\leq y}\frac{1}{p}\right)^k < x\sum_{k=m+1}^{r}\left(\frac{2e}{m}\right)^k\left(\sum_{p\leq y}\frac{1}{p}\right)^k < x\sum_{k=m+1}^{r}\left(\frac{c\log\log y}{m}\right)^k$$

dove c è una costante assoluta per il Teorema 2.19. Se riusciamo a scegliere m in modo che

$$m > 2c\log\log y$$

otteniamo

$$x\sum_{k=m+1}^{r}\left(\frac{c\log\log y}{m}\right)^k \leq x\sum_{k=m+1}^{r}\frac{1}{2^k} < \frac{x}{2^m}.$$

Stimiamo infine (C). Osserviamo che, per espansione del binomiale, vale $\binom{r}{k} < r^k$. Inoltre, dato che r è il numero di primi dispari $\leq y$, $2r \leq y$, e quindi

$$\sum_{k=0}^{m}\binom{r}{k}2^k < \sum_{k=0}^{m}(2r)^k \ll (2r)^m \leq y^m.$$

Sostituendo le tre stime ottenute risulta

$$\pi_2(x) \ll y + \frac{x}{(\log y)^2} + \frac{x}{2^m} + y^m \ll \frac{x}{(\log y)^2} + \frac{x}{2^m} + y^m$$

dove la costante è assoluta, $5 \leq y < x$ e $m > 2c\log\log y$. Poniamo allora $c' = \max\{2c, (\log 2)^{-1}\}$,

$$y = \exp\left(\frac{\log x}{3c'\log\log x}\right) = x^{\frac{1}{3c'\log\log x}}$$

e $m = 2[c' \log\log x]$. Per x sufficientemente grande y e m soddisfano le due condizioni imposte. Inoltre il Teorema 2.12 ci assicura che m cresca più lentamente di r. Sostituendo allora questi valori di m e y otteniamo

$$\frac{x}{(\log y)^2} \ll \frac{x(\log\log x)^2}{(\log x)^2}.$$

Inoltre, dato che $c' \geq (\log 2)^{-1}$,

$$\frac{x}{2^m} = \frac{x}{2^{2c' \log\log x}} = \frac{x}{e^{2c' \log\log x \log 2}} = \frac{x}{(\log x)^{2c' \log 2}} \leq \frac{x}{(\log x)^2}.$$

Infine

$$y^m \leq y^{2c' \log\log x} = \exp\left(\frac{2c' \log\log x \log x}{3c' \log\log x}\right) = x^{2/3}.$$

Combinando le stime ottenute otteniamo

$$\pi_2(x) \ll \frac{x(\log\log x)^2}{(\log x)^2}$$

□

Teorema 3.6 (Primi Gemelli) *Sia $p_1, p_2, \ldots$ la sequenza dei numeri primi p tali che $p+2$ è primo. Allora la somma*

$$\sum_{n=1}^{\infty} \left(\frac{1}{p_n} + \frac{1}{p_n + 2}\right),$$

ovvero la somma dei reciproci dei primi gemelli, converge.

Dimostrazione: Dato che per la gerarchia degli infiniti $(\log\log x)^2 \ll \sqrt{\log x}$, dal Teorema 3.5 otteniamo

$$\pi_2(x) \ll \frac{x}{(\log x)^{3/2}}$$

per tutti gli $x \geq 2$. Allora

$$n = \pi_2(p_n) \ll \frac{p_n}{(\log p_n)^{3/2}} \leq \frac{p_n}{(\log n)^{3/2}}$$

e quindi

$$\frac{1}{p_n} \ll \frac{1}{n(\log n)^{3/2}},$$

per $n \geq 2$. Di conseguenza la serie

$$\frac{1}{2}\left(\sum_{n=1}^{\infty}\left(\frac{1}{p_n} + \frac{1}{p_n+2}\right)\right) \leq \sum_{n=1}^{\infty}\frac{1}{p_n} = \frac{1}{3} + \sum_{n=2}^{\infty}\frac{1}{p_n} \ll \frac{1}{3} + \sum_{n=2}^{\infty}\frac{1}{n(\log n)^{3/2}}$$

converge, da cui la tesi. □

Osservazione 3.7 *Il Teorema 3.6 non ci permette di stabilire se esistano o meno infiniti primi gemelli, problema ad oggi ancora aperto.*

3.2 Metodo di Selberg

Lemma 3.8 *Siano $a_1, ..., a_n$ numeri reali positivi e $b_1, ..., b_n$ reali. Il minimo della forma quadratica*

$$Q(y_1, ..., y_n) = a_1 y_1^2 + \cdots + a_n y_n^2$$

vincolata da

$$b_1 y_1 + \cdots + b_n y_n = 1 \tag{11}$$

vale

$$m = \left(\sum_{i=1}^{n} \frac{b_i^2}{a_i}\right)^{-1}$$

ed è ottenuto se e solo se

$$y_i = \frac{m b_i}{a_i}$$

per ogni i.

Dimostrazione: Siano $y_1, ..., y_n$ numeri reali che rispettano il vincolo (11). Allora per la disuguaglianza di Cauchy-Schwartz abbiamo

$$1 = \left(\sum_{i=1}^{n} b_i y_i\right)^2 = \left(\sum_{i=1}^{n} \left(\frac{b_i}{\sqrt{a_i}}\right)\sqrt{a_i} y_i\right)^2 \leq \left(\sum_{i=1}^{n} \frac{b_i^2}{a_i}\right)\left(\sum_{i=1}^{n} a_i y_i^2\right).$$

da cui

$$\sum_{i=1}^{n} a_i y_i^2 \geq \left(\sum_{i=1}^{n} \frac{b_i^2}{a_i}\right)^{-1} = m.$$

Inoltre, sempre per Cauchy-Schwartz, il minimo è assunto (ovvero $\sum_{i=1}^{n} a_i y_i^2 = m$) se e solo se i due vettori sono paralleli, ovvero se esiste t tale che, per ogni i,

$$\sqrt{a_i} y_i = \frac{t b_i}{\sqrt{a_i}}$$

o equivalentemente

$$y_i = \frac{t b_i}{a_i}.$$

Questo implica

$$1 = \sum_{i=1}^{n} b_i y_i = t \sum_{i=1}^{n} \frac{b_i^2}{a_i} = \frac{t}{m}$$

ovvero $t = m$ e quindi $y_i = m b_i / a_i$. Viceversa, se $y_i = m b_i / a_i$ per ogni i, allora $\sum_{i=1}^{n} b_i y_i = 1$ e

$$Q(y_1, ..., y_n) = \sum_{i=1}^{n} a_i \left(\frac{m b_i}{a_i}\right)^2 = m^2 \sum_{i=1}^{n} \frac{b_i^2}{a_i} = m^2 \frac{1}{m} = m.$$

□

Lemma 3.9 *Indichiamo con $\omega(n)$ il numero di divisori primi distinti di n. Per ogni intero square-free d esistono esattamente $3^{\omega(d)}$ coppie di interi positivi d_1, d_2 tali che $[d_1, d_2] = d$.*

Dimostrazione: Possiamo scrivere $d = \prod_{i=1}^{\omega(d)} p_i$. Allora per ogni coppia d_1, d_2 tale che $[d_1, d_2] = d$ e per ogni p_i nella decomposizione di d si possono verificare tre casi: o $p_i | d_1$, o $p_i | d_2$ oppure li divide entrambi. Dato che i p_i sono $\omega(d)$, le coppie possibili sono $3^{\omega(d)}$. □

Teorema 3.10 (Crivello di Selberg) *Sia A una sequenza finita di interi, e indichiamo con $|A|$ il numero dei suoi termini. Sia inoltre $\mathcal{P}$ un insieme di primi. Per ogni numero reale $z \geq 2$ sia*

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

Con $S(A, \mathcal{P}, z)$ indichiamo il numero di termini di A non divisibili per alcun primo $p \in \mathcal{P}$, $p < z$. Per ogni intero positivo square-free (nel senso della Definizione 1.18) d, indichiamo con $|A_d|$ il numero di termini di A divisibili per d. Sia $g(k)$ una funzione moltiplicativa tale che $0 < g(p) < 1$ per ogni $p \in \mathcal{P}$. Allora esiste $g_1(m)$ totalmente moltiplicativa tale che $g_1(p) = g(p)$ per ogni $p \in \mathcal{P}$. Definiamo

$$r(d) = |A_d| - g(d)|A|$$

e

$$G(z) = \sum_{\substack{m<z \\ p|m \Rightarrow p \in \mathcal{P}}} g_1(m).$$

Allora

$$S(A, \mathcal{P}, z) \leq \frac{|A|}{G(z)} + \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)} |r(d)|.$$

Dimostrazione: Dato che g è moltiplicativa abbiamo, grazie al Teorema 1.11,

$$g([d_1,d_2])g((d_1,d_2)) = g(d_1)g(d_2).$$

Prendiamo $z \geq 2$. Per ogni d divisore di $P(z)$ (ovvero d prodotto di primi in $\mathcal{P}$ minori di z con esponente 1) scegliamo $\lambda(d) \in \mathbb{R}$, con le sole condizioni che $\lambda(1) = 1$ e $\lambda(d) = 0$ se $d \geq z$. Osserviamo che la quantità

$$\left(\sum_{d|(a,P(z))} \lambda(d)\right)^2$$

è certamente non negativa, e vale 1 se $(a, P(z)) = 1$. Allora

$$S(A,\mathcal{P},z) = \sum_{\substack{a\in A\\(a,P(z))=1}} 1 \leq \sum_{a\in A}\left(\sum_{d|(a,P(z))}\lambda(d)\right)^2 = \sum_{a\in A}\sum_{d_1|(a,P(z))}\sum_{d_2|(a,P(z))}\lambda(d_1)\lambda(d_2).$$

Ricordando che $d|(a,b)$ se e solo se $d|a$ e $d|b$, e analogamente $a|c$ e $b|c$ se e solo se $[a,b]|c$, possiamo riordinare le somme ottenendo

$$\sum_{a\in A}\sum_{d_1|(a,P(z))}\sum_{d_2|(a,P(z))}\lambda(d_1)\lambda(d_2) = \sum_{d_1,d_2|P(z)}\lambda(d_1)\lambda(d_2)\sum_{\substack{a\in A\\[d_1,d_2]|a}} 1 =$$

$$\sum_{d_1,d_2|P(z)}\lambda(d_1)\lambda(d_2)|A_{[d_1,d_2]}| = \sum_{d_1,d_2|P(z)}\lambda(d_1)\lambda(d_2)(g([d_1,d_2])|A| + r([d_1,d_2])).$$

Notiamo infatti che, avendo preso d_1 e d_2 tra i divisori di $P(z)$, che è prodotto di primi distinti, essi saranno entrambi square-free, e di conseguenza lo sarà anche $[d_1,d_2]$. Riordinando i termini e ricordando che $\lambda(d) = 0$ se $d \geq z$ abbiamo

$$\sum_{d_1,d_2|P(z)}\lambda(d_1)\lambda(d_2)(g([d_1,d_2])|A| + r([d_1,d_2])) =$$

$$|A|\sum_{d_1,d_2|P(z)} g([d_1,d_2])\lambda(d_1)\lambda(d_2) + \sum_{d_1,d_2|P(z)}\lambda(d_1)\lambda(d_2)r([d_1,d_2]) =$$

$$|A|\sum_{\substack{d_1,d_2|P(z)\\d_1,d_2<z}}\frac{g(d_1)g(d_2)}{g((d_1,d_2))}\lambda(d_1)\lambda(d_2) + \sum_{\substack{d_1,d_2|P(z)\\d_1,d_2<z}}\lambda(d_1)\lambda(d_2)r([d_1,d_2]).$$

Mettendo insieme i risultati ottenuti abbiamo

$$S(A,\mathcal{P},z) = |A|Q + R$$

dove

$$Q = \sum_{\substack{d_1,d_2|P(z)\\d_1,d_2<z}}\frac{1}{g((d_1,d_2))}g(d_1)\lambda(d_1)g(d_2)\lambda(d_2)$$

e

$$R = \sum_{\substack{d_1,d_2|P(z)\\d_1,d_2<z}}\lambda(d_1)\lambda(d_2)r([d_1,d_2]).$$

Sia ora

$$\mathcal{D} = \{k|P(z), 1 \leq k < z\}$$

l'insieme dei divisori di $P(z)$ minori di z. Notiamo che $\mathcal{D}$ è composto da interi square-free (dato che lo è $P(z)$) e chiuso per divisori. Per le ipotesi su g, se $k \in \mathcal{D}$ allora $0 < g(k) \leq 1$. Definiamo su $\mathcal{D}$ una funzione

$$f(k) = \sum_{d|k}\frac{\mu(d)}{g(k/d)} = \frac{1}{g(k)}\sum_{d|k}\mu(d)g(d) = \frac{1}{g(k)}\prod_{p|k}(1-g(p)) \tag{12}$$

grazie al Teorema 1.21. f è positiva e moltiplicativa su $\mathcal{D}$. Possiamo quindi applicare il Teorema 1.25 per ottenere

$$\frac{1}{g(k)} = \sum_{d|k} f(d). \tag{13}$$

Abbiamo quindi

$$Q = \sum_{d_1,d_2\in\mathcal{D}} \frac{1}{g((d_1,d_2))} g(d_1)\lambda(d_1)g(d_2)\lambda(d_2) =$$
$$= \sum_{d_1,d_2\in\mathcal{D}} \sum_{k|(d_1,d_2)} f(k)g(d_1)\lambda(d_1)g(d_2)\lambda(d_2) =$$
$$= \sum_{k\in\mathcal{D}} f(k) \sum_{\substack{d_1,d_2\in\mathcal{D}\\ k|d_1,k|d_2}} g(d_1)\lambda(d_1)g(d_2)\lambda(d_2).$$

grazie al fatto che $\mathcal{D}$ è chiuso per divisori. Riscrivendo il prodotto otteniamo

$$\sum_{k\in\mathcal{D}} f(k) \sum_{\substack{d_1,d_2\in\mathcal{D}\\ k|d_1,k|d_2}} g(d_1)\lambda(d_1)g(d_2)\lambda(d_2) =$$
$$= \sum_{k\in\mathcal{D}} f(k) \left(\sum_{\substack{d\in\mathcal{D}\\ k|d}} g(d)\lambda(d) \right)^2 = \sum_{k\in\mathcal{D}} f(k) y_k^2,$$

dove

$$y_k = \sum_{\substack{d\in\mathcal{D}\\ k|d}} g(d)\lambda(d).$$

Quindi fissato z Q è una forma quadratica nelle y_k. Applicando il Teorema 1.26 otteniamo

$$g(d)\lambda(d) = \sum_{\substack{k\in\mathcal{D}\\ d|k}} \mu\left(\frac{k}{d}\right) y_k = \mu(d) \sum_{\substack{k\in\mathcal{D}\\ d|k}} \mu(k) y_k. \tag{14}$$

