

# Contents

Introduction . . . . .	IV
<b>1 Analytic Number Theory Classic Results</b>	<b>1</b>
1.1 Arithmetical Functions . . . . .	1
1.1.1 Arithmetic Functions and Dirichlet Product . . . . .	1
1.1.2 Fundamental Identities : functions $\mu, \phi, \Lambda$ . . . . .	3
1.1.3 Dirichlet series. . . . .	5
1.1.4 Euler products. . . . .	9
1.2 Riemann $\zeta$ function . . . . .	12
1.2.1 Riemann $\zeta$ function . . . . .	12
1.2.2 Functional Equation for the $\zeta$ . . . . .	14
1.2.3 Riemann Hypotesis . . . . .	16
1.2.4 Zero-free Regions . . . . .	17
1.2.5 Zero-Density Estimates . . . . .	18
1.3 Dirichlet's $L$ -functions . . . . .	20
1.3.1 Dirichlet's $L$ -functions . . . . .	20
1.3.2 Functional Equation of the $L(s, \chi)$ . . . . .	20
1.3.3 Generalized Riemann Hypotesis and Siegel's Theorem	22
1.3.4 Zero-free Regions . . . . .	22
1.3.5 Zero Density Estimates . . . . .	23
1.4 Explicit Formulae . . . . .	24
1.4.1 Perron's Formula . . . . .	24
1.4.2 Riemann – von Mangoldt's Explicit Formula . . . . .	24
1.4.3 (Classic) Explicit Formula for $\psi(x, \chi)$ . . . . .	25
<b>2 Multiplicative Problems</b>	<b>27</b>
2.1 Multiplicative Problems . . . . .	27
2.2 Prime Number Theorem . . . . .	29
2.2.1 Function $\pi$ and Cebecev estimates . . . . .	29
2.2.2 Cebecev's functions $\psi$ and $\theta$ . . . . .	30
2.2.3 Prime Number Theorem . . . . .	32

2.3	Primes in Short Intervals . . . . .	36
2.4	Primes in the Arithmetic Progressions . . . . .	38
2.4.1	Arithmetic Progressions and Additive Characters . . . . .	38
2.4.2	Multiplicative Characters and Dirichlet Theorem . . . . .	39
2.4.3	Prime Number Theorem in the Arithmetic Progressions . . . . .	42
2.5	Bombieri's Theorem . . . . .	43
<b>3</b>	<b>Additive Problems</b>	<b>45</b>
3.1	Additive Problems . . . . .	45
3.2	Goldbach problems . . . . .	47
3.3	Hardy-Littlewood Method . . . . .	49
3.4	Vinogradov's Method . . . . .	51
3.5	Three-Primes Theorem . . . . .	52
3.6	Circle Method and Goldbach Problem . . . . .	56
<b>4</b>	<b>Sieves and Exponential Sums</b>	<b>59</b>
4.1	Sieves and Exponential Sums . . . . .	59
4.2	Small Sieve . . . . .	61
4.2.1	Eratosthenes-Legendre Sieve . . . . .	61
4.2.2	Combinatorial Sieve . . . . .	67
4.2.3	Selberg sieve . . . . .	70
4.3	Large Sieve . . . . .	73
4.4	Dispersion Method . . . . .	76
4.5	Exponential Sums . . . . .	78
4.6	Bilinear Forms . . . . .	79
4.7	Kloosterman Sums . . . . .	80
<b>5</b>	<b>Short Intervals Problems</b>	<b>81</b>
5.1	Short Intervals Problems . . . . .	81
5.2	Primes in almost all the Short Intervals . . . . .	83
5.2.1	Introduction and statement of the results . . . . .	83
5.2.2	Statement and Proof of Lemma 1 . . . . .	87
5.3	Goldbach Problem with almost equal primes . . . . .	90
5.3.1	Notations . . . . .	92
5.3.2	Sketch of the Proof . . . . .	93
5.3.3	Major Arcs Estimates . . . . .	93
5.3.4	Minor Arcs Estimates . . . . .	95
5.4	Large Sieve and $n(n+2)$ in short intervals . . . . .	98
5.4.1	Statement of the results . . . . .	98
5.4.2	Proof of the Theorem and of the Corollaries . . . . .	100
5.4.3	A variant of the Large Sieve . . . . .	103
5.5	Dispersion Method and $n(n+2)$ in short intervals . . . . .	106

*CONTENTS*

III

5.5.1	Statement of the results . . . . .	106
5.5.2	Proof of the Theorem . . . . .	107
5.6	Kloosterman Sums and $n(n+2)$ in short intervals . . . . .	111
5.6.1	Statement of the results . . . . .	111
5.6.2	Estimates of the fractional parts with Kloosterman sums . . . . .	112

## Introduction

The thesis introduces the main results of the Author regarding multiplicative and additive problems in short intervals, in the general setting of Analytic Number Theory.

In **Chapter 1** we recall the main “**classical**” results of Analytic Number Theory (abbrev. A.N.T.), **about : arithmetical functions, Dirichlet series, Euler products, Riemann’s  $\zeta$  function and Dirichlet’s  $L$ -functions.**

In **Chapter 2** we give the main **multiplicative problems** (i.e., those regarding the integers’ multiplicative structure) **and**, in particular, the problem of **prime numbers distribution** (in particular, in the arithmetic progressions).

In **Chapter 3** we give some of the main **additive problems** (i.e., those regarding the integers’ additive structure) **and**, in particular, **Goldbach’s problems and** one of the most important techniques used in this case, called **the Circle Method**.

In **Chapter 4** we expose something about **Sieve Methods, Exponential Sums and Bilinear Forms**; these are among the most powerful “modern” techniques of Analytic Number Theory.

Finally, in **Chapter 5** we show the **original results about particular additive and multiplicative problems in short intervals**, i.e. in those intervals whose length is much smaller (e.g., is  $o$ ) than their endpoints (see the following for the exact definition). In particular:

- **as for multiplicative problems** we get results about the **primes “in almost all short intervals” and the distribution in the arithmetic progressions of  $n(n+2)$  in the short intervals**;

- **as for additive problems** we get results about **Goldbach’s binary problem with “almost equal” primes**, i.e. with two primes from a short interval.

# Chapter 1

## Analytic Number Theory Classic Results

### 1.1 Arithmetical Functions

#### 1.1.1 Arithmetic Functions and Dirichlet Product

We call **arithmetic function** any function  $f : \mathbf{N} \rightarrow \mathbf{C}$ ; the set  $\mathcal{A}$  of arithmetic functions, with the operations:

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

(**sum**)

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

(**scalar multiplication**)

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

(**Dirichlet product**)

is a commutative algebra over  $\mathbf{C}$ , whose identity is the function  $\mathbf{e} : \mathbf{N} \rightarrow \mathbf{C}$ , defined by

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

We say that  $f \in \mathcal{A}$  is **multiplicative** if:

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

while it is **completely multiplicative** when:

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

It follows from these definitions that the multiplicative functions are determined by their values on the powers of primes, while to get the completely multiplicative  $f$  it suffices to know  $f(p)$ , for all primes  $p$ .

The Dirichlet product (or **convolution product**), multiplicative and completely multiplicative functions have an essential role in the theory of Dirichlet series and Euler products, as it will be clear in the following.

Let's denote with  $\mathcal{M}$  the set of multiplicative functions and with  $\mathcal{U}$  the set of unities, i.e. the **invertible elements** in  $\mathcal{A}$  **w.r.t. the Dirichlet product**.

The  $f \in \mathcal{U}$  are characterized by the condition: " $f(1)$  doesn't vanish" and it's easy to prove the:

**Theorem 1.1.**  $\mathcal{M}$  is a subgroup of  $\mathcal{U}$  (w.r.t.  $*$ ).

From this it follows that the Dirichlet product of two multiplicative functions is multiplicative (while, in general,  $f * g$  is **not completely multiplicative** when  $f$  and  $g$  are completely multiplicative).

Another remarkable property of the multiplicative functions is given by:

**Theorem 1.2.** If  $f$  is multiplicative then:

$$f \text{ is completely multiplicative} \Leftrightarrow f^{-1}(n) = \mu(n)f(n) \quad \forall n \in \mathbf{N}$$

( $f^{-1}$  stands for the inverse of  $f$  w.r.t.  $*$ ).

We say that a function  $f \in \mathcal{A}$  is **additive** when:

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

while we call it **completely additive** when:

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

In both the last two cases  $f$  is a non-invertible arithmetical function, since  $f(1) = 0$  (that's easy to verify from the definitions).

If we define the **ordinary product** between functions in  $\mathcal{A}$  :

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

we have that,  $\forall h$  completely additive, the map  $f \rightarrow hf$  is a derivation in the algebra  $\mathcal{A}$  .