Per $d = 1$ otteniamo il vincolo $\sum_{k\in\mathcal{D}} \mu(k)y_k = 1$. Applicando allora il Lemma 3.8 con $a_i = f(k)$ e $b_i = \mu(k)$, e posto

$$F(z) = \sum_{k\in\mathcal{D}} \frac{1}{f(k)}$$

vediamo che il minimo della forma quadratica Q vale

$$\left(\sum_{k\in\mathcal{D}} \frac{\mu(k)^2}{f(k)} \right)^{-1} = \left(\sum_{k\in\mathcal{D}} \frac{1}{f(k)} \right)^{-1} = \frac{1}{F(z)}$$

ed è ottenuto per

$$y_k = \frac{\mu(k)}{F(z)f(k)}.$$

Inserendo questi valori dentro (14) ricaviamo

$$\lambda(d) = \frac{\mu(d)}{g(d)} \sum_{\substack{k\in\mathcal{D}\\ d|k}} \mu(k)y_k = \frac{\mu(d)}{g(d)} \sum_{\substack{dl<z\\ dl|P(z)}} \mu(dl)y_{dl} = \frac{\mu(d)}{g(d)} \sum_{\substack{l<z/d\\ dl|P(z)}} \mu(dl) \left(\frac{\mu(dl)}{F(z)f(dl)} \right),$$

dove abbiamo semplicemente sostituito $k = dl$ sfruttando il fatto che $d|k$. Se $dl|P(z)$, essendo $P(z)$ square-free, d ed l devono essere coprimi, e quindi $f(dl) = f(d)f(l)$ per moltiplicatività di f in $\mathcal{D}$. Questo unito al fatto che $\mu(k)^2 = 1$ ci da

$$\frac{\mu(d)}{g(d)} \sum_{\substack{l<z/d\\ dl|P(z)}} \mu(dl) \left(\frac{\mu(dl)}{F(z)f(dl)} \right) = \frac{\mu(d)}{f(d)g(d)F(z)} \sum_{\substack{l<z/d\\ dl|P(z)}} \frac{1}{f(l)} = \frac{\mu(d)F_d(z)}{f(d)g(d)F(z)}$$

dove

$$F_d(z) = \sum_{\substack{l<z/d\\ dl|P(z)}} \frac{1}{f(l)}.$$

Sia ora d un divisore qualsiasi di $P(z)$. Raggruppando gli elementi k di $\mathcal{D}$ in base al valore di (k,d) otteniamo

$$F(z) = \sum_{k\in\mathcal{D}} \frac{1}{f(k)} = \sum_{l|d} \sum_{\substack{k\in\mathcal{D}\\(k,d)=l}} \frac{1}{f(k)} = \sum_{l|d} \sum_{\substack{lm<z\\lm|P(z)\\(lm,d)=l}} \frac{1}{f(lm)}$$

rinominando $k = lm$ dato che per definizione $l = (k,d)|k$. Inoltre, sfruttando di nuovo il fatto che se $lm|P(z)$ allora l ed m sono coprimi,

$$\sum_{l|d} \sum_{\substack{lm<z\\lm|P(z)\\(lm,d)=l}} \frac{1}{f(lm)} = \sum_{l|d} \frac{1}{f(l)} \sum_{\substack{m<z/l\\lm|P(z)\\(m,d/l)=1}} \frac{1}{f(m)} = \sum_{l|d} \frac{1}{f(l)} \sum_{\substack{m<z/l\\m|P(z)\\(m,d)=1}} \frac{1}{f(m)}.$$

Infatti se $lm|P(z)$ a maggior ragione $m|P(z)$, e da $(m,d/l)=1$ segue $(m,d)=1$ dal momento che m e l sono coprimi come visto sopra. Viceversa se $(m,d)=1$ anche $(m,d/l)=1$, e dato che $m|P(z)$, $l|d|P(z)$, e ancora m,l coprimi anche $ml|P(z)$. Le due condizioni sono quindi equivalenti. Applicando al contrario l'argomento sulla divisione di $P(z)$ a d ed m

$$\sum_{l|d} \frac{1}{f(l)} \sum_{\substack{m<z/l\\m|P(z)\\(m,d)=1}} \frac{1}{f(m)} = \sum_{l|d} \frac{1}{f(l)} \sum_{\substack{m<z/l\\dm|P(z)}} \frac{1}{f(m)} \geq \sum_{l|d} \frac{1}{f(l)} \sum_{\substack{m<z/d\\dm|P(z)}} \frac{1}{f(m)} =$$

$$F_d(z) \sum_{l|d} \frac{1}{f(l)} = \frac{F_d(z)}{f(d)} \sum_{l|d} f\left(\frac{d}{l}\right) = \frac{F_d(z)}{f(d)} \sum_{l|d} f(l) = \frac{F_d(z)}{f(d)g(d)}$$

dove gli ultimi tre passaggi sono giustificati prima da $f(d/l)f(l) = f(d)$ per d square-free, poi dal fatto che sommando d/l su tutti gli l divisori di d si ottengono esattamente i divisori l (in ordine opposto), e infine dall'espressione di g ricavata in (13). Risulta quindi

$$F(z) \geq \frac{F_d(z)}{f(d)g(d)}$$

da cui

$$|\lambda(d)| = \frac{F_d(z)}{f(d)g(d)F(z)} \leq 1.$$

Ora

$$|R| = \left| \sum_{\substack{d_1,d_2|P(z)\\d_1,d_2<z}} \lambda(d_1)\lambda(d_2) r([d_1,d_2]) \right| \leq$$

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

Infatti, da $d_1,d_2 < z$ segue $d = [d_1,d_2] < z^2$, e da $d_1,d_2|P(z)$ segue $d|P(z)$ e quindi anche d square-free. Grazie al Lemma 3.9 sappiamo allora che esistono esattamente $3^{\omega(d)}$ coppie ordinate d_1,d_2 tali che $[d_1,d_2]=d$. Mettendo insieme la stima di minimo per Q e quella per R abbiamo quindi ottenuto

$$S(A,\mathcal{P},z) \leq \frac{|A|}{F(z)} + \sum_{\substack{d<z^2\\d|P(z)}} 3^{\omega(d)} |r(d)|.$$

Ora è sufficiente mostrare che $F(z) \geq G(z)$. Sia $g_1(k)$ una funzione totalmente moltiplicativa tale che $g_1(p) = g(p)$ per tutti i primi $p \in \mathcal{P}$. L'esistenza di g_1 è garantita dal fatto che, essendo vincolata solo sui primi, possiamo estenderla in modo totalmente moltiplicativo a tutto $\mathbb{N}$, eventualmente assegnandole prima valori arbitrari sui primi non in $\mathcal{P}$. Grazie a (12) otteniamo

$$F(z) = \sum_{k\in\mathcal{D}} \frac{1}{f(k)} = \sum_{k\in\mathcal{D}} g(k) \prod_{p|k} (1-g(p))^{-1} = \sum_{k\in\mathcal{D}} g_1(k) \prod_{p|k} (1-g_1(p))^{-1} =$$

$$= \sum_{k\in\mathcal{D}} g_1(k) \prod_{p|k} \sum_{r=0}^{\infty} g_1(p)^r = \sum_{k\in\mathcal{D}} g_1(k) \prod_{p|k} \sum_{r=0}^{\infty} g_1(p^r).$$

Notiamo che $g(k) = g_1(k)$ dal momento che k è prodotto square-free di primi $p \in \mathcal{P}$. Inoltre la convergenza della serie è garantita dall'ipotesi $g_1(p) = g(p) < 1$. Svolgendo il prodotto otteniamo la somma di tutti i prodotti di potenza qualsiasi (eventualmente 0) dei primi che dividono k, ovvero la somma sugli l tali che $p|l \Rightarrow p|k$:

$$\sum_{k\in\mathcal{D}} g_1(k) \prod_{p|k} \sum_{r=0}^{\infty} g_1(p^r) = \sum_{k\in\mathcal{D}} g_1(k) \sum_{\substack{l=1 \\ p|l\Rightarrow p|k}}^{\infty} g_1(l) = \sum_{k\in\mathcal{D}} \sum_{\substack{l=1 \\ p|l\Rightarrow p|k}}^{\infty} g_1(kl)$$

per totale moltiplicatività di g_1. Ponendo $kl = m$ la somma diventa

$$\sum_{k\in\mathcal{D}} \sum_{\substack{l=1 \\ p|l\Rightarrow p|k}}^{\infty} g_1(kl) = \sum_{k\in\mathcal{D}} \sum_{\substack{m=1 \\ k|m \\ p|(m/k)\Rightarrow p|k}}^{\infty} g_1(m) = \sum_{m=1}^{\infty} g_1(m) \left(\sum_{\substack{k\in\mathcal{D} \\ k|m \\ p|(m/k)\Rightarrow p|k}} 1 \right) \geq$$

$$\geq \sum_{\substack{m<z \\ p|m\Rightarrow p\in\mathcal{P}}} g_1(m) \left(\sum_{\substack{k\in\mathcal{D} \\ k|m \\ p|(m/k)\Rightarrow p|k}} 1 \right) \geq \sum_{\substack{m<z \\ p|m\Rightarrow p\in\mathcal{P}}} g_1(m) = G(z).$$

Nell'ultima disuguaglianza stiamo affermando che la somma interna vale sempre almeno 1 se m soddisfa le condizioni della somma esterna. Infatti possiamo sempre prendere k come il prodotto dei primi distinti che dividono m. Dato che $m < z$ avremo $k \in \mathcal{D}$, chiaramente $k|m$, e se $p|(m/k)$ allora p è un fattore primo ripetuto in m che quindi compare singolarmente anche in k, da cui $p|k$. □

3.3 Applicazioni

Come applicazioni del Teorema 3.10, ricaviamo una stima del numero di rappresentazioni di un intero come somma e come differenza di numeri primi.

Teorema 3.11 *Dato N intero pari, indichiamo con $r(N)$ il numero di rappresentazioni di N come somma di due primi. Vale*

$$r(N) \ll \frac{N}{(\log N)^2} \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

dove la costante è assoluta e non dipende da N.

Dimostrazione: Per definizione $r(N) = \#\{p \leq N,\ N - p \text{ primo}\}$. Definiamo la successione $a_n = n(N - n)$, e poniamo $A = \{a_n\}_{n=1}^{N}$. Avremo quindi $|A| = N$. Prendiamo $\mathcal{P}$ come l'insieme di tutti i primi, e $2 < z \leq \sqrt{N}$. La funzione di Seldberg $S(A, \mathcal{P}, z)$ indica il numero di termini di A non divisibili da primi $p < z$. Se $\sqrt{N} < n < N - \sqrt{N}$ e $a_n \equiv 0 \ (mod\ p)$ per qualche primo $p < z$, allora o n o $N - n$ non sono primi, e quindi n non contribuisce ad $r(N)$. Notiamo che è necessario escludere gli estremi, in quanto se $n \leq \sqrt{N}$ è primo sarà certamente divisibile per se stesso, e quindi $a_n \equiv 0 \ (mod\ n)$, rendendo impossibile distinguere i primi dai composti. Lo stesso discorso vale per il termine $N - n$ se $n \geq N - \sqrt{N}$. Abbiamo quindi la stima

$$r(N) \leq 2\sqrt{N} + S(A, \mathcal{P}, z).$$

Definiamo, nelle notazioni del Teorema 3.10,

$$g(p) = \begin{cases} 2/p \text{ se p non divide N} \\ 1/p \text{ se p divide N} \end{cases} \tag{15}$$

In questo modo g è totalmente moltiplicativa e quindi $g_1(k) = g(k)$ per ogni k. Dato che abbiamo preso N pari, $2|N$ e $g(2) = 1/2$, quindi $0 < g(p) < 1$ per ogni primo p. Notiamo anche che $a_n = n(N - n) \equiv 0 \ (mod\ p)$ se e solo se $n \equiv 0$ oppure $n \equiv N \ (mod\ p)$. Se p non divide N, $N \not\equiv 0 \ (mod\ p)$ e le due congruenze sono distinte, altrimenti coincidono. Sia ora

$$d = p_1 \cdots p_k q_1 \cdots q_l$$

un intero square-free dove i primi p_i dividono N e i primi q_j no. Allora

$$g(d) = \frac{2^l}{d}.$$

Dato che a_n è divisibile per d se e solo se è divisibile per ogni primo p che divide d, per il Teorema Cinese del Resto i q_j danno esattamente 2^l distinte classi di congruenza modulo d in cui $a_n \equiv 0 \ (mod\ d)$, mentre i p_i individuano un'unica classe. Allora, grazie al Lemma 3.3,

$$|A_d| = \#\{x \in A,\ d|x\} = 2^l \left(\frac{|A|}{d} + \theta \right) = |A|g(d) + r(d)$$

dove

$$|r(d)| = |2^l \theta| \leq 2^l \leq 2^{\omega(d)}. \tag{16}$$

Grazie al Teorema 3.10,

$$S(A, \mathcal{P}, z) \leq \frac{|A|}{G(z)} + \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)} |r(d)|,$$

dove

$$G(z) = \sum_{m<z} g(m)$$

dato che abbiamo preso $\mathcal{P}$ come l'insieme di tutti i primi. Sia ora

$$m = \prod_{i=1}^{k} p_i^{r_i} \prod_{j=1}^{l} q_j^{s_j}$$

dove i p_i dividono N e i q_j non dividono N. Gli indici e i primi coinvolti non sono però necessariamente quelli indicati in precedenza. Consentiamo inoltre agli r_i e agli s_i di valere 0. Allora

$$g(m) = \prod_{i=1}^{k} \left(\frac{1}{p_i} \right)^{r_i} \prod_{j=1}^{l} \left(\frac{2}{q_j} \right)^{s_j} = \frac{2^{s_1 + \cdots + s_l}}{m}.$$

Indichiamo ora con $d_N(m)$ il numero di divisori di m coprimi ad N. Abbiamo, grazie al Teorema 1.14,

$$d_N(m) = d\left(\prod_{j=1}^{l} q_j^{s_j} \right) = \prod_{j=1}^{l} (s_j + 1) \leq \prod_{j=1}^{l} 2^{s_j} = 2^{s_1 + \cdots s_l}.$$

Quindi $g(m) \geq d_N(m)/m$ e

$$G(z) = \sum_{m<z} g(m) \geq \sum_{m<z} \frac{d_N(m)}{m}.$$

Dato che, ripetendo il ragionamento del Teorema 1.39, si può vedere

$$\prod_{p|N} \left(1 - \frac{1}{p} \right)^{-1} = \sum_{\substack{t=1 \\ p|t \Rightarrow p|N}}^{\infty} \frac{1}{t},$$

segue che

$$\prod_{p|N} \left(1 - \frac{1}{p} \right)^{-1} G(z) \geq \sum_{m<z} \frac{d_N(m)}{m} \sum_{\substack{t=1 \\ p|t \Rightarrow p|N}}^{\infty} \frac{1}{t} = \sum_{m<z} d_N(m) \sum_{\substack{t=1 \\ p|t \Rightarrow p|N}}^{\infty} \frac{1}{mt} =$$

$$= \sum_{m<z} d_N(m) \sum_{\substack{w=1 \\ m|w \\ p|(w/m) \Rightarrow p|N}}^{\infty} \frac{1}{w} = \sum_{w=1}^{\infty} \frac{1}{w} \sum_{\substack{m<z \\ m|w \\ p|(w/m) \Rightarrow p|N}} d_N(m) \geq$$

$$\geq \sum_{w<z} \frac{1}{w} \sum_{\substack{m|w \\ p|(w/m) \Rightarrow p|N}} d_N(m).$$

Indichiamo allora, con la notazione di m (ma primi eventualmente differenti),

$$w = \prod_{i=1}^{k} p_i^{u_i} \prod_{j=1}^{l} q_j^{v_j}.$$

Dato che $m|w$, come osservato prima possiamo considerare nell'espressione di m tutti i fattori di w che non vi comparirebbero normalmente, presi con esponente 0. In questo modo abbiamo $0 \leq r_i \leq u_i$ e $0 \leq s_j \leq v_j$ per ogni i, j. Inoltre

$$\frac{w}{m} = \prod_{i=1}^{k} p_i^{u_i - r_i} \prod_{j=1}^{l} q_j^{v_j - s_j},$$

ma nella sommatoria abbiamo imposto che tutti i divisori di w/m dividano anche N, quindi $s_j = v_j$ per ogni j. Segue

$$m = \prod_{i=1}^{k} p_i^{r_i} \prod_{j=1}^{l} q_j^{v_j}.$$

e quindi

$$d_N(m) = \prod_{j=1}^{l} (v_j + 1).$$

Applicando ancora il Teorema 1.14 abbiamo che per ogni w il numero di divisori m in questa forma vale

$$\prod_{i=1}^{k} (u_i + 1).$$

Quindi per ogni $w < z$ vale

$$\sum_{\substack{m|w \\ p|(w/m) \Rightarrow p|N}} d_N(m) = \sum_{\substack{m|w \\ p|(w/m) \Rightarrow p|N}} \prod_{j=1}^{l} (v_j + 1) = \prod_{i=1}^{k} (u_i + 1) \prod_{j=1}^{l} (v_j + 1) = d(w).$$

Prendiamo allora

$$z = N^{1/8}$$

. Mettendo insieme le stime ottenute e applicando il Teorema 1.16 otteniamo

$$\prod_{p|N} \left(1 - \frac{1}{p}\right)^{-1} G(z) \geq \sum_{w<z} \frac{d(w)}{w} \gg (\log z)^2 \gg (\log N)^2,$$

da cui segue

$$\frac{|A|}{G(z)} \ll \frac{N}{(\log N)^2} \prod_{p|N} \left(1 - \frac{1}{p}\right)^{-1} =$$

$$= \frac{N}{(\log N)^2} \prod_{p|N} \left(1 - \frac{1}{p^2}\right)^{-1} \prod_{p|N} \left(1 + \frac{1}{p}\right) \ll \frac{N}{(\log N)^2} \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

dato che il prodotto infinito $\prod_{p=2}^{\infty}(1 - p^{-2})$ converge, come si verifica facilmente applicando il Teorema 1.35. Dobbiamo ora stimare il secondo termine. Grazie a (16) abbiamo

$$R = \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)} |r(d)| \leq \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)} 2^{\omega(d)} \leq \sum_{d<z^2} 6^{\omega(d)}.$$

Ricordando che $\omega(d)$ è il numero di divisori primi distinti di d, abbiamo che $2^{\omega(d)} \leq d$, e quindi, cambiando base dell'esponenziale,

$$6^{\omega(d)} = \left(2^{\omega(d)}\right)^{\log 6/\log 2} \leq d^{\log 6/\log 2} < z^{2 \log 6/\log 2}.$$

Ora dato che abbiamo posto $z = N^{1/8}$ segue

$$R \leq \sum_{d<z^2} z^{2 \log 6/\log 2} < z^{2+2 \log 6/\log 2} < z^{7.2} = N^{9/10}.$$

Allora

$$S(A, \mathcal{P}, z) \ll \frac{N}{(\log N)^2} \prod_{p|N} \left(1 + \frac{1}{p}\right) + N^{9/10} \ll \frac{N}{(\log N)^2} \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

e quindi in conclusione

$$r(N) \leq 2\sqrt{N} + S(A, \mathcal{P}, z) \ll \frac{N}{(\log N)^2} \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

□

Teorema 3.12 *Dato N intero pari, indichiamo con $\pi_N(x)$ il numero di primi $p \leq x$ tali che anche $p + N$ è primo. Allora*

$$\pi_N(x) \ll \frac{x}{(\log x)^2} \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

Dimostrazione: Seguiamo una dimostrazione analoga al Teorema 3.11. Sia $a_n = n(n+N)$ e $A = \{a_n : 1 \leq n \leq x\}$. Allora $|A| = [x]$. Sia $\mathcal{P}$ l'insieme di tutti i primi. Per ogni z tale che $2 < z \leq \sqrt{x}$ indichiamo con $S(A, \mathcal{P}, z)$ il numero di termini di A che non sono divisibili per nessun primo $p < z$. Se $n \geq \sqrt{x}$ e $a_n \equiv 0 \ (mod\ p)$ per qualche $p < z$, o n o $n + N$ non sono primi. Come sopra ciò non vale per gli $n \leq \sqrt{z}$. Otteniamo quindi

$$\pi_N(x) \leq \sqrt{x} + S(A, \mathcal{P}, z).$$

Preso $d = p_1 \cdots p_k q_1 \cdots q_l$, dove i p_i dividono N e i q_j no come sopra, e $g(d)$ definita in (15) abbiamo la stessa stima per $|A_d|$ e $|r(d)|$. Usando sempre il Teorema 3.10 otteniamo

$$S(A, \mathcal{P}, z) \leq \frac{|A|}{G(z)} + \sum_{\substack{d < z^2 \\ d | P(z)}} 3^{\omega(d)} |r(d)|$$

che può essere stimata esattamente come sopra fornendo la tesi. □

Corollario 3.13 *Per $N = 2$ otteniamo una stima migliore di quella del Teorema 3.5:*

$$\pi_2(x) \ll \frac{x}{(\log x)^2}.$$

4 Teorema di Goldbach-Shnirel'man

4.1 Densità di Shnirel'man

Definizione 4.1 (Densità di Shnirel'man) *Sia A un insieme di interi. Per ogni numero reale x indichiamo con $A(x)$ il numero di elementi positivi di A non maggiori di x, ovvero*

$$A(x) = \sum_{\substack{a\in A\\ 1\le a\le x}} 1.$$

*Se $x > 0$, $0 \le A(x) \le [x] \le x$ da cui $0 \le A(x)/x \le 1$. La densità di Shnirel'man dell'insieme A, indicata con $\sigma(a)$, è definita come l'*inf *sugli interi positivi di questa quantità, ovvero*

$$\sigma(A) = \inf_{n>0} \frac{A(n)}{n}.$$

Osservazione 4.2 *Se $1 \notin A$ allora $A(1) = 0$ e quindi $\sigma(A) = 0$. D'altra parte $\sigma(A) = 1$ se e solo se A contiene tutti gli interi positivi. In generale, se $\sigma(A) = \alpha$ avremo $A(n) \ge \alpha n$ per ogni n.*

Definizione 4.3 *Se A e B sono insiemi di interi, l'insieme somma $A + B$ è l'insieme costituito da tutti gli interi della forma $a + b$ con $a \in A, b \in B$. Indichiamo con hA l'insieme somma di h copie di A.*

Definizione 4.4 *Diciamo che A è una base di ordine h se hA contiene tutti gli interi non negativi, o equivalentemente se ogni intero non negativo può essere scritto come somma di h elementi (non necessariamente distinti) di A. Per l'Osservazione 4.2, se $0 \in A$ questo equivale a chiedere $\sigma(hA) = 1$.*

Lemma 4.5 *Siano A e B insiemi di interi tali che $0 \in A, 0 \in B$. Se $n \ge 0$ e $A(n)+B(n) \ge n$, allora $n \in A+B$.*

Dimostrazione: Se $n \in A$ o $n \in B$ allora $n = n + 0 \in A + B$. Supponiamo allora $n \notin A \cup B$. Definiamo

$$A' = \{n - a \ : \ a \in A,\ 1 \le a \le n - 1\}$$

e

$$B' = \{b \ : \ b \in B,\ 1 \le b \le n - 1\}.$$

Allora, dato che $n \notin A \cup B$, $|A'| = A(n)$ e $|B'| = B(n)$. Inoltre $A' \cup B' \subseteq [1, n - 1]$ per definizione. Dato che per ipotesi $|A'| + |B'| = A(n) + B(n) \ge n$ segue $A' \cap B' \ne \emptyset$. Ma allora $n - a = b$ per qualche $a \in A, b \in B$ e quindi $n = a + b \in A + B$. □

Lemma 4.6 *Siano A e B insiemi di interi tali che $0 \in A, 0 \in B$. Se $\sigma(A) + \sigma(B) \ge 1$, allora $n \in A + B$ per ogni n non negativo.*

Dimostrazione: Dato che per definizione $A(n) \ge n\sigma(A)$ per ogni n,

$$A(n) + B(n) \ge (\sigma(A) + \sigma(B))n \ge n.$$

La tesi segue allora dal Lemma 4.5. □

Lemma 4.7 *Sia A un insieme di interi tale che $0 \in A$ e $\sigma(A) \ge 1/2$. Allora A è una base di ordine 2.*