In particular we can choose  $h(n) = -\log(n)$  (i.e.  $h = -\mathbf{L}$ , see §1.1.3).

### 1.1.2 Fundamental Identities : functions $\mu, \phi, \Lambda$ .

Define  $\mu \in \mathcal{A}$  , the **Möbius function** as:

$$\mu(n) \stackrel{def}{=} \begin{cases} 1 & \text{if } n = 1 \\ (-1)^r & \text{if } n \text{ is the product of } r \text{ distinct primes,} \\ 0 & \text{otherwise,} \end{cases}$$

that is clearly multiplicative (but not completely multiplicative) and satisfies the identity:

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

which, on defining the **constant-one function**:

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

may be expressed saying that  $\mu$  is the inverse (w.r.t.  $*$ ) of  $\mathbf{1}$  :

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

Thanks to this last equation we can obtain the:

**MÖBIUS INVERSION FORMULA.** If  $f, g \in \mathcal{A}$  then:

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

or, in short form:

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

(The proof follows immediately from 1.2).

Let's define, now, the **Euler totient function**  $\phi$ :

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

and the **identity function**:

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

that have the property:

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

in fact  $\mu, I \in \mathcal{M}$  and by Theorem 1.1  $\phi$  is multiplicative; hence it's given by the values  $\phi(p^\alpha)$ , for  $\alpha \geq 0$ ;  $\phi(1) = 1$  and ( $\mathbf{P}$  is the **set of primes**):

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

from which we have (the product is over all the prime divisors of  $n$ ):

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

From 1.3, multiplying (with  $*$ ) both the sides by  $\mathbf{1}$ , we also have:

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

Furthermore, we have the following property of multiplicative functions

**PROPOSITION 1.1.** *Let  $f \in \mathcal{M}$ . Then*

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

A very important arithmetic function in A.N.T. is the **von Mangoldt function**  $\Lambda$ :

$$\Lambda(n) \stackrel{def}{=} \begin{cases} \log p & \text{if } n = p^\alpha, \text{ for some } \alpha \in \mathbf{N}, \\ 0 & \text{otherwise.} \end{cases}$$

that in §2.2.2 will be a good substitute for the characteristic function of primes; and it also has the remarkable property:

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

where " $\mathbf{L}$ " is the usual logarithmic function (in base  $e \approx 2.718\dots$ ), but with domain restricted to  $\mathbf{N}$  (so that  $\mathbf{L} \in \mathcal{A}$ ); i.e.:

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

The 1.8 is the link between the von Mangoldt function  $\Lambda$  and the Riemann  $\zeta$  function; that's why we can study the distribution of primes using the properties of this function, in particular its zeros distribution.

### 1.1.3 Dirichlet series.

We define the following a **Dirichlet series** (abbrev. **D.s.**) of coefficients  $a(n)$ , with  $a \in \mathcal{A}$  (and  $f$  will be its sum, when it converges):

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

We'll write  $s = \sigma + it$ , with  $\sigma$  and  $t$  real numbers, using a notation that has become standard after Riemann's contributes to the A.N.T.

Let's study, now, the convergence properties of the Dirichlet series at 1.9.

It's easy to prove the:

**Theorem 1.3.** *If  $\sum_{n=1}^{\infty} a(n)n^{-s}$  converges for  $s_0 = \sigma_0 + it_0$ , then:*

*i)  $\sum_{n=1}^{\infty} a(n)n^{-s}$  converges  $\forall s \in \mathbf{C}$  such that  $\sigma > \sigma_0$ ;*

*ii)  $\sum_{n=1}^{\infty} a(n)n^{-s}$  converges uniformly in each compact subset of the halfplane  $\sigma > \sigma_0$ .*

Thanks to Theorem 1.3 we can define the **abscissa of convergence** of a Dirichlet series:

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

and, considering the series  $\sum_{n=1}^{\infty} |a(n)n^{-s}|$  in the same Theorem, the **abscissa of absolute convergence** of a D.s.:

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

From these definitions we get at once (for all D.s.):

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

An example of Dirichlet series with distinct abscissae of convergence is given by:

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

that converges for  $\sigma > 0 = \sigma_c$ , but converges absolutely only for  $\sigma > 1 = \sigma_{ac}$  (in this case we have the biggest distance between  $\sigma_{ac}$  and  $\sigma_c$ , cfr. 1.10).

Let's give a result which will be useful in the following:

**Theorem 1.4 (of UNIQUENESS for DIRICHLET SERIES).**

If  $f(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ ,  $g(s) = \sum_{n=1}^{\infty} b(n)n^{-s}$  (for both  $\sigma_{ac} < \infty$ ) and exists a sequence of complex numbers,  $\{s_k\}$ , such that:

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

then  $a = b$ .

From the Theorem, it follows that every D.s. not identically zero has a **zero-free half-plane**, i.e. an half-plane in which it never vanishes.

Let's state the most interesting Theorem, about D.s.; it links directly the Dirichlet product,  $*$ , (see §1.1.1) with the (usual) product between D.s.:

**Theorem 1.5.** If  $f(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ ,  $g(s) = \sum_{n=1}^{\infty} \frac{b(n)}{n^s}$  and  $\sigma_{ac} < \infty$  for both, then:

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

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

In fact i) says that the product of two absolutely convergent D.s. is a new D.s. with coefficients which are the convolution product of the coefficients of the starting D.s.; ii) is, then, a simple consequence of Theorem 1.4.

The following Theorem gives a sufficient condition for the regularity of the function  $f$  at 1.9 and, also, the explicit expression of  $df/ds$  (we write  $f'(s)$ ):

**Theorem 1.6.** If  $\sigma > \sigma_c$  then:

i) the sum of  $\sum_{n=1}^{\infty} a(n)n^{-s} = f(s)$  is an analytic function;

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

From ii) we see immediately that the choice  $h(n) = -\log n$  we made in §1.1.1 is coherent with the rules to calculate  $f'(s)$  (that we get differentiating term by term).

8 CHAPTER 1. ANALYTIC NUMBER THEORY CLASSIC RESULTS

Let's see some example of D.s. (we abbreviate "assoc." for "associated"):

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

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

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

$$\sum_{n=1}^{\infty} \mu(n)n^{-s} \quad \text{with } \sigma_{ac} = 1 \text{ (D.s. assoc. to Möbius } \mu)$$

$$\sum_{n=1}^{\infty} \phi(n)n^{-s} \quad \text{with } \sigma_{ac} \leq 2 \text{ (D.s. assoc. to Euler's } \phi)$$

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

Using 1.6 and the Theorems 1.3 and 1.5 we get

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

Applying the Theorems 1.2, 1.3 and 1.5 we obtain:

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

whence:

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

By the same Theorems, if  $f(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ :

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

in the halfplane  $\sigma > \sigma_{ac}$ .

Let's apply the Theorems 1.3, 1.5 and 1.6 to get a relation that will be very useful for the following (being the starting point for the proof of the Prime Number Theorem).

If  $\sigma > 1$  then:

$$\begin{aligned}\zeta'(s) &= \text{(by ii) of Theor.1.6)} = - \sum_{n=1}^{\infty} \log(n)n^{-s} = \\ &= \text{(by Theor. 1.5 and 1.7)} = -\zeta(s) \sum_{n=1}^{\infty} \Lambda(n)n^{-s},\end{aligned}$$

from which:

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

We now give a classical result about the singularities of the functions defined by D.s. with positive coefficients, due to Landau (v. [Te], p.110)

**Theorem 1.7.** (E. LANDAU)

If  $\sum_{n=1}^{\infty} a(n)n^{-s}$  has  $\sigma_c < \infty$  and  $\exists n_0$  such that  $a(n) \geq 0 \quad \forall n \geq n_0$ , then the sum  $f(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$  has a singularity in  $\sigma_c$ .

From this Theorem it follows, in particular, that the Riemann  $\zeta$  function has a singularity in  $s = 1$ , likewise the function:

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

(for the proofs of the Theorems in this paragraph see [A], chap. XI; also [Te], Chapter I.2, §2.3 and chap. II.1, §1.1, §1.2, §1.3.)

#### 1.1.4 Euler products.

Let's consider the **infinite product**  $\prod_{n=1}^{\infty} (1 + a(n))$ , with  $a \in \mathcal{A}$ , that is defined as:

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

when this limit exists (if the limit is finite and non zero we say that **the product is convergent**).

Furthermore,  $\prod_{n=1}^{\infty} (1 + a(n))$  **converges absolutely**, by definition, if  $\sum_{n=1}^{\infty} a(n)$  is absolutely convergent.

We'll write  $\prod_p$  to indicate the infinite product over all primes  $p$  (and we'll omit  $p \in \mathbf{P}$ ).

We have the following Theorem :

**Theorem 1.8 (EULER'S IDENTITY).**

Let  $f \in \mathcal{M}$  and  $\sum_{n=1}^{\infty} |f(n)| < \infty$ ; then:

i)  $\sum_{n=1}^{\infty} f(n) = \prod_p (1 + f(p) + f(p^2) + f(p^3) + f(p^4) + \dots)$  and this product converges absolutely;

ii)  $f$  completely multiplicative  $\Rightarrow \sum_{n=1}^{\infty} f(n) = \prod_p (\frac{1}{1-f(p)})$ .

Choosing  $f(n) = a(n)n^{-s}$  in the preceding Theorem we have the remarkable:

**Corollary 1.1. (EULER PRODUCTS)**

If  $a \in \mathcal{M}$  and  $\sigma > \sigma_{ac}$  then :

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

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

In particular, for  $a = \mathbf{1}$ , we get the identity for the Riemann  $\zeta$  function

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

which is called **Euler Identity**, and is the **analytic version of the Fundamental Theorem of Arithmetics**.

Also, for  $a(n) = \chi(n)$ , with  $\chi$  non-principal Dirichlet character (mod  $q$ ) (see §2.4.2)

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

which is instead, for the principal character, (since  $\chi_0(p) = 0 \Leftrightarrow p|q$ , see §2.4.2)

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

whence  $L(s, \chi_0)$  and the Riemann  $\zeta$  function coincide, modulo a finite product (that defines a function, analytic in  $s \in \mathbf{C}$  and depending on the modulo  $q$ ).

## 1.2 Riemann $\zeta$ function

### 1.2.1 Riemann $\zeta$ function

As we saw in §1.1.3, the **Riemann  $\zeta$  function** is defined by:

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

In order to obtain an extension of the  $\zeta$  to other values of  $s \in \mathbf{C}$ , we give an application of the partial summation Lemma 1.1 to the general D.s. (with any coefficients  $a(n)$ ,  $a \in \mathbb{C}$ ):

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

from which, passing to the limit  $x \rightarrow \infty$ , we get:

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

Applying the present formula for  $a = \mathbf{1}$  and  $\sigma > 1$  we obtain ( $[x]$  stands for the **integral part** of  $x$  and  $\{x\} \stackrel{def}{=} x - [x]$  is its **fractional part**):

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

that (since the integral converges  $\forall \sigma > 0$  and uniformly for  $\sigma \geq \delta > 0$ ,  $\forall \delta > 0$ ), gives the **analytic continuation of the Riemann  $\zeta$ -function in the halfplane  $\sigma > 0$  except for the point 1, in which the  $\zeta$  has a simple pole with residue 1.**

In the following we'll see how to extend the  $\zeta$  to all of  $\mathbf{C}$ , except the point 1 (1.19 alone doesn't tell anything about the presence of other singularities), through the results given by Riemann in his famous memoir (of the 1859, see §1.2.3).

We first briefly recall the definition and the main properties of the **Euler  $\Gamma$  function** (for the proofs see [Gr], §1 of chap.XII):

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

**The function  $1/\Gamma(s)$  has the following Weierstrass product:**

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

where:

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

is **Euler's constant** ( $\gamma \approx 0.577\dots$ ).

We have the following functional relations:

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

that is, the **Functional Equation of the Euler  $\Gamma$  function**;

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

which is called **Complements Relation**, and the so-called **Legendre Duplication Formula**

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

their combination give us:

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

Assuming,  $\forall \delta > 0$  fixed, that  $-\pi + \delta < \arg(s) < \pi - \delta$  and  $|s| \rightarrow \infty$ , we have the famous **Stirling Formula**:

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

From this, we can approximate the **logarithmic derivative of  $\Gamma$** :

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

### 1.2.2 Functional Equation for the $\zeta$

Riemann proved that (see §1.2.3):

i) the  $\zeta$  function, defined in 1.17, can be continued as an **analytic function over  $\mathbf{C}$ , except in 1, where has a simple pole with residue 1**;

ii) it satisfies the **Functional Equation** :

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

From the *F.E.* and the property of  $\Gamma$  we obtain also the properties :

iii)  $\zeta(s) = 0, \sigma < 0 \Leftrightarrow s = -2, -4, -6, -8, \dots$  (**trivial zeros**) (since  $|\zeta(s)| > 0 \quad \forall \sigma > 1$  by 1.11);

iv) the zeros in  $0 < \sigma < 1$ , the **critical strip**, are symmetrical w.r.t. both the real axis and the line  $\sigma = 1/2$ , called the **critical line** (i.e., we have **symmetry of the non-trivial zeros w.r.t. the point  $s = 1/2$** );

v) **the function  $\xi(s) \stackrel{def}{=} \frac{s(s-1)}{2} \pi^{-s/2} \Gamma(s/2) \zeta(s)$  is integral and has the following Functional Equation:**

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

We now turn to the study of  $\xi$ ; we say that an integral function  $f$  has **finite order** (or, also, "is of finite order") if  $\exists \alpha > 0$  such that:

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

and we'll call **order** of  $f$  the greatest lower bound of the  $\alpha > 0$  for which the estimate 1.30 holds (see that we exclude the case:  $f$  constant).

It can be proved that (cfr. [D], chap. 11 and [Gr], chap. X):

**Theorem 1.9.** *An integral function  $f$  of ordines 1 has the form:*

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

(called **Weierstrass product** of  $f$ ); here  $\{z_n\}_{n \in \mathbf{N}}$  is the sequence of the zeros of  $f$ , ordered with  $r_n \stackrel{\text{def}}{=} |z_n|$  and repeated according to their multiplicities; also, we have :

- i)  $\forall \epsilon > 0 \quad \sum_{n=1}^{\infty} r_n^{-1-\epsilon} < \infty$ ;
- ii)  $\sum_{n=1}^{\infty} r_n^{-1} < \infty \Leftrightarrow \exists C : |f(z)| = \mathcal{O}(e^{C|z|}), \quad |z| \rightarrow \infty$ .

Using this Theorem, we can expand  $\xi$  in an infinite product, since

**Theorem 1.10.**  $\xi(s)$  is an integral function of order 1.

Furthermore, from Stirling's Formula 1.27, it follows that  $\xi(s)$  doesn't satisfy the bound in the point ii) of Theorem 1.9, hence it has an infinite number of zeros; they are exactly the **non-trivial zeros of  $\zeta$** , i.e. those zeros in the critical strip, see v).

We can also show, by Theorems 1.9 and 1.10 (like Hadamard did, in the 1893) the:

**Corollary 1.2.**  $\xi$  has an infinity of zeros,  $\rho_1, \rho_2, \dots, \rho_n, \dots$ ; furthermore,

- i)  $\forall \epsilon > 0 \quad \sum_{n=1}^{\infty} |\rho_n|^{-1-\epsilon}$  converges;
- ii)  $\sum_{n=1}^{\infty} |\rho_n|^{-1}$  diverges;
- iii)  $\exists A, B \in \mathbf{C} : \xi(s) = e^{A+Bs} \prod_{\rho} (1 - s/\rho) e^{s/\rho} \quad (\text{product over } \xi \text{'s zeros.})$

The constants  $A$  and  $B$  can be calculated easily (see [D], chap. 12):

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

(Here  $\gamma$  is Euler's constant 1.22).

Taking the logarithms of iii) and differentiating (i.e., calculating the **logarithmic derivative**) we get:

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

$\xi$  definition gives therefore:

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

that, for brevity, we'll write as (like for the other logarithmic derivatives) :

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

As a consequence of the remark following Theorem 1.10, the sum is over the non-trivial zeros of  $\zeta$ ; we'll indicate them, now on, with  $\rho = \beta + i\gamma$ ,  $\beta \in [0, 1]$  and  $\gamma \in \mathbf{R}$ ; see that the sum over  $1/\rho$  converges, even if it's absolutely divergent : in fact, grouping the terms  $\rho$  and  $\bar{\rho}$  we get

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

and this is the general term of a convergent series, by i) of Cor.1.2.

### 1.2.3 Riemann Hypothesis

Bernhard Riemann, in his famous 1859 memoir (also, his only publication in the theory of number, only 8 pages-long), entitled "*Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse*", (i.e., "On the number of prime numbers under a given quantity") cfr. [Ed], proved i) and ii) for the  $\zeta$  (see previous section); also, he stated the following conjectures:

- 1) the  $\zeta$  has an infinity of zeros in the critical strip (cfr. Cor.1.2);
- 2) there holds the formula of Theorem 1.14;
- 3)  $\xi$  has the representation iii) of Cor.1.2;

4) there holds the Explicit Formula for  $\pi(x) - li(x)$  (proved by von Mangoldt in 1895, see §1.4);

5) the  $\zeta$  has all its non-trivial zeros on the critical line, i.e.:

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

the famous **Riemann Hypothesis**, the only one of which not yet proved (nor disproved).