Dimostrazione: Segue dal Lemma 4.6 con $A = B$. □

Teorema 4.8 (Schirel'man) *Siano A e B insiemi di interi tali che $0 \in A, 0 \in B$. Detti $\sigma(A) = \alpha$ e $\sigma(B) = \beta$ vale*

$$\sigma(A + B) \ge \alpha + \beta - \alpha\beta$$

o equivalentemente

$$1 - \sigma(A + B) \le (1 - \sigma(A))(1 - \sigma(B)).$$

Dimostrazione: Prendiamo $n \ge 1$, $a_0 = 0$ e siano

$$1 \le a_1 < \cdots < a_k \le n$$

i $k = A(n)$ elementi positivi di A non maggiori di n. Dato che $0 \in B$, vale $a_i \in A + B$ per $i = 1, ..., k$. Per $i = 0, ..., k - 1$ siano

$$1 \le b_1 < \cdots < b_{r_i} \le a_{i+1} - a_i - 1$$

gli $r_i = B(a_{i+1} - a_i - 1)$ elementi positivi di B minori di $a_{i+1} - a_i$. Allora

$$a_i < a_i + b_1 < \cdots < a_i + b_{r_i} < a_{i+1}$$

e $a_i + b_j \in A + B$ per $j = 1, ..., r_i$. Lo stesso discorso vale posto $r_k = B(n - a_k)$, con in questo caso $a_k + b_{r_k} \leq n$ e $a_k + b_j \in A + B$ per $j = 1, ..., r_k$. Abbiamo quindi

$$(A+B)(n) \geq A(n) + \sum_{i=0}^{k-1} B(a_{i+1} - a_i - 1) + B(n - a_k) \geq$$
$$\geq A(n) + \beta \sum_{i=0}^{k-1} (a_{i+1} - a_i - 1) + \beta(n - a_k) =$$
$$= A(n) + \beta \sum_{i=0}^{k-1} (a_{i+1} - a_i) + \beta(n - a_k) - \beta k =$$
$$A(n) + \beta(a_k - a_0 + n - a_k - k) = A(n) + \beta n - \beta k$$

sfruttando il fatto che la somma è telescopica e che $a_0 = 0$. Da qui, ricordando che $k = A(n)$, segue

$$A(n) + \beta n - \beta k = A(n) + \beta n - \beta A(n) =$$
$$= (1 - \beta)A(n) + \beta n \geq (1 - \beta)\alpha n + \beta n = (\alpha + \beta - \alpha\beta)n,$$

quindi

$$\frac{(A+B)(n)}{n} \geq \alpha + \beta - \alpha\beta$$

e di conseguenza

$$\sigma(A+B) = \inf_{n>0} \frac{(A+B)(n)}{n} \geq \alpha + \beta - \alpha\beta.$$

□

Teorema 4.9 *Sia $h \geq 1$, $A_1, ..., A_h$ insiemi di interi tali che $0 \in A_i$ per ogni i. Allora*

$$1 - \sigma(A_1 + \cdots + A_h) \leq \prod_{i=1}^{h} (1 - \sigma(A_i)).$$

Dimostrazione: Ragioniamo per induzione su h. Se $h = 1$ abbiamo un'identità, mentre la validità per $h = 2$ è garantita dal Teorema 4.8. Per $h \geq 3$, assumiamo la tesi valida per $h - 1$. Allora dati $A_1, ..., A_h$ tali che $0 \in A_i$ per ogni i, poniamo $B = A_2 + \cdots A_h$. Per ipotesi induttiva abbiamo

$$1 - \sigma(B) = 1 - \sigma(A_2 + \cdots + A_h) \leq \prod_{i=2}^{h} (1 - \sigma(A_i)),$$

e applicando ancora l'ipotesi (o equivalentemente il Teorema 4.8) ad $A + B$ otteniamo

$$1 - \sigma(A_1 + \cdots + A_h) = 1 - \sigma(A_1 + B) \leq (1 - \sigma(A_1))(1 - \sigma(B)) \leq$$
$$\leq (1 - \sigma(A_1)) \prod_{i=2}^{h} (1 - \sigma(A_i)) = \prod_{i=1}^{h} (1 - \sigma(A_i)).$$

□

Teorema 4.10 (Shnirel'man) *Sia A un insieme di interi tale che $0 \in A$ e $\sigma(A) > 0$. Allora A è una base di ordine finito.*

Dimostrazione: Poniamo $\sigma(A) = \alpha > 0$. Allora $0 \leq 1 - \alpha < 1$, e quindi $0 \leq (1 - \alpha)^l \leq 1/2$ per qualche $l \geq 1$. Per il Teorema 4.9 segue che

$$1 - \sigma(lA) \leq (1 - \sigma(A))^l = (1 - \alpha)^l \leq 1/2$$

e quindi $\sigma(lA) \geq 1/2$. Ma allora grazie al Lemma 4.7 lA è una base di ordine 2, o equivalentemente A è una base di ordine $2l$. □

4.2 Teorema di Goldbach-Shnirel'man

Lemma 4.11 *Sia $r(N)$ il numero di rappresentazioni di N come somma di due primi. Allora*

$$\sum_{N\le x} r(N) \gg \frac{x^2}{(\log x)^2}.$$

Dimostrazione: Se $p, q \le x/2$ sono primi, $p+q = n \le x$ è la rappresentazione di un intero come somma di due primi e compare quindi nella somma di sinistra. Il numero di tali rappresentazioni è $\pi(x/2)^2$. D'altra parte, in questo modo escludiamo tutte le rappresentazioni che contengano un primo maggiore di $x/2$. Applicando allora il Teorema 2.12 (di Chebyshev) abbiamo

$$\sum_{N\le x} r(N) \ge \pi(x/2)^2 \gg \frac{(x/2)^2}{(\log(x/2))^2} \gg \frac{x^2}{(\log x)^2}.$$

□

Lemma 4.12 *Sia $r(N)$ come sopra. Allora*

$$\sum_{N\le x} r(N)^2 \ll \frac{x^3}{(\log x)^4}.$$

Dimostrazione: Grazie al Teorema 3.11, per N pari abbiamo

$$r(N) \ll \frac{N}{(\log N)^2} \prod_{p|N}\left(1+\frac{1}{p}\right) \le \frac{N}{(\log N)^2}\sum_{d|N}\frac{1}{d}.$$

N dispari invece può essere scritto come somma di due primi se e solo se $N-2$ è primo, e in tal caso $r(N) = 2$. La stima è quindi valida per ogni N. Abbiamo allora

$$\sum_{N\le x} r(N)^2 \ll \sum_{N\le x} \frac{N^2}{(\log N)^4}\left(\sum_{d|N}\frac{1}{d}\right)^2 \ll \frac{x^2}{(\log x)^4}\sum_{N\le x}\left(\sum_{d|N}\frac{1}{d}\right)^2.$$

Stimando la somma interna abbiamo

$$\sum_{N\le x}\left(\sum_{d|N}\frac{1}{d}\right)^2 = \sum_{N\le x}\sum_{d_1|N}\sum_{d_2|N}\frac{1}{d_1 d_2} \le \sum_{d_1,d_2\le x}\frac{1}{d_1 d_2}\sum_{\substack{N\le x\\ d_1|N, d_2|N}} 1 =$$
$$= \sum_{d_1,d_2\le x}\frac{1}{d_1 d_2}\sum_{\substack{N\le x\\ [d_1,d_2]|N}} 1 \le \sum_{d_1,d_2\le x}\frac{1}{d_1 d_2}\frac{x}{[d_1,d_2]}.$$

Ora, sfruttando il fatto che se un fattore primo compare sia in d_1 che in d_2 comparirà due volte in $d_1 d_2$ e una sola volta in (d_1, d_2), mentre se compare in uno solo dei due numeri comparirà nel prodotto ma non nell'mcd, abbiamo

$$[d_1, d_2] = \frac{d_1 d_2}{(d_1, d_2)} \ge (d_1 d_2)^{1/2}$$

da cui otteniamo

$$\sum_{d_1,d_2\le x}\frac{1}{d_1 d_2}\frac{x}{[d_1,d_2]} \le x\sum_{d_1,d_2\le x}\frac{1}{d_1^{3/2} d_2^{3/2}} = x\left(\sum_{d\le x}\frac{1}{d^{3/2}}\right)^2.$$

Dato che la somma tra parentesi converge abbiamo

$$\sum_{N\le x} r(N)^2 \ll \frac{x^2}{(\log x)^4}\sum_{N\le x}\left(\sum_{d|N}\frac{1}{d}\right)^2 \le \frac{x^3}{(\log x)^4}\left(\sum_{d\le x}\frac{1}{d^{3/2}}\right)^2 \ll \frac{x^3}{(\log x)^4}.$$

□

Teorema 4.13 *L'insieme*

$$A = \{0, 1\} \cup \{p + q : p, q \text{ primi}\}$$

ha densità positiva.

Dimostrazione: Indichiamo sempre con $r(N)$ il numero di rappresentazioni di N come somma di due primi. Per la disuguaglianza di Cauchy-Schwarz otteniamo

$$\left(\sum_{N\leq x} r(N)\right)^2 \leq \sum_{\substack{N\leq x \\ r(N)\geq 1}} 1 \sum_{N\leq x} r(N)^2 \leq A(x) \sum_{N\leq x} r(N)^2$$

per definizione di A, che contiene gli n tali che $r(n) \geq 1$ oltre a 0 e 1. Ricordando ora le stime ottenute nei Lemmi 4.11 e 4.12 abbiamo

$$\frac{A(x)}{x} \geq \frac{1}{x} \frac{(\sum_{N\leq x} r(N))^2}{\sum_{N\leq x} r(N)^2} \gg \frac{1}{x} \frac{x^4}{(\log x)^4} \frac{(\log x)^4}{x^3} \gg 1.$$

Esiste quindi una costante $c_1 > 0$ e un numero x_0 tali che $A(x) \geq c_1 x$ per ogni $x \geq x_0$. Ma dato che $1 \in A$, esiste anche una costante $c_2 > 0$ tale che $A(x) \geq c_2 x$ per $1 \leq x \leq x_0$ (possiamo prendere $1/x_0$). Quindi $A(x) \geq \min(c_1, c_2)x$ per ogni $x \geq 1$ e la densità di A $\sigma(A) \geq \min(c_1, c_2)$ è positiva. □

Teorema 4.14 (Goldbach-Shnirel'man) *Esiste una costante S_0 tale che ogni intero maggiore di 1 è somma di al più S_0 numeri primi.*

Dimostrazione: Nel Teorema 4.13 abbiamo dimostrato che l'insieme

$$A = \{0, 1\} \cup \{p + q : p, q \text{ primi}\}$$

ha densità positiva. Grazie al Teorema 4.10 A è quindi una base di ordine finito. Indicando l'ordine di A con h, questo significa che ogni intero positivo è somma di esattamente h elementi di A. Prendiamo un intero $N \geq 2$. Allora $N - 2 \geq 0$ e per quanto visto esisteranno due interi k, l tali che $k + l \leq h$ (dato che anche $0 \in A$) e l coppie di primi tali che

$$N - 2 = \underbrace{1 + \cdots + 1}_{\text{k}} + (p_1 + q_1) + \cdots + (p_l + q_l).$$

Dobbiamo ora eliminare gli 1 presenti nella somma. Se $k = 0$ siamo a posto, mentre se $k = 1$, avendo preso $N - 2$ possiamo scrivere

$$N = 3 + (p_1 + q_1) + \cdots + (p_l + q_l).$$

Per $k > 1$, detto $m = [k/2]$ possiamo sostituire la somma di k volte 1 con m volte 2 se k pari, $m - 1$ volte 2 e una volta 3 se k dispari. Portando a destra il -2 avremo in generale la somma di $m + 1$ copie di 2 o 3 e di l coppie di primi. In ogni caso possiamo scrivere N come somma di al più $2l + m + 1 \leq 3h = S_0$ numeri primi, con S_0 costante dato che h è fissato. □

5 Teorema di Vinogradov

5.1 Metodo del Cerchio

Definizione 5.1 *Indichiamo con $r_{A,s}(N)$ il numero di rappresentazioni di N come somma di s elementi di A. Indichiamo invece con $r_{A,s}^{(N)}(m)$ il numero di rappresentazioni di m come somma di s elementi di A non eccedenti N.*

Presentiamo ora il metodo del cerchio. Dato un insieme A di interi non negativi, studiamo la funzione generatrice

$$f(z) = \sum_{a \in A} z^a.$$

Possiamo considerare $f(z)$ come una serie formale di potenze o come la serie di Taylor di una funzione analitica, convergente del disco complesso $|z| < 1$. In ogni caso, elevando f a potenza e riordinando le somme, otteniamo

$$f(z)^s = \sum_{N=0}^{\infty} r_{A,s}(N) z^N.$$

Ricordando il Teorema di Taylor sulle serie di potenze in campo complesso, che afferma che

$$c_n = \frac{1}{2\pi i} \int_{\delta B(a,\rho)} \frac{f(z)}{(z-a)^{n+1}} dz$$

(una dimostrazione si può trovare, ad esempio, in [3]), abbiamo in questo caso

$$r_{A,s}(N) = \frac{1}{2\pi i} \int_{|z|=\rho} \frac{f(z)^s}{z^{N+1}} dz$$

dove $\rho \in (0,1)$ e la serie è centrata nell'origine. Questo metodo, introdotto da Hardy, Littlewood e Ramanujan, è stato poi perfezionato da Vinogradov, che ha sostituito $f(z)$ con il polinomio

$$p(z) = \sum_{\substack{a \in A \\ a \leq N}} z^a.$$

In questo modo elevando $p(z)^s$ il massimo esponente raggiungibile è sN, e abbiamo la serie finita

$$p(z)^s = \sum_{m=0}^{sN} r_{A,s}^{(N)}(m) z^m.$$

Osserviamo che se $m \leq N$, allora tutti gli a coinvolti in una possibile rappresentazione di m saranno anch'essi non maggiori di N. Avremo quindi in questo caso $r_{A,s}^N(m) = r_{A,s}(m)$. Inoltre, per quanto detto prima, $r_{A,s}^N(m) = 0$ se $m > sN$. Facciamo variare ora z sul cerchio unitario, ponendo

$$z = e(\alpha) = e^{2\pi i \alpha}.$$

Sostituendo nelle espressioni precedenti abbiamo

$$F(\alpha) = p(e(\alpha)) = \sum_{\substack{a \in A \\ a \leq N}} e(a\alpha)$$

$$F(\alpha)^s = \sum_{m=0}^{sN} r_{A,s}^{(N)}(m) e(m\alpha).$$

Ricordando che gli $e(\alpha)$ sono tra loro ortogonali, ovvero

$$\int_0^1 e(m\alpha) e(-n\alpha) d\alpha = \begin{cases} 1 \text{ se } m = n \\ 0 \text{ se } m \neq n \end{cases}$$

abbiamo

$$\int_0^1 F(\alpha)^s e(-N\alpha) d\alpha = \int_0^1 \sum_{j=0}^{sN} r_{A,s}^{(N)}(j) e(j\alpha) e(-N\alpha) d\alpha = r_{A,s}^{(N)}(N) = r_{A,s}(N)$$

per quanto osservato prima.
L'intervallo $[0,1]$ (e quindi la sua immagine, il cerchio unitario) viene poi diviso in due insiemi disgiunti, detti arco maggiore ($\mathfrak{M}$) e arco minore ($\mathfrak{m}$). Fissato N, prendiamo $B > 0$ e poniamo $Q = (\log N)^B$. Allora per ogni $1 \leq q \leq Q$ e $0 \leq a \leq q$ tali che $(a,q) = 1$ l'arco maggiore $\mathfrak{M}(q,a)$ è l'insieme dei reali $\alpha \in [0,1]$ tali che