As regards (R.H.), G. H. Hardy proved in 1914 that an infinity of non-trivial zeros lie on the critical line, while in 1942 A. Selberg proved that this, indeed, contains a positive proportion of them. More precisely, calling

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

the number of zeros of the  $\zeta$  in the rectangle inside the critical strip cut by  $t = 0$  and  $t = T$  and, instead, indicating with

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

the number of these zeros on the critical line, Selberg proved that  $\exists c > 0$  such that

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

Riemann Hypothesis is therefore equivalent to:  $N(T) = N_0(T)$  ( $\forall T \geq 0$ ).

It has important consequences on the distribution of primes (see §2.2.3).

### 1.2.4 Zero-free Regions

Let's see the heuristic argument of Hadamard to prove that :

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

that is the analytic information for the proof of the Prime Number Theorem.

Hadamard argued that, since (see Euler's Identity 1.14):

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

whether  $\zeta(1 + it) = 0$ , then:

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

from which  $\cos(tm \log p)$  should be "almost always" negative; therefore  $\cos(2tm \log p)$  should be "almost always" positive, which contrasts with the fact that  $\operatorname{Re}(\log \zeta(\sigma + 2it))$  is bounded for  $\sigma \rightarrow 1^+$  (see [D], chap. 13).

**Theorem 1.11.** *On the line  $\sigma = 1$  the  $\zeta$  never vanishes.*

Let's see an extension which improves this Theorem, giving our first **zero-free region** for  $\zeta$ , i.e. a subset of the critical strip free from zeros.

**Theorem 1.12.** *There is a  $c > 0$  (absolute and explicitly computable) such that  $|\zeta(s)| > 0$  in:*

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

The widest (known up to nowadays) zero-free region is due to Vinogradov and Korobov, who independently found it, in 1958 (using estimates of exponential sums, see Vinogradov estimates at §3.5):

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

*For all  $\alpha > 2/3$   $\exists c = c(\alpha)$  such that  $|\zeta(\sigma + it)| > 0$  in :*

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

### 1.2.5 Zero-Density Estimates

We call **Density Estimates (or Theorems)** all the results regarding estimates of the number of zeros of  $\zeta$  (or, also, of the  $L(s, \chi)$ ) in a given region (usually, a rectangle) of the critical strip.

Let's see the first one, conjectured by Riemann in his memoir and proved by von Mangoldt in 1905 :

**Theorem 1.14.** *Let  $N(T)$  be the number of zeros of the  $\zeta$ , defined in 1.32; then:*

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

In the applications, the most used Density Estimates are those giving bounds on the number of zeros with real part greater than  $\sigma$ :

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

(if  $\sigma \geq 1$ , trivially  $N(\sigma, T) = 0$ ); we give two examples :

**Ingham's density estimate** (see [In]):

**Theorem 1.15.** (A. E. INGHAM)

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

and **Huxley's density estimate** (see [Hu(1)] and [Hu(2)]):

**Theorem 1.16.** (M. N. HUXLEY)

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

Combining these two Theorems, we obtain (see [Hu(1)], chap. 28)

**PROPOSITION 1.2.** (INGHAM - HUXLEY)

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

## 1.3 Dirichlet's $L$ -functions

### 1.3.1 Dirichlet's $L$ -functions

Fix  $q \in \mathbf{N}$  and  $\chi(\bmod q)$ ; we define **Dirichlet's  $L(s, \chi)$  function** as the sum of the D.s. associated to the function  $\chi \in \mathcal{A}$  :

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

using 1.16 we obtain the analytic continuation of  $L(s, \chi_0)$ , by 1.19 in  $\sigma > 0$ , but with a simple pole in 1; also, if  $\chi$  is non-principal, the term  $A(x)$  in 1.18 is bounded, by 2.17, so we have the analytic continuation in  $\sigma > 0$ .

### 1.3.2 Functional Equation of the $L(s, \chi)$

For the functions  $L(s, \chi)$ , with  $\chi$  a primitive Dirichlet character, it holds a functional equation which is analogous to the one the Riemann  $\zeta$  function; this time it depends on the "parity" of the character  $\chi(\bmod q)$ . In fact, since  $1 = \chi(1) = \chi(-1)^2$ , we have  $\chi(-1) = 1$  or  $\chi(-1) = -1$ ; in order to distinguish between these two cases, we define:

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

We have the

**Theorem 1.17.** (FUNCTIONAL EQUATION of the  $L(s, \chi)$ )

Let  $\chi(\bmod q)$  be a primitive Dirichlet character  $\bmod q$  ( $q \in \mathbf{N}$  is fixed); if we define:

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

then :

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

(the factor multiplying  $\xi(s, \chi)$  has modulus 1 for la 2.23).

The proof (see [D], chap. 9) follows the same lines of the proof of the F.E..

As for the  $\zeta$ , the functional equation of the  $L(s, \chi)$  implies:

i)  $L(s, \chi)$  defined in 1.35 have an **analytic continuation to the whole complex plain**;

ii) for  $\chi(-1) = 1$  (i.e.  $a(\chi) = 0$ ) we have:

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

whereas for  $\chi(-1) = -1$  (i.e.  $a(\chi) = 1$ ):

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

iii) in the strip  $0 < \sigma \leq 1$  the  $L(s, \chi)$  have **non-trivial zeros**, which are still symmetrical w.r.t. the line  $\sigma = 1/2$ , but, in general (for non-real  $\chi$ ), not w.r.t. the real line.

The function  $\xi(s, \chi)$  is of finite order; actually:

**Theorem 1.18.**  $\xi(s, \chi)$  is an integral function of order 1.

From Theorems 1.9 and 1.18 we get the :

**Corollary 1.3.**  $\xi(s, \chi)$  has an infinity of zeros,  $\rho_1, \rho_2, \dots$ , such that :

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

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

iii)  $\exists A, B \in \mathbf{C}$  :  $\xi(s) = e^{A+Bs} \prod_{\rho} (1 - s/\rho)e^{s/\rho}$  (the product is over the zeros  $\rho$  of  $\xi(s, \chi)$  ).

This time, not as for the product of  $\xi$ , the constants  $A$  and  $B$  depend on the character  $\chi(\text{mod } q)$ ; by iii) and the definition of  $\xi(s, \chi)$  we have, like in 1.31:

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

where the sum is over the zeros of the  $\xi(s, \chi)$ ; these are the non-trivial zeros of the corresponding  $L(s, \chi)$ .

### 1.3.3 Generalized Riemann Hypothesis and Siegel's Theorem

Like for the  $\zeta$ -function, there's a conjecture about the location of the non-trivial zeros of the  $L(s, \chi)$ , called **Generalized Riemann Hypothesis** (it seems to have been formulated for the first time by Piltz, in 1884):

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

For  $L$ -functions there's a new (w.r.t. the theory of the  $\zeta$ ) problem : if  $\chi$  is real and non-principal, then  $L(s, \chi)$  has at most one real (simple) zero, called the **exceptional zero** (or **Siegel zero**).

However, nobody knows how to prove (or disprove) that such a zero exists. Actually, the existence of the exceptional zero is like (R.H.) or, also, (G.R.H.): there are lots of "conditional" results, meaning with "conditional" = "under the assumption of the truth of", or, also, "conditional" = "under the assumption of the falsity of".

The following **Theorem of Siegel** gives the widest zero-free region (known up to nowadays) for the  $L$ -functions (for an "easy" proof see [D], chap.21):

**Theorem 1.19.** (C. L. SIEGEL)  $\forall \epsilon > 0 \exists C(\epsilon) > 0$  such that :  $\chi$  non-principal  $\Rightarrow |L(s, \chi)| > 0$  in :

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

### 1.3.4 Zero-free Regions

For the zero-free regions of the  $L(s, \chi)$  we have the following properties.

**Theorem 1.20.** There exists a constant  $c > 0$  (explicitable) such that, if  $\chi \pmod{q}$  is complex,  $L(s, \chi)$  has no zeros in the region:

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

Furthermore, if  $\chi$  is real and non-principal,  $L(s, \chi)$  has at most one real (simple) zero in this region, the *exceptional zero* (or *Siegel zero*, see §1.3.3).

In this case, for this  $\chi \pmod{q}$  there exists a positive constant  $c > 0$  (that will not always be the same at each occurrence) for which every zero of  $L(s, \chi)$  with  $|\Gamma| \geq \frac{c}{\log q}$  has real part  $\beta < 1 - \frac{c}{5(\log q + \log(|\Gamma| + 2))}$ .

For a wider zero-free region, but with an implicit constant (which can't be explicit), see the *Theorem of Siegel* (prev. section). For the proofs of the results in this section, see [D], chap.14.

### 1.3.5 Zero Density Estimates

Since the non-trivial zeros of the  $L(s, \chi)$  are not, in general, symmetrical w.r.t. the real line, we define:

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

and :

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

Generalizing Theorem 1.18 to the  $L(s, \chi)$ , since  $N(T, \chi) = 2N(T) \quad \forall \chi \pmod{1}$ , (by 1.37), we have (see [D], chap. 16) the:

**Theorem 1.21.** *Let  $q \in \mathbf{N}$ ,  $\chi = \chi \pmod{q}$  and  $N(T, \chi)$  defined in 1.37; then :*

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

As regards the number of zeros in 1.38, we have (see also [M(1)]), for example, the famous Theorem of Enrico Bombieri (see Cor. in [B(2)])

**PROPOSITION 1.3.** *Uniformly for  $\frac{1}{2} \leq \alpha \leq 1$  and  $2 \leq T \leq X^{1/2}$  we have*

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

also, uniformly for  $\frac{5}{6} \leq \alpha \leq 1$  and  $2 \leq T \leq X^2$ , we have

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

## 1.4 Explicit Formulae

### 1.4.1 Perron's Formula

The formulae of Perron are an essential tool of T.A.N., as they permit to obtain an "explicit" estimate of  $\psi(x)$  (and thus, by partial summation, of  $\pi(x)$ ).

In fact, they link (more in general) the partial sums of a D.s. to the sum of the same series (whenever this converges absolutely).

Let's see a classic result of Perron, which gives the name to all similar formulae:

**Theorem 1.22 (PERRON'S FORMULA).** *Let  $c > 0$ ,  $x > 0$ ,  $f(s) \stackrel{def}{=} \sum_{n=1}^{\infty} a(n)n^{-s}$ ,  $w = u + iv$  and  $u > \sigma_{ac} - c$ . Then:*

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

Here (and in the following) **the sum with a dash** indicates, by def., that the term relative to  $x$ ,  $a(x)x^{-w}$ , if present, i.e. if  $x \in \mathbf{N}$ , has to be halved.

The proof can be performed, for example, using the (Cauchy's) Residue Theorem.

Analogally, we can prove the other similar formulas (for the proof of the Theorem and further remarks, see [Te], pp. 130-134).

### 1.4.2 Riemann – von Mangoldt's Explicit Formula

We give, now, the *explicit formula* for  $\psi$ , proved in 1905 by von Mangoldt on the lines indicated by Riemann in his 1859 memoir; for this reason it is called the **Riemann-von Mangoldt (Classic) Explicit Formula**.

Defining (see upside for the dash-defintion):

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

there holds the following formula.

**Theorem 1.23 ("CLASSIC" EXPLICIT FORMULA).** *If  $x > 1$  we have:*

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

with

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

and:

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

where

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

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

In particular, if  $T \leq x$ , we have:

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

where

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

In order to prove 1.40 it is used Perron's formula (see prev.sec.) and the estimates for the  $\zeta$ -function (deriving from the expression of its logarithmic derivative, see 1.31).

### 1.4.3 (Classic) Explicit Formula for $\psi(x, \chi)$

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

Then we have the following (see [D], chap.19)

**Theorem 1.24 ("CLASSIC" EXPLICIT FORMULA for  $\psi(x, \chi)$ ).** Let  $q \geq 1$  and  $x > 1$ ; then  $\forall \chi = \chi \pmod{q}$ , primitive, we have :

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

where the first series is over the non-trivial zeros  $\rho$  of the  $L(s, \chi)$  and

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

with  $a = a(\chi)$  defined in §1.3.2 and

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

also,

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

where

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

In particular, if  $T \leq x$ , there holds:

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

where

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

## Chapter 2

# Multiplicative Problems

### 2.1 Multiplicative Problems

In Analytic Number Theory the multiplicative problems are all those problems linked to the factorization of positive integers.

In particular, the main ones regard :

- the distribution of the prime numbers (both in "long" and "short" intervals, see §2.3) and therefore all the analytic methods linked to it (explicit formulae, estimates on the zeros of the  $\zeta$  function, combinatorial identities to approximate the characteristic function of prime numbers, Sieve methods, bilinear forms estimates, estimates on Dirichlet polynomials, and so on);
- the distribution of primes in the arithmetic progressions (again, both in long and short intervals) and the relative analytic tools (which include, apart from the previous ones, estimates of Gauss sums, Ramanujan sums, character sums, and so on);
- the distribution of primes among the values of a polynomial (as before, in long and short intervals), i.e. the estimate of the number of these primes (once fixed the polynomial); using the Sieve methods this problem is often reduced to the following:
- the distribution of the values of a polynomial in the arithmetic progressions (usually, for the sieve applications, with variable modulus, with remainder 0; but, also, with variable remainder class, for other applications);

- the mean value of the divisor function (also, of similar functions, like the number of prime divisors, the sum-of-divisors function, and so on)
- more in general, the representation of positive integers as a product of a fixed number of integers in a (fixed) subset of  $\mathbf{N}$ .

In order to study multiplicative problems we use the Dirichlet series, because

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

with  $s \in \mathbf{C}$  fixed.

We remark that Euler, as early as 1742, already used this property, but with  $s \in \mathbf{R}$ .

Then, Dirichlet and Riemann skillfully used this idea; in particular, at the hands of Riemann, it was used in his (quite new) complex analytical methods; these, in turn, allowed an improved understanding of arithmetical properties, since they gave for the first time the possibility to manage infinite quantities, by the residue theorem and the "classification of infinities" (i.e., the isolated singularities of analytic functions).

Of course, everything can be studied in the environment of real analytical methods, but with a price to be paid in terms of a less transparent argument and, sometimes, also of a worst efficiency of the estimates (as an example, compare the "elementary" proof of the Prime Number Theorem, see §2.2.1, which has as remainder only  $o(x/\log x)$ , with the one in the "classical" proof, see §2.2.3).

## 2.2 Prime Number Theorem

### 2.2.1 Function $\pi$ and Cebicev estimates

We define the **function**  $\pi$ , that counts the prime numbers up to  $x$  ( $x > 0$ ):

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

(note that  $\pi$  is not an arithmetic function; also, it's a step function, being constant in the intervals  $[p, p']$ , where  $p'$  is the prime consecutive to  $p$ , and it's discontinuous at  $x$  prime).

The first result about  $\pi$  is, of course, **Euclid's Theorem** : there exist infinite primes, i.e.  $\pi(x) \rightarrow \infty$ , as  $x \rightarrow \infty$ .

The first systematic study of  $\pi$  began with the russian mathematician Cebicev, who, in 1852, proved "Bertrand's postulate", i.e. : every interval  $]n, 2n]$ , with  $n \geq 1$  integer, always contains (at least) one prime.

This result follows from Cebicev's lower and upper estimates

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

( $c_1 = \log(2^{1/2}3^{1/3}5^{1/5}30^{-1/30})$  and  $c_2 = \frac{6}{5}c_1$ ) and, as usual,  $f = o(g)$  indicates  $f(x)/g(x) \rightarrow 0$ , when  $x \rightarrow \infty$ .

In the following we'll call **Cebicev's estimates**

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

where we have used **Vinogradov's notation**  $f \ll g$ , to indicate, for  $g > 0$ , that  $\exists X > 0, \exists C > 0$  (eventually  $C = C(X)$ , here) such that  $|f(x)| \leq Cg(x) \quad \forall x > X$ .

From numerical tables data K. F. Gauss (in 1792) and A. M. Legendre (in 1798) conjectured that:

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

i.e.:

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

(As usual,  $f(x) \sim g(x)$ ,  $f$  and  $g$  are asymptotical(ly equivalent), if  $\lim \frac{f(x)}{g(x)} = 1$ , with  $x$  going to the specified limit: in this case  $x \rightarrow \infty$ ).

The formula 2.3 is called the **Prime Number Theorem** (abbrev. PNT), and has been proved for the first time in 1896, independently, by J. Hadamard and C. de la Vallee Poussin with complex analytical methods, using the properties of the Riemann  $\zeta$  function. In particular, the required property is the non-vanishing on the line  $\sigma = 1$ .

The condition  $|\zeta(1 + it)| > 0$  has been used also in other two proofs. The first, in 1935, was given by Ingham with Fourier analysis techniques. The other, has been given in 1980, by Newman, employing complex-integrals techniques.