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{Q}{N}.$$

Ora se avessimo $\alpha \in \mathfrak{M}(q,a) \cap \mathfrak{M}(q',a')$ e $a/q \neq a'/q'$ allora $|aq' - a'q| \geq 1$ dal momento che deve essere intero e diverso da 0, e quindi

$$\frac{1}{Q^2} \leq \frac{1}{qq'} \leq \frac{|aq' - a'q|}{qq'} = \left|\frac{a}{q} - \frac{a'}{q'}\right| \leq$$
$$\leq \left|\frac{a}{q} - \alpha\right| + \left|\alpha - \frac{a'}{q'}\right| \leq \frac{2Q}{N},$$

o equivalentemente

$$N \leq 2Q^3 \leq 2(\log N)^{3B}.$$

Questo non è possibile per N sufficientemente grande, e quindi per tali N gli archi maggiori $\mathfrak{M}(q,a)$ sono a due a due disgiunti. Definiamo allora

$$\mathfrak{M} = \bigcup_{q=1}^{Q} \bigcup_{\substack{a=0 \\ (a,q)=1}}^{q} \mathfrak{M}(q,a) \subseteq [0,1]$$

e

$$\mathfrak{m} = [0,1] \backslash \mathfrak{M}.$$

Indichiamo ora per brevità

$$r(N) = r_{\mathcal{P},3}(N) = \sum_{p_1+p_2+p_3=N} 1$$

il numero di rappresentazioni di un dato numero N come somma di tre primi. Per ottenere una stima asintotica per $r(N)$, Vinogradov sfruttò un'altra funzione,

$$R(N) = \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3$$

ovvero la somma pesata delle rappresentazioni di N. Applicando il metodo del cerchio tenendo conto dei pesi abbiamo

$$F(\alpha) = \sum_{p \leq N} (\log p) e(p\alpha)$$

e

$$R(N) = \int_0^1 F(\alpha)^3 e(-N\alpha) d\alpha =$$
$$\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha) d\alpha + \int_{\mathfrak{m}} F(\alpha)^3 e(-N\alpha) d\alpha$$

5.2 Serie Singolare

Definizione 5.2 (Serie singolare) *La funzione aritmetica*

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \frac{\mu(q) c_q(N)}{\varphi(q)^3},$$

dove $c_q(N)$ è la somma di Ramanujan definita in 1.30, è detta serie singolare per il problema ternario di Goldbach.

Teorema 5.3 *La serie singolare $\mathfrak{S}(N)$ converge assolutamente e uniformemente in N. Inoltre per ogni $\epsilon > 0$ vale*

$$\mathfrak{S}(N,Q) = \sum_{q \leq Q} \frac{\mu(q) c_q(N)}{\varphi(q)^3} = \mathfrak{S}(N) + \mathcal{O}(Q^{-(1-\epsilon)})$$

dove la costante dipende solo da ϵ.

Dimostrazione: Dalla definizione di c_q è chiaro che $c_q(N) \ll \varphi(q)$. Grazie al Teorema 1.29 $\phi(q) > q^{1-\epsilon}$ per $\epsilon > 0$ e q sufficientemente grande. Abbiamo allora

$$\frac{\mu(q)c_q(N)}{\varphi(q)^3} \ll \frac{1}{\varphi(q)^2} \ll \frac{1}{q^{2-\epsilon}}.$$

La serie singolare converge quindi assolutamente e uniformemente in N. Inoltre utilizzando le stesse stime e sommando alla fine otteniamo

$$\mathfrak{S}(N) - \mathfrak{S}(N,Q) \ll \sum_{q>Q} \frac{1}{\varphi(q)^2} \ll \sum_{q>Q} \frac{1}{q^{2-\epsilon}} \ll \frac{1}{Q^{1-\epsilon}}.$$

□

Teorema 5.4 *La serie singolare $\mathfrak{S}(N)$ ha prodotto di Eulero*

$$\mathfrak{S}(N) = \prod_p \left(1 + \frac{1}{(p-1)^3}\right) \prod_{p|N} \left(1 - \frac{1}{p^2 - 3p + 3}\right).$$

Per N pari è quindi nulla, mentre per N dispari esistono due costanti positive c_1, c_2 tali che

$$c_1 < \mathfrak{S}(N) < c_2$$

per ogni N.

Dimostrazione: Le funzioni $c_q(N), \varphi(q)$ e $\mu(q)$ sono moltiplicative in q rispettivamente per i Teoremi 1.31 e 1.28 e per l'Osservazione 1.20. La funzione

$$\frac{\mu(q)c_q(N)}{\varphi(q)^3}$$

è quindi moltiplicativa. Visto che la serie singolare converge assolutamente, grazie al Teorema 1.39 avrà prodotto di Eulero

$$\mathfrak{S}(N) = \prod_p \left(1 + \sum_{j=1}^{\infty} \frac{\mu(p^j)c_{p^j}(N)}{\varphi(p^j)^3}\right).$$

Per definizione, $\mu(p^j)$ vale -1 se e solo se $j = 1$, e altrimenti vale 0, cancellando i rispettivi termini nella somma. Grazie al Teorema 1.28 $\varphi(p) = p - 1$. Infine, per il Teorema 1.32,

$$c_p(N) = \begin{cases} p-1 \text{ se } p|N \\ -1 \text{ se } p \nmid N. \end{cases}$$

Sostituendo nell'espressione precedente ricaviamo quindi

$$\mathfrak{S}(N) = \prod_p \left(1 - \frac{c_p(N)}{\varphi(p)^3}\right) =$$

$$\prod_{p\nmid N} \left(1 + \frac{1}{(p-1)^3}\right) \prod_{p|N} \left(1 - \frac{1}{(p-1)^2}\right) = \prod_p \left(1 + \frac{1}{(p-1)^3}\right) \prod_{p|N} \left(1 - \frac{1}{p^2 - 3p + 3}\right).$$

L'ultima uguaglianza può essere verificata per calcolo diretto. Stiamo chiedendo che per $p|N$ valga

$$\left(1 - \frac{1}{(p-1)^2}\right) = \left(1 + \frac{1}{(p-1)^3}\right)\left(1 - \frac{1}{p^2 - 3p + 3}\right).$$

Il membro a destra vale

$$1 + \frac{1}{(p-1)^3} - \frac{1}{p^2 - 3p + 3} - \frac{1}{(p-1^3)(p^2 - 3p + 3)} = 1 + \frac{p^2 - 3p + 3 - (p-1)^3 - 1}{(p-1)^3(p^2 - 3p + 3)}$$

e la verifica è completata dato che il numeratore vale esattamente $-(p-1)(p^2 - 3p + 3)$. Ora per N dispari la serie singolare si divide in due prodotti infiniti, entrambi convergenti grazie al Teorema 1.35 (se estendiamo il secondo) e quindi esistono due costanti positive c_1, c_2 tali che

$$c_1 < \mathfrak{S}(N) < c_2.$$

□

5.3 Arco Maggiore

Teorema 5.5 *Indichiamo con $r_{1,s}(N)$ il numero di rappresentazioni di N come somma di s interi. Per $s \geq 1$ vale*

$$r_{1,s}(N) = \binom{N-1}{s-1} = \frac{N^{s-1}}{(s-1)!} + \mathcal{O}(N^{s-2}).$$

Dimostrazione: Prendiamo $N \geq s$. Allora

$$N = a_1 + \cdots + a_s$$

è una decomposizione di N come somma di s interi ≥ 1 se e solo se

$$N - s = (a_1 - 1) + \cdots + (a_s - 1)$$

è una decomposizione di $N - s$ come somma di s interi ≥ 0. Indicando con $R_{1,s}(N)$ il numero di queste rappresentazioni vale

$$r_{1,s}(N) = R_{1,s}(N - s).$$

Immaginiamo ora di avere $N + s - 1$ scatole. Data una partizione $N = a_1 + \cdots + a_s$, possiamo colorare le prime a_1 di rosso, poi una di blu, poi a_2 di rosso, poi una di blu e così via. In questo modo abbiamo associato ad una colorazione con N scatole rosse e $s-1$ blu la partizione. Il processo inverso consiste, date le $N+s-1$ scatole di cui $s-1$ blu, di indicare con a_1 il numero di scatole rosse prima della prima blu, con a_2 quelle tra la prima e la seconda e così via. Chiaramente in questo modo $a_1 + \cdots + a_s = N$. Si tratta quindi di una biezione. Il numero di queste partizioni, ovvero $R_{1,s}(N)$ dal momento che accettiamo elementi nulli, è però anche in relazione con i sottoinsiemi di $s-1$ elementi (le scatole blu) su $N+s-1$. Abbiamo quindi $R_{1,s}(N) = \binom{N+s-1}{s-1}$ da cui

$$r_{1,s}(N) = R_{1,s}(N - s) = \binom{N-1}{s-1}.$$

□

Lemma 5.6

$$J(N) = \int_{-1/2}^{1/2} u(\beta)^3 e(-N\beta) d\beta = \frac{N^2}{2} + \mathcal{O}(N),$$

dove

$$u(\beta) = \sum_{m=1}^{N} e(m\beta).$$

Dimostrazione: Applicando il metodo del cerchio abbiamo

$$r_{1,3}(N) = \int_{-1/2}^{1/2} u(\beta)^3 e(-N\beta) d\beta = J(N),$$

e grazie al Teorema 5.5,

$$r_{1,3}(N) = \binom{N-1}{2} = \frac{N^2}{2} + \mathcal{O}(N).$$

□

Teorema 5.7 (Siegel-Walfisz) *Se $q \geq 1$ e $(a,q) = 1$, allora per ogni $C > 0$*

$$\vartheta(x; q, a) = \sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} \log p = \frac{x}{\varphi(q)} + \mathcal{O}\left(\frac{x}{(\log x)^C}\right).$$

Una dimostrazione di questo Teorema, che qui non riportiamo, si trova in [2].

Lemma 5.8 *Siano*

$$F_x(\alpha) = \sum_{p \leq x} (\log p) e(p\alpha)$$

e B, C costanti positive. Allora se $1 \leq q \leq Q = (\log N)^B$, $(q,a) = 1$ e $1 \leq x \leq N$ abbiamo

$$F_x(a/q) = \frac{\mu(q)}{\varphi(q)} x + \mathcal{O}\left(\frac{QN}{(\log N)^C}\right).$$

Dimostrazione: Sia $p \equiv r \pmod q$. Allora $p|q$ se e solo se $(r,q) = (p,q) > 1$. Vale allora

$$\sum_{\substack{r=1\\(r,q)>1}}^{q} \sum_{p\le x \atop p\equiv r \pmod q} (\log p) e(pa/q) = \sum_{\substack{p\le x\\ p|q}} (\log p) e(pa/q) \ll \sum_{p|q} \log p \le \log q.$$

Spezzando la somma otteniamo allora

$$F_x\left(\frac{a}{q}\right) = \sum_{r=1}^{q} \sum_{p\le x \atop p\equiv r \pmod q} (\log p) e\left(\frac{pa}{q}\right) =$$

$$= \sum_{\substack{r=1\\(r,q)=1}}^{q} \sum_{p\le x \atop p\equiv r \pmod q} (\log p) e\left(\frac{ra}{q}\right) + \sum_{\substack{r=1\\(r,q)>1}}^{q} \sum_{p\le x \atop p\equiv r \pmod q} (\log p) e\left(\frac{ra}{q}\right) =$$

$$= \sum_{\substack{r=1\\(r,q)=1}}^{q} e\left(\frac{ra}{q}\right) \sum_{p\le x \atop p\equiv r \pmod q} (\log p) + \mathcal{O}(\log q) =$$

$$\sum_{\substack{r=1\\(r,q)=1}}^{q} e\left(\frac{ra}{q}\right) \vartheta(x;q,r) + \mathcal{O}(\log Q) = \sum_{\substack{r=1\\(r,q)=1}}^{q} e\left(\frac{ra}{q}\right)\left(\frac{x}{\varphi(q)} + \mathcal{O}\left(\frac{x}{(\log x)^C}\right)\right) + \mathcal{O}(\log Q)$$

per ogni $C > 0$ grazie al Teorema 5.7. Ora, ricordando che per il Teorema 1.32 $c_q(a) = \mu(q)$ se $(q,a) = 1$, otteniamo

$$\sum_{\substack{r=1\\(r,q)=1}}^{q} e\left(\frac{ra}{q}\right)\left(\frac{x}{\varphi(q)} + \mathcal{O}\left(\frac{x}{(\log x)^C}\right)\right) + \mathcal{O}(\log Q) = \frac{c_q(a)}{\varphi(q)} x + \mathcal{O}\left(\frac{qx}{(\log x)^C}\right) + \mathcal{O}(\log Q) =$$

$$= \frac{\mu(q)}{\varphi(q)} x + \mathcal{O}\left(\frac{QN}{(\log N)^C}\right).$$

□

Lemma 5.9 *Siano B, C costanti positive con $C > 2B$. Se $\alpha \in \mathfrak{M}(q,a)$ e $\beta = \alpha - a/q$, allora*

$$F(\alpha) = \frac{\mu(q)}{\varphi(q)} u(\beta) + \mathcal{O}\left(\frac{Q^2 N}{(\log N)^C}\right)$$

e

$$F(\alpha)^3 = \frac{\mu(q)}{\varphi(q)^3} u(\beta)^3 + \mathcal{O}\left(\frac{Q^2 N^3}{(\log N)^C}\right)$$

dove le costanti dipendono solo da B e C.

Dimostrazione: Se $\alpha \in \mathfrak{M}(q,a)$ allora $\alpha = a/q + \beta$ con $|\beta| \le Q/N$. Definiamo

$$\lambda(m) = \begin{cases} \log p \text{ se } m = p \text{ è primo} \\ 0 \text{ altrimenti.} \end{cases}$$

Abbiamo quindi

$$F(\alpha) - \frac{\mu(q)}{\varphi(q)} u(\beta) = \sum_{p\le N} \log p e(p\alpha) - \frac{\mu(q)}{\varphi(q)} \sum_{m=1}^{N} e(m\beta) =$$

$$\sum_{m=1}^{N} \lambda(m) e(m\alpha) - \frac{\mu(q)}{\varphi(q)} \sum_{m=1}^{N} e(m\beta) = \sum_{m=1}^{N} \lambda(m) e\left(\frac{ma}{q} + m\beta\right) - \frac{\mu(q)}{\varphi(q)} \sum_{m=1}^{N} e(m\beta) =$$

$$= \sum_{m=1}^{N} \left(\lambda(m) e\left(\frac{ma}{q}\right) - \frac{\mu(q)}{\varphi(q)}\right) e(m\beta).$$

Se $1 \leq x \leq N$, applicando il Lemma 5.8 e ricordando che la prima parte della somma è solo sui primi grazie a $\lambda(m)$ otteniamo

$$A(x) = \sum_{m=1}^{x} \left(\lambda(m) e\left(\frac{ma}{q}\right) - \frac{\mu(q)}{\varphi(q)} \right) =$$
$$\sum_{m=1}^{x} \lambda(m) e\left(\frac{ma}{q}\right) - \frac{\mu(q)}{\varphi(q)} x =$$
$$F_x\left(\frac{a}{q}\right) - \frac{\mu(q)}{\varphi(q)} x = \mathcal{O}\left(\frac{QN}{(\log N)^C}\right).$$

Dato che chiaramente $e(t)$ ha derivata continua, possiamo applicare il Teorema 1.7 con le scelte $u(m) = \lambda(m) e\left(\frac{ma}{q}\right) - \frac{\mu(q)}{\varphi(q)}$ e $f(m) = e(m\beta)$, otteniamo

$$F(\alpha) - \frac{\mu(q)}{\varphi(q)} u(\beta) = \sum_{m=1}^{N} u(m) f(m) = A(N) e(N\beta) - 2\pi i \beta \int_1^N A(x) e(x\beta) dx \ll$$
$$\ll |A(N)| + |\beta| N \max\{A(x) : 1 \leq x \leq N\} \ll \frac{Q^2 N}{(\log N)^c}.$$

Infatti il primo termine cresce come $QN/(\log N)^C$ mentre il secondo è maggiorato asintoticamente da

$$\frac{Q}{N} N \left(\frac{QN}{(\log N)^C}\right) = \frac{Q^2 N}{(\log N)^C}.$$

Questo dimostra la stima per $F(\alpha)$. Per $F(\alpha)^3$ è sufficiente osservare che $\mu(q)^3 = \mu(q)$ e, dato che per ipotesi $C > 2B$,

$$\frac{Q^2 N}{(\log N)^C} = \frac{N}{(\log N)^{C-2B}} < N.$$

□

Teorema 5.10 *Dati B, C, ϵ reali positivi con $C > 2B$, l'integrale sull'arco maggiore vale*

$$\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha) d\alpha = \mathfrak{S}(N) \frac{N^2}{2} + \mathcal{O}\left(\frac{N^2}{(\log N)^{(1-\epsilon)B}}\right) + \mathcal{O}\left(\frac{N^2}{(\log N)^{C-5B}}\right)$$

dove le costanti dipendono solo da B, C ed ϵ.

Dimostrazione: Ricordiamo che l'arco maggiore $\mathfrak{M}(q,a)$ con $(q,a) = 1$ è l'insieme degli $\alpha \in [0,1]$ tali che

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{Q}{N}.$$

Se $q = 1$ allora $a = 1$ oppure $a = 0$. Nel primo caso possiamo accettare solo $\alpha \in [1 - Q/N, 1]$, nel secondo $\alpha \in [0, Q/N]$. In entrambi i casi la lunghezza dell'arco vale Q/N. Se invece $q \geq 2$, dato che abbiamo supposto N sufficientemente grande da rendere gli archi maggiori a due a due disgiunti, ogni arco si estende a destra e a sinistra di q/a, per una lunghezza di $2Q/N$. Iniziamo a valutare, sfruttando il Lemma 5.9 e quanto appena osservato,

$$\int_{\mathfrak{M}} \left(F(\alpha)^3 - \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha - \frac{a}{q}\right)^3 \right) e(-N\alpha) d\alpha =$$
$$= \sum_{q \leq Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} \left(F(\alpha)^3 - \frac{\mu(q)}{\varphi(q)^3} u\left(\alpha - \frac{a}{q}\right)^3 \right) e(-N\alpha) d\alpha \ll$$
$$\ll \sum_{q \leq Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} \int_{\mathfrak{M}(q,a)} \frac{Q^2 N^3}{(\log N)^C} d\alpha \ll \sum_{q \leq Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} \frac{Q^3 N^2}{(\log N)^C} d\alpha \overset{(A)}{\leq}$$
$$\leq \frac{Q^5 N^2}{(\log N)^C} \leq \frac{N^2}{(\log N)^{C-5B}}.$$

Nel passaggio (A) sfruttiamo il fatto che

$$\sum_{q \leq Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} 1 = \sum_{q \leq Q} \varphi(q) \leq \sum_{q \leq Q} (q-1) \leq (Q^2 + Q) - Q = Q^2.$$

Nella notazione del Lemma 5.9, abbiamo $\alpha = a/q + \beta$, da cui segue, essendo α nell'arco maggiore, $|\beta| \leq Q/N$. Otteniamo quindi, per quanto riguarda la seconda parte dell'integrale valutato prima,

$$\sum_{q\leq Q} \sum_{\substack{a=0\\(a,q)=1}}^{q} \frac{\mu(q)}{\varphi(q)^3} \int_{\mathfrak{M}(q,a)} u\left(\alpha - \frac{a}{q}\right)^3 e(-N\alpha)d\alpha =$$

$$\overset{(B)}{=} \sum_{q\leq Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} \frac{\mu(q)}{\varphi(q)^3} \int_{a/q-Q/N}^{a/q+Q/N} u\left(\alpha - \frac{a}{q}\right)^3 e(-N\alpha)d\alpha =$$

$$= \sum_{q\leq Q} \frac{\mu(q)}{\varphi(q)^3} \sum_{\substack{a=1\\(a,q)=1}}^{q} e(-Na/q) \int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)d\beta =$$

$$\overset{(C)}{=} \sum_{q\leq Q} \frac{\mu(q)c_q(N)}{\varphi(q)^3} \int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)d\beta =$$

$$= \mathfrak{S}(N,Q) \int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)d\beta.$$

Nel passaggio (B) attacchiamo la parte iniziale e finale dell'arco maggiore per $q = 1$, e possiamo quindi eliminare il caso $a = 0$, dato che $(a, q) = 1$ se e solo se $q = 1$. Il passaggio (C) è invece giustificato dal fatto che se $(a, q) = 1$ allora chiaramente anche $(q - a, q) = 1$. L'unico caso in cui non possiamo spostare la somma sui negativi è $q = 1$, per cui $1 - q = 0$ non è incluso nella sommatoria, ma in tal caso $c_q(-N) = c_q(N) = 1$. Per il Lemma 1.45, se $|\beta| \leq 1/2$ (sempre vero per N sufficientemente grande) $u(\beta) \ll |\beta|^{-1}$, da cui

$$\int_{Q/N}^{1/2} u(\beta)^3 e(-N\beta)d\beta \ll \int_{Q/N}^{1/2} |u(\beta)|^3 \ll$$

$$\ll \int_{Q/N}^{1/2} \beta^- 3d\beta < \frac{N^2}{Q^2}.$$

Allo stesso modo

$$\int_{-1/2}^{-Q/N} u(\beta)^3 e(-N\beta)d\beta \ll \frac{N^2}{Q^2}.$$

Attaccando i tre pezzi dell'integrale e utilizzando il Lemma 5.6 otteniamo

$$\int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)d\beta = \int_{-1/2}^{1/2} u(\beta)^3 e(-N\beta)d\beta + \mathcal{O}\left(\frac{N^2}{Q^2}\right) =$$

$$= \frac{N^2}{2} + \mathcal{O}(N) + \mathcal{O}\left(\frac{N^2}{Q^2}\right) = \frac{N^2}{2} + \mathcal{O}\left(\frac{N^2}{Q^2}\right).$$

Inoltre, per il Teorema 5.3,

$$\mathfrak{S}(N,Q) = \mathfrak{S}(N) + \mathcal{O}\left(\frac{1}{Q^{1-\epsilon}}\right).$$

In conclusione, mettendo insieme tutte le stime ricavate, otteniamo

$$\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha)d\alpha =$$

$$= \mathfrak{S}(N,Q) \int_{-Q/N}^{Q/N} u(\beta)^3 e(-N\beta)d\beta + \mathcal{O}\left(\frac{N^2}{(\log N)^{C-5B}}\right) =$$

$$\mathfrak{S}(N)\frac{N^2}{2} + \mathcal{O}\left(\frac{N^2}{Q^{1-\epsilon}}\right) + \mathcal{O}\left(\frac{N^2}{(\log N)^{C-5B}}\right) =$$

$$= \mathfrak{S}(N)\frac{N^2}{2} + \mathcal{O}\left(\frac{N^2}{(\log N)^{(1-\epsilon)B}}\right) + \mathcal{O}\left(\frac{N^2}{(\log N)^{C-5B}}\right).$$

□

5.4 Arco Minore

Lemma 5.11 (Identità di Vaughan) *Per $u \geq 1$, definiamo*

$$M_u(k) = \sum_{\substack{d|k \\ d\leq u}} \mu(d).$$

Sia $\Phi(k,l)$ una funzione aritmetica di due variabili. Allora

$$\sum_{u<l\leq N} \Phi(1,l) + \sum_{u<k\leq N} \sum_{u<l\leq N/k} M_u(k)\Phi(k,l) = \sum_{d\leq u} \sum_{u<l\leq N/d} \sum_{m\leq N/ld} \mu(d)\Phi(dm,l).$$

Dimostrazione: Valutiamo in due modi differenti la somma

$$S = \sum_{k=1}^{N} \sum_{u<l<N/k} M_u(k)\Phi(k,l).$$

Dato che, per il Teorema 1.22,

$$\sum_{d|n} \mu(d) = \delta(n) = \begin{cases} 1 \text{ se } n = 1 \\ 0 \text{ altrimenti,} \end{cases}$$

segue che

$$M_u(k) = \begin{cases} 1 \text{ se } k = 1 \\ 0 \text{ se } 1 < k \leq u, \end{cases}$$

dato che nel secondo caso la somma è su tutti i divisori di k. Otteniamo quindi

$$S = \sum_{u<l\leq N} \Phi(1,l) + \sum_{u<k\leq N} \sum_{u<l\leq N/k} M_u(k)\Phi(k,l),$$

dove il primo termine corrisponde al caso $k = 1$ mentre sono stati tolti dalla somma i k tali che $1 < k \leq u$. D'altra parte, invertendo l'ordine delle somme e operando la sostituzione $k = dm$, garantita dal fatto che $d|k$, otteniamo

$$S = \sum_{k=1}^{N} \sum_{u<l\leq N/k} \sum_{\substack{d|k \\ d\leq u}} \mu(d)\Phi(k,l) = \sum_{d\leq u} \sum_{\substack{k=1 \\ d|k}}^{N} \sum_{u<l\leq N/k} \mu(d)\Phi(k,l) =$$

$$\sum_{d\leq u} \sum_{m\leq N/d} \sum_{u<l\leq N/(dm)} \mu(d)\Phi(dm,l) = \sum_{d\leq u} \sum_{u<l\leq N/d} \sum_{m\leq N/dl} \mu(d)\Phi(dm,l),$$

dove nel penultimo passaggio abbiamo semplicemente imposto ad m le condizioni precedenti su k e nell'ultimo abbiamo scambiato la posizione di m ed l senza alterare la somma, preservando il fatto che $lm < N/d$. □

Lemma 5.12 *Sia $\Lambda(l)$ la funzione di von Mangoldt, introdotta con la Definizione 2.15. Per ogni α*

$$F(\alpha) = S_1 - S_2 - S_3 + \mathcal{O}(N^{1/2}),$$

dove

$$S_1 = \sum_{d\leq N^{2/5}} \sum_{l\leq \frac{N}{d}} \sum_{m\leq \frac{N}{ld}} \mu(d)\Lambda(l)e(\alpha dlm)$$

$$S_2 = \sum_{d\leq N^{2/5}} \sum_{l\leq N^{2/5}} \sum_{m\leq \frac{N}{ld}} \mu(d)\Lambda(l)e(\alpha dlm)$$

$$S_3 = \sum_{k>N^{2/5}} \sum_{N^{2/5}<l\leq \frac{N}{k}} M_{N^{2/5}}(k)\Lambda(l)e(\alpha kl).$$