In 1949, Paul Erdős and Atle Selberg, independently, gave an "elementary" proof of 2.3, i.e. not using complex analysis, nor properties of the  $\zeta$ . (See, for example, [H-W], chap. XXII.). Recently (1984) Daboussi gave another elementary proof (see [Te]).

### 2.2.2 Cebicev's functions $\psi$ and $\theta$

Let's define, now, the **Cebicev's functions**,  $\psi$  and  $\theta$  ( $x > 0$ ):

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

It's immediately verified that:

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

where  $f(x) = \mathcal{O}(g(x))$  is the usual notation, equivalent to  $f(x) \ll g(x)$  (even here  $x \rightarrow \infty$  and  $g(x) > 0$ ), even if Vinogradov's is more frequently used in Analytic Number Theory. We'll also write  $f(x) = \mathcal{O}_{\varepsilon, \vartheta, A, \dots}(g(x))$

or  $f(x) \ll_{\varepsilon, \vartheta, A, \dots}(g(x))$  to mean that the implied constant  $C$  depends on the variables  $\varepsilon, \vartheta, A, \dots$  (apart from, eventually, also  $X$ , see after 2.2).

The notation  $\mathcal{O}$  is due to E. Landau, who used it systematically just in Analytic Number Theory (since then it's also a standard notazione of mathematical analysis). Futhermore, also Vinogradov's notation (see upside),  $f \ll g$ , is used; it's more frequently used in Analytic Number Theory, as it's more practical than Landau's.

In order to show the links between  $\theta$  and  $\pi$  we'll use a simple consequence of the Fundamental Theorem of Calculus :

**LEMMA 2.1.** (PARTIAL SUMMATION)

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

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

Applying the lemma with  $a(n) = \chi_{\mathbf{P}}(n) \log(n)$ , (here  $\chi_{\mathbf{P}}$  is the primes characteristic function), and  $f(t) = 1/\log(t)$ ,  $t \in [2, x]$ , we have:

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

This last equation, together with 2.4 and the definition of "li", the "**logarithmic integral**" function:

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

we have the

**LEMMA 2.2.** If  $\psi(x) = x + \mathcal{O}(R(x))$  then

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

Since in 2.6 it holds  $\text{li}(x) \sim x/\log(x)$ , we obtain from 2.7, for  $R(x) = o(\text{li}(x) \log x)$ ,

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

i.e. the Prime Number Theorem.

In the next section we'll see how to get  $R(x) = o(x)$ , in order to obtain 2.8 whence the PNT from Lemma 2.2.

### 2.2.3 Prime Number Theorem

As we saw in §1.3, the function  $\psi$  is a good substitute for  $\pi$ , the function counting prime numbers up to  $x$ ; hence, any formula containing  $\pi$  can be replaced by its analogue for  $\psi$ ; thus, the formula for  $\pi(x) - li(x)$  given by Riemann in his famous memoir of 1860 and proved by von Mangoldt in 1895 is equivalent to the relation for  $\psi(x) - x$  from the *classic explicit formula* (see §1.4.2):

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

where the sum is over the non-trivial zeros  $\rho$  of the  $\zeta$  for which  $|Im(\rho)| = |\gamma| \leq T$ ; assuming  $T \leq x$ , the remainder  $E(x, T)$  is:

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

Using this formula we can prove the PNT by means of the zero-free region given in Theorem 1.12:

**THEOREM 2.1 (DE LA VALLEE POUSSIN).**  $\exists c > 0$  (computable) such that:

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

**Proof:** We want to show that

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

and we choose  $T \leq x$  such that 1.42 holds; therefore by the symmetry of the zeros  $\rho$  w.r.t. the real line we will prove that:

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

By Theorem 1.12 we have ( $c$  is not always the same at each occurrence):

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

for  $|\gamma| < T$  and  $T$  enough large (as we may suppose).

See that  $\gamma > 0 \Rightarrow |\rho| \geq \gamma$  whence:

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

this sum can be expressed as a Riemann – Stieltjes integral:

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

having integrated by parts ( $N(T)$  is defined in 1.32); from 2.10 and 1.34 we then get

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

Combining this and 2.9 we have

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

and from this the Theorem, choosing  $T$  such that  $\log^2(T) = \log(x)$ .

The PNT follows easily from lemma 2.2; it suffices, in fact, to choose in this lemma the remainder given by the previous Theorem:

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

It's now clear the importance of a good estimate of the remainder  $R(x)$ , that's to say to have good explicit formulae, i.e., with a good  $E(x, T)$  (see 1.42).

As we saw in this last theorem, it suffices to estimate the sum over the  $\zeta$  zeros and  $E(x, T)$  in the classic explicit formula to get the PNT (with a suitable choice of  $T$ ); using Riemann Hypothesis *R.H.* (cfr. §1.2.3), the estimate 2.9 becomes:

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

whence (we apply 1.42 with  $T \leq x$ ):

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

i.e.o, taking  $T = x^{1/2}$

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

under *R.H.* we then get

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

i.e. the "best possible" remainder in Lemma 2.2 and in

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

We remark that the size of the remainder depends of course on the location of the zeros, and precisely on the width of the  $\zeta$  zero-free regions.

In fact, we have the following:

**PROPOSITION 2.1.** *Let  $1/2 \leq \theta < 1$  be fixed. Then*

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

**Proof:** We suppose first that

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

using 1.18, with  $a = \Lambda$ , i.e.  $A(x) = \psi(x)$ , we then have, by 1.13:

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

with  $R(x) \ll x^{\theta} \log^2 x$ , whence the integral is defined and regular for  $\sigma > \theta$ , in which  $\zeta$  doesn't vanish (otherwise the logarithmic derivative would have a singularity there).

Arguing as in the previous Theorem proof we prove the other implication.

In the same way, by means of the wider zero-free region due to Vinogradov and Korobov (see §1.2.4) we obtain the stronger Theorem :

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

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

In fact, it can be proved as the previous, choosing:

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

with  $\beta = \frac{1}{\alpha+1}$ , where  $\alpha$  is the constant in the Vinogradov – Korobov zero-free region (cit., §1.2.4).

## 2.3 Primes in Short Intervals

We say that  $[x, x + H]$  is a short interval if  $H = H(x)$  is a positive and increasing function of  $x$  such that  $H/x$  is decreasing,  $H \rightarrow \infty$  and  $H = o(x)$  as  $x \rightarrow \infty$ .

In 1972 M. N. Huxley [Hu(2)] has proved that, when  $H \geq x^{7/12+\epsilon}$ , with  $\epsilon > 0$ , the short interval  $[x, x + H]$  always contains at least one prime number, for  $x$  enough large; also, that the number of such primes in this interval is the expected value (i.e.,  $H/\log x$ ).

Furthermore, using his result about density estimates (cit.), it can be shown, with standard analytic techniques, that the requirement on the size of  $H$  can be weakened up to  $H \geq x^{1/6+\epsilon}$  to obtain, for "almost all" the  $x \in [N, 2N]$ , the interval  $[x, x + H]$  always contains at least one prime (for  $N$  enough large; also, their number is the expected one); by this we mean that the set of  $x \in [N, 2N]$  for which  $[x, x + H]$  doesn't contain a prime has measure at most  $o(N)$  (in general, we say that a relation holds for almost all  $x \in I$  if it's true  $\forall x \in I \setminus S$ , where  $|S| = o(|I|)$ ).

More in general, there is the following relation between density theorems and primes in short intervals (respectively, all or almost all).

We say that there holds the **Prime Number Theorem in the short interval**  $[x, x + h]$  if

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

The following result links the density estimates to the Prime Number Theorem in Short Intervals:

**THEOREM 2.3 (DENSITY ESTIMATES FOR PRIMES IN SHORT INTERVALS).** *Let*

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

for some  $D \geq 1$  and  $A(\sigma)(1-\sigma) \leq 0$ , where for some  $\frac{1}{2} < u < 1$  we have  $A(\sigma) \leq 2$  for  $\sigma \geq u$  and, for  $\frac{1}{2} \geq \sigma \leq u$  we have  $A(\sigma) \leq C$ , for some  $C > 1$ . Then there holds 2.11, with  $h \geq x^{1-1/C} \log^M x$  and  $\forall M > \frac{D+2}{C(1-u)}$ .

As regards, instead, the PNT in almost all the Short Intervals (i.e. 2.11 for almost all the short intervals  $[x, x + h]$ ), we have the

**THEOREM 2.4 (DENSITY ESTIMATES FOR PRIMES IN ALMOST ALL THE SHORT INTERVALS).** *Let*

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

*for some  $C \geq 2$  and  $D \geq 1$ . Then for almost all the  $x$  we have the 2.11, under the hypothesis that*

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

*with  $B = B(C, D)$  explicitly computable.*

As regards the proof of the two Theorems upside, see [Iv] (§12.5).