Dimostrazione: Applichiamo l'identità di Vaughan (Lemma 5.11) con le scelte $u = N^{2/5}$ e

$$\Phi(k,l) = \Lambda(l)e(\alpha kl).$$

Il primo termine dell'identità vale

$$\sum_{u<l\leq N}\Phi(1,l)=\sum_{N^{2/5}<l\leq N}\Lambda(l)e(\alpha l)=\sum_{l=1}^{N}\Lambda(l)e(\alpha l)-\sum_{l\leq N^{2/5}}\Lambda(l)e(\alpha l)=$$

$$\sum_{p^k\leq N}(\log p)e(\alpha p^k)+\mathcal{O}(N^{2/5}\log N)=\sum_{p\leq N}(\log p)e(\alpha p)+\sum_{\substack{p^k\leq N\\ k\geq 2}}(\log p)e(\alpha p^k)+\mathcal{O}(N^{2/5}\log N)=$$

$$=F(\alpha)+\mathcal{O}\left(\sum_{\substack{p^k\leq N\\ k\geq 2}}\log p\right)+\mathcal{O}(N^{2/5}\log N)=$$

$$=F(\alpha)+\mathcal{O}\left(\sum_{p^2\leq N}\left[\frac{\log N}{\log p}\right]\log p\right)+\mathcal{O}(N^{2/5}\log N)=$$

$$F(\alpha)+\mathcal{O}(\pi(N^{1/2})\log N)+\mathcal{O}(N^{2/5}\log N)=F(\alpha)+\mathcal{O}(N^{1/2}),$$

dato che, per il Teorema 2.12,

$$\sum_{p^2<N}1=\pi(N^{1/2})\ll\frac{N^{1/2}}{\log N}.$$

Il secondo termine, dopo le sostituzioni, vale già

$$\sum_{k>N^{2/5}}\sum_{N^{2/5}<l\leq\frac{N}{k}}M_{N^{2/5}}(k)\Lambda(l)e(\alpha kl)=S_3.$$

Il terzo temine invece vale

$$\sum_{d\leq N^{2/5}}\sum_{N^{2/5}<l\leq\frac{N}{d}}\sum_{m\leq\frac{N}{ld}}\mu(d)\Lambda(l)e(\alpha ldm)=$$

$$\sum_{d\leq N^{2/5}}\sum_{l\leq\frac{N}{d}}\sum_{m\leq\frac{N}{ld}}\mu(d)\Lambda(l)e(\alpha dlm)-\sum_{d\leq N^{2/5}}\sum_{l\leq N^{2/5}}\sum_{m\leq\frac{N}{ld}}\mu(d)\Lambda(l)e(\alpha dlm)=$$

$$=S_1-S2.$$

□

Lemma 5.13 *Se a,q sono interi tali che $1\leq q\leq N$, $(a,q)=1$ e*

$$\left|\alpha-\frac{a}{q}\right|\leq\frac{1}{q^2}$$

allora

$$|S_1|\ll\left(\frac{N}{q}+N^{2/5}+q\right)(\log N)^2.$$

Dimostrazione: Indichiamo come prima $u=N^{2/5}$. Dato che, se $r=\prod p_i^{k_i}$,

$$\sum_{l|r}\Lambda(l)=\sum_{p|r}k_i\log p_i=\sum_{p|r}\log p_i^{k_i}=\log r$$

abbiamo, riordinando le somme e ponendo $r=lm$

$$S_1=\sum_{d\leq u}\sum_{l\leq\frac{N}{d}}\sum_{m\leq\frac{N}{ld}}\mu(d)\Lambda(l)e(\alpha dlm)=$$

$$=\sum_{d\leq u}\sum_{lm\leq\frac{N}{d}}\mu(d)\Lambda(l)e(\alpha dlm)=\sum_{d\leq u}\sum_{r\leq\frac{N}{d}}\mu(d)e(\alpha dr)\sum_{l|r}\Lambda(l)=$$

$$=\sum_{d\leq u}\mu(d)\sum_{r\leq\frac{N}{d}}e(\alpha dr)\log r\ll\sum_{d\leq u}\left|\sum_{r\leq\frac{N}{d}}e(\alpha dr)\log r\right|.$$

Valutiamo la somma all'interno del modulo. Riscrivendo il logaritmo in forma integrale e scambiando integrali e somme otteniamo

$$\sum_{r\leq \frac{N}{d}} e(\alpha dr)\log r = \sum_{r\leq \frac{N}{d}} e(\alpha dr)\int_1^r \frac{dx}{x} =$$

$$\sum_{r=2}^{[N/d]} e(\alpha dr)\sum_{s=2}^{r}\int_{s-1}^{s}\frac{dx}{x} = \sum_{r=2}^{[N/d]}\sum_{s=2}^{r}\int_{s-1}^{s} e(\alpha dr)\frac{dx}{x} =$$

$$= \sum_{s=2}^{[N/d]}\sum_{r=s}^{[N/d]}\int_{s-1}^{s} e(\alpha dr)\frac{dx}{x} = \sum_{s=2}^{[N/d]}\int_{s-1}^{s}\left(\sum_{r=s}^{[N/d]} e(\alpha dr)\right)\frac{dx}{x}.$$

Lo scambio di indici tra r ed s mantiene le somme inalterate, andando a sommare sui punti a coordinate intere del piano (r,s) tra la retta $r=s$ e quella $s=2$ (nel quadrante positivo). Grazie al Lemma 1.45 abbiamo

$$\sum_{r=s}^{[N/d]} e(\alpha dr) \ll \min\left(\frac{N}{d}, \|\alpha d\|^{-1}\right)$$

che non dipende da s, quindi sostituendo e portando fuori otteniamo

$$\sum_{r\leq \frac{N}{d}} e(\alpha dr)\log r \ll \min\left(\frac{N}{d}, \|\alpha d\|^{-1}\right)\sum_{s=2}^{[N/d]}\int_{s-1}^{s}\frac{dx}{x} \ll \min\left(\frac{N}{d}, \|\alpha d\|^{-1}\right)\log N.$$

Grazie al Lemma 1.48, che possiamo applicare per ipotesi,

$$\sum_{d\leq u}\min\left(\frac{N}{d}, \|\alpha d\|^{-1}\right) \ll \left(\frac{N}{q}+u+q\right)\log N$$

e quindi in conclusione

$$S_1 \ll \sum_{d\leq u}\min\left(\frac{N}{d}, \|\alpha d\|^{-1}\right)\log N \ll \left(\frac{N}{q}+N^{2/5}+q\right)(\log N)^2.$$

□

Lemma 5.14 *Se a, q sono interi tali che $1\leq q\leq N$, $(a,q)=1$ e*

$$\left|\alpha-\frac{a}{q}\right| \leq \frac{1}{q^2}$$

allora

$$|S_2| \ll \left(\frac{N}{q}+N^{4/5}+q\right)(\log N)^2.$$

Dimostrazione: Se $d\leq N^{2/5}$ e $l\leq N^{2/5}$, $dl\leq N^{4/5}$. Ponendo $k=dl$ abbiamo

$$S_2 = \sum_{d\leq N^{2/5}}\sum_{l\leq N^{2/5}}\sum_{m\leq \frac{N}{ld}}\mu(d)\Lambda(l)e(\alpha dlm) =$$

$$= \sum_{k\leq N^{4/5}}\left(\sum_{m\leq \frac{N}{k}} e(\alpha km)\right)\left(\sum_{\substack{k=dl\\ d,l\leq N^{2/5}}}\mu(d)\Lambda(l)\right)$$

dato che in questo modo il termine all'interno dell'esponenziale non dipende singolarmente ne da l ne da d. Ma

$$\sum_{\substack{k=dl\\ d,l\leq N^{2/5}}}\mu(d)\Lambda(l) \ll \sum_{\substack{k=dl\\ d,l\leq N^{2/5}}}\Lambda(l) \leq \sum_{l|k}\Lambda(l) = \log k \ll \log N,$$

sfruttando nel penultimo passaggio l'uguaglianza osservata nel Lemma precedente. Seguendo sempre i passaggi della dimostrazione precedente, applicando in sequenza i Lemmi 1.45 e 1.48, in questo caso con $U=N^{4/5}$, otteniamo

$$S_2 \ll \log N\sum_{k\leq N^{4/5}}\sum_{m\leq N/k} e(\alpha km) \ll$$

$$\ll \sum_{k\leq N^{4/5}}\min\left(\frac{N}{k}, \|\alpha k\|^{-1}\right)\log N \ll \left(\frac{N}{q}+N^{4/5}+q\right)(\log N)^2.$$

□

Lemma 5.15 *Se a, q sono interi tali che $1 \leq q \leq N$, $(a,q) = 1$ e*

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$$

allora

$$|S_3| \ll \left(\frac{N}{q^{1/2}} + N^{4/5} + N^{1/2}q^{1/2}\right)(\log N)^4.$$

Dimostrazione: Poniamo $u = N^{2/5}$ e

$$h = \left[\frac{\log N}{5\log 2}\right] + 1.$$

Dato che

$$2^{\frac{\log N}{5\log 2}} = e^{\frac{\log N}{5\log 2}\log 2} = N^{1/5}$$

abbiamo

$$N^{1/5} = 2^{\frac{\log N}{5\log 2}} < 2^h \leq 2 \cdot 2^{\frac{\log N}{5\log 2}} = 2N^{1/5.}$$

Inoltre $h \ll \log N$. Se $i \leq h$, $2^i u \leq 2N^{3/5} \ll N$. Se $N^{2/5} < l \leq N/k$, allora

$$k \leq N/l < N^{3/5} = N^{1/5}u < 2^h u.$$

Utilizzando questa stima possiamo scrivere

$$S_3 = \sum_{k > N^{2/5}} \sum_{N^{2/5} < l \leq \frac{N}{k}} M_{N^{2/5}}(k)\Lambda(l)e(\alpha kl) = \sum_{k>u} M_u(k) \sum_{u < l \leq \frac{N}{k}} \Lambda(l)e(\alpha kl)$$
$$= \sum_{i=1}^{h} \sum_{2^{i-1}u < k \leq 2^i u} M_u(k) \sum_{u < l \leq \frac{N}{k}} \Lambda(l)e(\alpha kl)$$

dal momento che k parte da u come prima, e si ferma a $2^h u$, termine oltre il quale la somma interna era vuota. Definendo

$$S_{3,i} = \sum_{2^{i-1}u < k \leq 2^i u} M_u(k) \sum_{u < l \leq \frac{N}{k}} \Lambda(l)e(\alpha kl)$$

abbiamo

$$S_3 = \sum_{i=1}^{h} S_{3,i}.$$

Applicando Chauchy-Schwarz alla somma $S_{3,i}$ otteniamo

$$|S_{3,i}|^2 \leq \sum_{2^{i-1}u < k \leq 2^i u} |M_u(k)|^2 \cdot \sum_{2^{i-1}u < k \leq 2^i u} \left|\sum_{u < l \leq \frac{N}{k}} \Lambda(l)e(\alpha kl)\right|^2. \tag{17}$$

Per quanto riguarda la prima somma, osserviamo che

$$|M_u(k)| = \left|\sum_{\substack{d|k \\ d \leq u}} \mu(d)\right| \leq \sum_{\substack{d|k \\ d \leq u}} 1 \leq d(k),$$

dove l'ultima d indica la funzione divisore. Applicando il Teorema 1.17 e ricordando che, come osservato a inizio dimostrazione, $2^i u \ll N$, abbiamo

$$\sum_{2^{i-1}u < k \leq 2^i u} |M_u(k)|^2 \leq \sum_{2^{i-1}u < k \leq 2^i u} d(k)^2 \ll$$
$$\ll 2^i u(\log 2^i u)^3 \ll 2^i u(\log N)^3.$$

Stimiamo ora la seconda somma. Svolgendo il prodotto scalare abbiamo

$$\sum_{2^{i-1}u<k\leq 2^i u}\left|\sum_{u<l\leq \frac{N}{k}}\Lambda(l)e(\alpha kl)\right|^2 =$$
$$\sum_{2^{i-1}u<k\leq 2^i u}\sum_{u<l\leq \frac{N}{k}}\sum_{u<m\leq \frac{N}{k}}\Lambda(l)\Lambda(m)e(\alpha k(l-m)) =$$
$$\sum_{u<l<\frac{N}{2^{i-1}u}}\sum_{u<m<\frac{N}{2^{i-1}u}}\Lambda(l)\Lambda(m)\sum_{k\in I(l,m)}e(\alpha k(l-m)),$$

definendo $I(l,m)$ come l'intervallo degli interi consecutivi k tali che

$$2^{i-1}u < k \leq \min\left(2^i u, \frac{N}{l}, \frac{N}{m}\right).$$

Infatti se consideriamo la somma nel penultimo passaggio $l, m < N/k$ e $k > 2^{i-1}u$, e allora certamente $l, m < N/2^{i-1}u$. Inoltre k è minore dei tre termini utilizzati nel minimo. Viceversa nell'ultima somma $l, m \leq N/k$ grazie alle condizioni imposte su k, mentre l'intervallo iniziale di k è certamente rispettato. Ora dato che $2^{i-1}u < k \leq 2^i u$ abbiamo $|I(l,m)| \leq 2^{i-1}u$ e quindi, per il Lemma 1.45

$$\sum_{k\in I(l,m)} e(\alpha k(l-m)) \ll \min(2^{i-1}u, \|\alpha(l-m)\|^{-1}).$$

Inoltre chiaramente $0 \leq \Lambda(l), \Lambda(m) \leq \log N$ per $l, m \in [1, N]$ e quindi

$$\sum_{2^{i-1}u<k\leq 2^i u}\left|\sum_{u<l\leq \frac{N}{k}}\Lambda(l)e(\alpha kl)\right|^2 \ll$$
$$\ll \sum_{u<l<\frac{N}{2^{i-1}u}}\sum_{u<m<\frac{N}{2^{i-1}u}}\Lambda(l)\Lambda(m)\min(2^{i-1}u, \|\alpha(l-m)\|^{-1}) \ll$$
$$\ll (\log N)^2 \sum_{u<l<\frac{N}{2^{i-1}u}}\sum_{u<m<\frac{N}{2^{i-1}u}}\min(2^{i-1}u, \|\alpha(l-m)\|^{-1})$$

Indichiamo ora $j = l - m$. Dato che $u < l, m < N/(2^{i-1}u)$, anche $|j| < N/(2^{i-1}u)$ e ognuno di questi j sarà ottenuto da al più $N/(2^{i-1}u)$ coppie (l, m). Sfruttando questo fatto e applicando poi il Lemma 1.48 con ovvie scelte di n e di U otteniamo

$$(\log N)^2 \sum_{u<l<\frac{N}{2^{i-1}u}}\sum_{u<m<\frac{N}{2^{i-1}u}}\min(2^{i-1}u, \|\alpha(l-m)\|^{-1}) \ll$$
$$\ll (\log N)^2 \frac{N}{2^{i-1}u}\sum_{1\leq j\leq \frac{N}{2^{i-1}u}}\min(2^{i-1}u, \|\alpha j\|^{-1}) \ll$$
$$\ll (\log N)^2 \frac{N}{2^{i-1}u}\sum_{1\leq j\leq \frac{N}{2^{i-1}u}}\min(\frac{N}{j}, \|\alpha j\|^{-1}) \ll$$
$$\ll \frac{N}{2^{i-1}u}\left(\frac{N}{q} + \frac{N}{2^{i-1}u} + q\right)(\log N)^3.$$

Inserendo ora le stime ottenute nella (17) abbiamo

$$|S_{3,i}|^2 \ll (2^i u(\log N)^3)\frac{N}{2^{i-1}u}\left(\frac{N}{q} + \frac{N}{2^{i-1}u} + q\right)(\log N)^3 \ll$$
$$\ll N^2(\log N)^6\left(\frac{1}{q} + \frac{1}{u} + \frac{q}{N}\right).$$

Quindi, ricordando che $u = N^{2/5}$,

$$|S_{3,i}| \ll N(\log N)^3\left(\frac{1}{q^{1/2}} + \frac{1}{N^{1/5}} + \frac{q^{1/2}}{N^{1/2}}\right).$$

Sommando tutti questi termini, dato che $h \ll \log N$, abbiamo in conclusione

$$S_3 = \sum_{i=1}^{h} S_{3,i} \ll (\log N)^4 \left(\frac{N}{q^{1/2}} + N^{4/5} + q^{1/2} N^{1/2} \right).$$

□

Teorema 5.16 (Vinogradov) *Se a, q sono interi tali che $1 \leq q \leq N$, $(a,q) = 1$ e*

$$\left| \alpha - \frac{a}{q} \right| \leq \frac{1}{q^2}$$

allora

$$F(\alpha) \ll \left(\frac{N}{q^{1/2}} + N^{4/5} + N^{1/2} q^{1/2} \right) (\log N)^4.$$

Dimostrazione: È sufficiente inserire nel Lemma 5.12 le stime per S_1(Lemma 5.13), S_2(Lemma 5.14) e S_3(Lemma 5.15). Ricordando che $q \leq N$, la tesi segue scartando i termini di ordine inferiore. □

Teorema 5.17 *Per ogni $B > 0$ vale*

$$\int_{\mathfrak{m}} F(\alpha)^3 e(-\alpha N) d\alpha \ll \frac{N^2}{(\log N)^{(B/2)-5}},$$

dove la costante dipende solo da B.

Dimostrazione: Prendiamo $\alpha \in \mathfrak{m} = [0,1] \backslash \mathfrak{M}$. Il Teorema 1.43, applicato ad α e N/Q, garantisce l'esistenza di due interi $1 \leq q \leq N/Q$ e $1 \leq a \leq q$ tali che $(a,q) = 1$ e

$$\left| \alpha - \frac{a}{q} \right| \leq \frac{Q}{qN} \leq \min \left(\frac{Q}{N}, \frac{1}{q^2} \right)$$

grazie alle condizioni su q. Ora se fosse $q \leq Q$, per definizione $\alpha \in \mathfrak{M}(q,a)$, che è assurdo dato che abbiamo preso $\alpha \in \mathfrak{m}$. Avremo quindi $Q < q \leq N/Q$. Applicando il Teorema 5.16, e ricordando che abbiamo posto $Q = (\log N)^B$, otteniamo

$$\begin{gathered} F(\alpha) \ll \left(\frac{N}{q^{1/2}} + N^{4/5} + N^{1/2} q^{1/2} \right) (\log N)^4 \ll \\ \ll \left(\frac{N}{(\log N)^{B/2}} + N^{4/5} + N^{1/2} \left(\frac{N}{(\log N)^B} \right)^{1/2} \right) (\log N)^4 \ll \\ \ll \frac{N}{(\log N)^{(B/2)-4}}. \end{gathered}$$

Per il Teorema 2.12

$$\vartheta(N) = \sum_{p \leq N} \log p \ll N$$

e quindi, per definizione di F,

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

In conclusione

$$\begin{gathered} \int_{\mathfrak{m}} |F(\alpha)|^3 d\alpha \ll \sup\{|F(\alpha)| : \alpha \in \mathfrak{m}\} \int_{\mathfrak{m}} |F(\alpha)|^2 d\alpha \ll \\ \ll \frac{N}{(\log N)^{(B/2)-4}} \int_0^1 |F(\alpha)|^2 d\alpha \ll \frac{N^2}{(\log N)^{(B/2)-5}}. \end{gathered}$$

□

5.5 Teorema di Vinogradov

Teorema 5.18 *Sia $\mathfrak{S}(N)$ la serie singolare. Per N dispari sufficientemente grande e per ogni $A > 0$*

$$R(N) = \mathfrak{S}(N)\frac{N^2}{2} + \mathcal{O}\left(\frac{N^2}{(\log N)^A}\right),$$

dove la costante dipende solo da A.

Dimostrazione: Grazie ai Teoremi 5.10 e 5.17 otteniamo, per ogni scelta di B, C ed ϵ positivi tali che $C > 2B$,

$$R(N) = \int_0^1 F(\alpha)^3 e(-N\alpha)d\alpha =$$
$$\int_{\mathfrak{M}} F(\alpha)^3 e(-N\alpha)d\alpha + \int_{\mathfrak{m}} F(\alpha)^3 e(-N\alpha)d\alpha =$$
$$\mathfrak{S}(N)\frac{N^2}{2} + \mathcal{O}\left(\frac{N^2}{(\log N)^{(1-\epsilon)B}}\right) + \mathcal{O}\left(\frac{N^2}{(\log N)^{C-5B}}\right) + \mathcal{O}\left(\frac{N^2}{(\log N)^{(B/2)-5}}\right)$$

dove le costanti dipendono solo da B, C ed ϵ. Dato $A > 0$ scegliamo $B = 2A + 10$, $C = A + 5B$ e $\epsilon = 1/2$. La scelta è accettabile dato che chiaramente $C > 2B$ e inoltre

$$\min((1-\epsilon)B, C - 5B, (B/2) - 5) = A.$$

Abbiamo quindi la tesi

$$R(N) = \mathfrak{S}(N)\frac{N^2}{2} + \mathcal{O}\left(\frac{N^2}{(\log N)^A}\right).$$

□

Teorema 5.19 (Vinogradov) *Sia $r(N)$ il numero di rappresentazioni di un intero dispari N come somma di tre primi, ovvero*

$$r(N) = \sum_{p_1+p_2+p_3=N} 1.$$

Allora

$$r(N) = \mathfrak{S}(N)\frac{N^2}{2(\log N)^3}\left(1 + \mathcal{O}\left(\frac{\log\log N}{\log N}\right)\right).$$

Dimostrazione: Stimando $R(N)$ dall'alto abbiamo

$$R(N) = \sum_{p_1+p_2+p_3=N} \log p_1 \log p_2 \log p_3 \leq$$
$$\leq (\log N)^3 \sum_{p_1+p_2+p_3=N} 1 = (\log N)^3 r(N).$$

Fissato $0 < \delta < 1/2$, indichiamo con $r_\delta(N)$ il numero di rappresentazioni di $N = p_1 + p_2 + p_3$ tali che per almeno uno dei p_i valga $p_i \leq N^{1-\delta}$. Allora

$$r_\delta(N) \leq 3 \sum_{\substack{p_1+p_2+p_3=N \\ p_1 \leq N^{1-\delta}}} \ll \sum_{p_1 \leq N^{1-\delta}} \left(\sum_{p_2+p_3=N-p_1} 1\right) \leq$$
$$\leq \sum_{p_1 \leq N^{1-\delta}} \left(\sum_{p_2<N} 1\right) \leq \pi(N^{1-\delta})\pi(N) \ll \frac{N^{2-\delta}}{(\log N)^2}$$

grazie al Teorema 2.12. Possiamo ora stimare dal basso $R(N)$, considerando solo le rappresentazioni in cui tutti i primi coinvolti siano maggiori di $N^{1-\delta}$, ovvero l'insieme di rappresentazioni complementare a quello di cui abbiamo stimato la grandezza con $r_\delta(N)$.

$$R(N) \geq \sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3>N^{1-\delta}}} \log p_1 \log p_2 \log p_3 \geq (1-\delta)^3(\log N)^3 \sum_{\substack{p_1+p_2+p_3=N \\ p_1,p_2,p_3>N^{1-\delta}}} 1 \geq$$
$$\geq (1-\delta)^3(\log N)^3(r(N) - r_\delta(N)) \gg (1-\delta)^3(\log N)^3\left(r(N) - \frac{N^{2-\delta}}{(\log N)^2}\right),$$

ovvero

$$(\log N)^3 r(N) \ll (1-\delta)^{-3} R(N) + (\log N) N^{2-\delta}.$$

Avendo preso per ipotesi $0 < \delta < 1/2$, abbiamo $1/2 < 1-\delta < 1$ e quindi

$$0 < (1-\delta)^{-3} - 1 = \frac{1-(1-\delta)^3}{(1-\delta)^3} \leq 8(1-(1-\delta)^3) < 24\delta.$$

Grazie al Teorema 5.18, e ricordando che $\mathfrak{S}(N)$ è limitata da due costanti grazie al Teorema 5.4, $R(N) \ll N^2$ e quindi

$$0 \leq (\log N)^3 r(N) - R(N) \ll ((1-\delta)^{-3} - 1) R(N) + (\log N) N^{2-\delta} \ll$$
$$\ll \delta R(N) + (\log N) N^{2-\delta} \ll \delta N^2 + (\log N) N^{2-\delta} = N^2 \left(\delta + \frac{\log N}{N^\delta} \right)$$

per ogni $\delta \in (0, 1/2)$. Inoltre le costanti non dipendono da δ. Fissiamo allora

$$\delta = \frac{2 \log\log N}{\log N} \in (0, 1/2)$$

per N sufficientemente grande. Dato che

$$N^{\frac{2\log\log N}{\log N}} = e^{\frac{2\log\log N}{\log N} \log N} = (\log N)^2$$

abbiamo

$$\delta + \frac{\log N}{N^\delta} = \frac{2\log\log N}{\log N} + \frac{\log N}{(\log N)^2} \ll \frac{\log\log N}{\log N}$$

e quindi

$$0 \leq (\log N)^3 r(N) - R(N) \ll \frac{N^2 \log\log N}{\log N}.$$

Applicando il Teorema 5.18 con $A \geq 1$ otteniamo

$$(\log N)^3 r(N) = R(N) + \mathcal{O}\left(\frac{N^2 \log\log N}{\log N} \right) =$$
$$\mathfrak{S}(N) \frac{N^2}{2} + \mathcal{O}\left(\frac{N^2}{(\log N)^A} \right) + \mathcal{O}\left(\frac{N^2 \log\log N}{\log N} \right) = \mathfrak{S}(N) \frac{N^2}{2} \left(1 + \mathcal{O}\left(\frac{\log\log N}{\log N} \right) \right)$$

e quindi, dividendo per $(\log N)^3$, abbiamo la tesi

$$r(N) = \mathfrak{S}(N) \frac{N^2}{2(\log N)^3} \left(1 + \mathcal{O}\left(\frac{\log\log N}{\log N} \right) \right).$$

□

References

[1] Chris Caldwell. *Prime Pages - Goldbach's Conjecture*. 2020. URL: https://primes.utm.edu/glossary/page.php?sort=GoldbachConjecture.

[2] Harold Davenport. *Multiplicative Number Theory*. 1971.

[3] Gianni Gilardi. *Analisi 3*. 2003.

[4] H. A. Helfgott. "Major arcs for Goldbach's problem". In: *arXiv:1305.2897* (2013).

[5] H. A. Helfgott. "Minor arcs for Goldbach's problem". In: *arXiv:1205.5252* (2012).

[6] H. A. Helfgott. "The ternary Goldbach problem". In: *arXiv:1501.05438* (2015).

[7] Melvyn B. Nathanson. *Additive Number Theory - The Classical Bases*. Ed. by Springer. 1996.