## 2.4 Primes in the Arithmetic Progressions

### 2.4.1 Arithmetic Progressions and Additive Characters

We call **arithmetic progression** of modulus  $q$  (or, modulo  $q$ ) any subset of the integers of the kind  $\{qn + a : n \in \mathbf{N}\}$ , with  $q \in \mathbf{N}$  and  $a \in \mathbf{Z}$ .

We define **additive character** any of the  $q$ -th roots of unity in the complex field, say  $e_q(a) \stackrel{\text{def}}{=} e^{2\pi ia/q}$ .

In order to express the condition  $n \equiv a \pmod{q}$  (i.e.  $n$  belongs to the arithmetic progression  $\pmod{q}$  relative to  $a$ ) we can use the relation called **additive characters orthogonality** (see the next section for multiplicative characters orthogonality)

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

Starting from this (which is proved easily) we can evaluate the **Ramanujan sums**

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

in fact

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

and through Möbius inversion formula we obtain the 2.12

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

whence, in particular,  $c_q(n)$  is a multiplicative function w.r.t.  $q$  for all fixed  $n$ ; evaluating it on the prime-powers we finally obtain

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

### 2.4.2 Multiplicative Characters and Dirichlet Theorem

We can prove Euclid's theorem by Euler's Identity 1.14, like the same swiss mathematician Leonhard Euler did in 1737, letting  $s \rightarrow 1^+$  and using the divergence of the harmonic series.

This idea was used by Peter Gustav Lejeune Dirichlet to prove his famous Theorem on the infinitude of primes in non-trivial arithmetic progressions (see the following) in his memoir of 1837, which marks the beginning of Analytic Number Theory (actually, it is still, nowadays, the only theorem on the representability of infinite primes as values of a polynomial).

The **Dirichlet Characters (or Multiplicative Characters)**,  $\chi(\bmod q)$  can be defined as completely multiplicative arithmetic functions and of period  $q$ , vanishing on the naturals not coprime to  $q$ , but not identically zero (for further details see chapters 1 and 4 [D]).

We define **the principal (or trivial) character** the character  $\chi_0(\bmod q)$  defined by:

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

**primitive** a character  $\chi$  such that:

$$(2.16) \quad \chi : \mathbf{N} \rightarrow \mathbf{C} \quad \text{doesn't have period } q_1, \quad \forall q_1 < q;$$

(and we'll consider the principal character neither not primitive, nor primitive)

and **real** a character  $\chi : \mathbf{N} \rightarrow \mathbf{R}$ .

It can be proved that:

i) for any  $q \in \mathbf{N}$  there exist exactly  $\phi(q)$  characters  $\chi(\bmod q)$  ( $\phi$  is the Euler totient function, def. in §1.1.2);

ii)  $|\chi(n)| > 0 \Leftrightarrow \chi(n)$  is a root of unity (whence  $|\chi(n)| = 1$ );

iii)  $\chi(mn) = \chi(m)\chi(n) \quad \forall m, n \in \mathbf{N} \quad \forall \chi(\bmod q) \quad \forall q \in \mathbf{N}$  (**the Dirichlet characters are completely multiplicative arithmetic functions**).

Furthermore, there hold the **orthogonality relations** among characters ([D], chap. 4):

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

(by  $\chi(\bmod q)$  periodicity the sum can be performed w.r.t. any complete set of residues mod  $q$ )

and:

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

(the sum is over all the  $\phi(q)$  characters  $\chi(\bmod q)$ ).

Through 2.18 we can build a sum, giving the characteristic function of the remainder class  $a(\bmod q)$  :

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

actually, this relation allows to choose the primes  $p \equiv a(\bmod q)$  to prove the

**THEOREM 2.5 (DIRICHLET).** *Let  $q \in \mathbf{N}$  and  $a$  an integer coprime to  $q$ . Then the non trivial arithmetic progression  $\{qn+a : n \in \mathbf{N}\}$  contains an infinity of primes.*

Let's see a brief sketch of the proof.

First of all, from 1.15 we have  $|L(s, \chi)| > 0$  in  $s > 1$  :

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

which, by 2.19, gives (now on  $n \equiv r(q)$  stands for  $n \equiv r(\bmod q)$ )

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

Since, for  $s > 1$

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

we have (by 2.20)

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

since in the left hand side the term due to the principal character is the  $\zeta$  function times a constant (see §1.1.4), it diverges for  $s \rightarrow 1^+$ . In order to

prove the divergence of all the left hand side (as  $s \rightarrow 1^+$ ), Dirichlet proved that  $L(1, \chi)$  never vanishes for all non-principal  $\chi(\bmod q)$  through his **Class Number Formula**.

This result, actually, proves also the following asymptotic relation

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

Define the **Gauss sum**  $\tau(\chi)$  relative to  $\chi$  ( $q > 1$  is a fixed integer):

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

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

When  $\chi(\bmod q)$  is primitive, the following equations are easy to prove (see [D], chap. 9):

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

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

Also, we have that for all non-principal  $\chi(\bmod q)$

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

From 2.17 we get, in particular,  $\forall N \in \mathbf{Z}, \forall M \in \mathbf{N}$

$$\left| \sum_{n=N}^{N+M} \chi(n) \right| \leq q \quad \text{if } \chi \text{ is non-principal}$$

(trivial estimate), that can be much improved. In fact, there holds the

**POLYA-VINOGRADOV INEQUALITY.** *For all non-principal  $\chi(\bmod q)$  ( $q > 1$ ) we have,  $\forall N \in \mathbf{Z}, \forall M \in \mathbf{N}$*

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

### 2.4.3 Prime Number Theorem in the Arithmetic Progressions

Defining the "counting function" (with logarithmic weight) of primes in the arithmetic progression  $qn + a$ :

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

we get the following two results (**Prime Number Theorem in the Arithmetic Progressions**). The first is an effective result (the constant  $c$  is effective, i.e., it can be computed)

**PROPOSITION 2.2.** *Fixed  $\delta \in ]0, 1[$  we have*

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

where  $c$  is an absolute (computable) constant.

The best result of this kind, as regards the uniformity in  $q$ , is the following application of Siegel's Theorem (see previous sections)

**THEOREM 2.6 (SIEGEL-WALFISZ).** *Given  $A > 0$ ,  $\exists C = C(A)$  such that*

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

uniformly in  $q$ .

Because of non-constructive arguments in the proof of Siegel's Theorem,  $C(A)$  and the " $\mathcal{O}$ "-constant are not computable, whence Siegel-Walfisz Theorem is "non-effective".

However, it is a valid tool for the estimate of contributes due to major arcs, in the Circle Method (see chap. 3).

## 2.5 Bombieri's Theorem

**Bombieri's Theorem** is a remarkable consequence of Siegel-Walfisz Theorem and of the Large Sieve (hence is non-effective); it describes the mean value of the remainder

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

computed over the moduli  $q \leq Q$  (see [D], chap. 28):

**THEOREM 2.7 (BOMBIERI).** *For any  $A > 0$ , there exists  $B = B(A) > 0$  such that, for  $Q \leq x^{\frac{1}{2}}(\log x)^{-B}$ , we have*

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

with, for example,  $B = 3A + 23$  (see [B(2)]).

(In the following, better values of  $B = B(A)$  have been given, esp., by Gallagher [Ga(2)],  $B = 16A + 103$ , and by Vaughan [Va(2)],  $B = A + 7/2$ ).

Bombieri's Theorem is equivalent to have, on average on the moduli, the estimate

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

which follows by GRH (see §1.3.3).

Bombieri's Theorem proof is performed by Siegel - Walfisz Theorem (see §2.4.3) and the Large Sieve (see §4.3); these tools can be used in different ways getting different proofs. For example, one can use the Large Sieve (see [Hu(1)], chap.24, or Bombieri's paper, cit.) to find estimates on the number of zeros of the  $L$ -functions; or (like [D], cit.) Siegel - Walfisz Theorem on "small" moduli (i.e.  $q \leq \log^N x$ ) and the Large Sieve on the remaining, after having estimated the bilinear forms coming from Vaughan's identity for the  $\Lambda$ -function:

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

with:

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

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

This (combinatorial) identity follows from the corresponding identity for the relative Dirichlet series:

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

i.e., in the half-plane  $\sigma > 1$  we have **Vaughan's Identity** (see [Va(3)])

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

Analogously, we have **Heath - Brown's Identity** in  $\sigma > 1$  and  $\forall k \in \mathbf{N}$  (see Lemma 1 in [HB])

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

whence we get the corresponding combinatorial identity for  $\Lambda$ .

Using this last result, Perelli, Pintz and Salerno have generalized Bombieri's Theorem, in order to obtain an analogous estimate in the short intervals (see [P-P-S(1)] and [P-P-S(2)]).

## Chapter 3

# Additive Problems

### 3.1 Additive Problems

We call additive problems all the problems of the kind:

given an integer  $n$ , and  $r$  sets  $A_1, A_2, \dots, A_r$  (of integers),

determine the number  $\nu(n)$  of solutions of the equation:

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

in particular, we may ask for the values  $\nu(n)$ , for  $n$  "enough large", i.e. greater than a certain integer  $N > N_0$  (we have often only existence results, i.e. no explicit value of  $N_0$ ).

For example, we may suppose that all the  $A_j$  ( $j = 1, \dots, s$ ) are the set of  $k$ -th powers; in this case we are studying **Waring's Problem** (originated by two conjectures, in 1770, of Edward Waring):

find the number of representations of a natural number as a sum of  $s$   $k$ -th powers.

Defining the quantities  $g(k)$  and  $G(k)$ :

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

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

then *Waring's problem* consists in finding  $g(k)$  and  $G(k)$ ; Waring conjectures that  $g(3) = 9$  and  $g(4) = 19$  (this last has been recently proved by Balasubramanian, Deshouillers and Dress, see [B-D-D]).

By elementary considerations we have (here  $[x]$  is the integer part of  $x$ )  
:

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

and  $g(4) = 19$  (quoted upside).

For  $k$  different from 4, it has been proved (here  $\{ \}$  stands for fractional part):

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

and, if  $k$  doesn't verify the hypothesis, we have that  $g(k)$  equals:

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

depending on if (respectively)

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

is  $2^k$  or greater than  $2^k$ .

The values  $g(k)$  are then all known, since  $g$  depends on the behaviour of few naturals not too large;  $G(k)$ , instead, is much harder to calculate.

The best results for  $G$  are:

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

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

Other instances of additive problems are, for example, the homogenous diofantine equations, the diofantine inequalities and the arithmetic progressions among subsets of naturals.

The Circle Method (see §3.3 and §3.4) has several applications to additive problems (see, for example, §3.5 and §3.6; also, [Va(1)]).

## 3.2 Goldbach problems

In a letter to Euler, in 1742, Christian Goldbach conjectured that each even natural number is the sum of two primes and every odd natural number is the sum of three primes; he included 1 among prime numbers, whence the modern versions of *Goldbach's Conjecture* are:

- 1) (**Goldbach's Binary Conjecture**) all even  $n > 2$  are sum of two primes;
- 2) (**Goldbach's Ternary Conjecture**) all odd  $n > 5$  are sum of three primes.

The best result for the ternary conjecture was obtained in 1937 by I. M. Vinogradov, with his famous "Three Primes Theorem" (see §3.5), which proves 2) for all "enough large" odd  $n$ .

The Theorem was proved by Vinogradov (see §2.4 and §2.5) with a big refinement on the Hardy-Littlewood method (§2.1); in fact, they were the first, in 1923, to prove 1) for almost all enough large even numbers and the Theorem, but assuming the Generalized Riemann Hypothesis (*G.R.H.*) (see §1.3.3); they used this Hypothesis in the treatment of minor arcs. Vinogradov used (for the same purpose), instead, his method of exponential sums (originated in the 20s), giving then a non-conditional proof of the Theorem.

As regards 1), the Circle Method (abbrev. C.M.) gives (as stated) a solution "for almost all even  $n$  enough large" (see cor. 2.3); the proposition 1), being not yet proved, is referred to as **Goldbach problem**.

There are other approaches employing sieve methods (see chap. 4) which prove the existence of a natural  $N$  (non-computable) such that:

1-r) (*weak version of Goldbach conjecture*)

each even  $n > N$  is the sum of a prime and of a quasi-prime  $P_r$ ,

where a **quasi-prime**  $P_r$  is by definition a natural number which is the product of at most  $r$  primes (distinct or not).

Clearly, the conjecture 1) is 1-r) for  $r = 1$ ; hence we seek a "minimal"  $r$  (which renders the conjecture a theorem).

In 1948, Renyi, using sieve methods, proved that exists a  $r \in \mathbf{N}$ , fixed, for which 1-r) holds.

In 1966, Chen found (with the most sophisticated sieve methods) the best result for 1- $r$ ), i.e. he proved it for  $r = 2$ ; Chen's Theorem states, in fact, that all enough large even numbers are sum of a prime and a  $P_2$ , prime or product of two primes (see esp. [H-R]).

### 3.3 Hardy-Littlewood Method

The method of trigonometric sums (also called **Hardy-Littlewood Method**, abbrev. H-L method) was originated in a 1918 paper of G. H. Hardy and S. Ramanujan, in which they studied the problem of the number  $R_s(n)$  of representations of a natural  $n$  as a sum of  $s$  squares (and, more in general, as a sum of  $s$   $k$ -th powers: see §3.1).

Hardy and Ramanujan considered the function:

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

relative to the strictly increasing sequence  $(a_m)_{m \in \mathbf{N}}$ :

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

where  $R_s(n)$  is the number of representations of  $n$  as a sum of  $s$  elements of  $(a_m)_{m \in \mathbf{N}}$  (being this strictly increasing, two representations differing only for the order of the summands are counted as one); they treated then, in particular, the case  $a_m = m^2$ .

As for the estimate of  $R_s(n)$  we can use Cauchy's formula, with  $C$  the circle of center 0 and radius  $0 < \rho < 1$  in the complex plane:

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

(that's why it's also called **Circle Method**).

Hardy and Ramanujan found that the function  $F$  (analytic in the interior of  $C$ , but with a dense set of singularities on  $C$ ) has an asymptotic expression in  $z = \rho(\alpha)$  ( $0 < \rho < 1$  and  $\alpha \in [-1/2, 1/2]$ ) "close" to of the points of  $C$ ,  $(a/q)$ , for which  $q$  is "enough small"; i.e., if  $\rho = 1 - 1/n$ , with  $n$  "large" and  $\beta = \alpha - a/q$  is small (with  $q$  suitably small), then we have:

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

( $c$  is a suitable constant,  $F$  is referred to  $a_m = m^2$ ,

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

and the sum starts from  $m = 1$ ).

By Dirichlet's approximation Theorem every  $\alpha \in [-1/2, 1/2]$  is "close" to a suitable  $a/q$  (see [Va(1)]), so that (2.1.4) holds  $\forall \alpha$  in  $[-1/2, 1/2]$  (in the case of squares).

By 3.2 and 3.3 we then get (for  $s \geq 5$ ):

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

where  $\mathfrak{S}_s$  is the **singular series**:

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

and  $J_s$  is the **singular integral**:

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

(The series and the integral here defined refer to the particular sequence of squares; every sequence  $(a_m)_{m \in \mathbf{N}}$  has its own singular series and its own singular integral: see the following sections).

Hardy, together with J. E. Littlewood, applied the same argument to  $a_m = m^k$ , with  $k \geq 3$ , to get informations on the number  $R_s(n)$  of representations of  $n$  as a sum of  $s$   $k$ -th powers; the expansion for the corresponding  $F$  was valid non in all of the circle  $C$ , but only on the pieces of this, which were called **major arcs**; the remaining parts of  $C$  being the **minor arcs** (see that "minor" is not referred to their measure, which, actually, in most cases is the top possible, i.e. 1; but qualifies their contribute to the number of representations).

An estimate for  $F$  on the minor arcs was then required; this was supplied, for the particular sequence  $a_m = m^k$  ( $k \geq 3$ ), for example, by Weyl's Lemma (see [Ti], chap.6).

### 3.4 Vinogradov's Method

Around the end of 20s the H-L method was improved by Vinogradov, who introduced a number of changes, most notably he substituted to  $F$  the *trigonometric sum*:

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

whence the other name **Trigonometric Sums Method**; but it's more commonly known as "Circle Method" (abbrev. **C.M.**).

We have at once:

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

where  $R_s(m, n)$  is the number of representations of  $n$  as a sum of  $s$   $k$ -th powers, none of which is greater than  $n$ ; also, if  $R_s(m)$  is the same number of representations for  $m$ , but with no constraints, then

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

since, trivially,  $\forall h \in \mathcal{Z}$ :

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

we have:

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

In order to estimate this integral we proceed as for the H-L method, dividing the integration interval into major and minor arcs (we continue using this terminology, even if now they're intervals in  $[0,1]$ ).

**REMARK 3.1.** Because of the periodicity of  $f$ , all the integrals on a length1-interval are the same, whichever translation is applied.

For an example of Vinogradov's Method see the next section.

### 3.5 Three-Primes Theorem

We give, now, the best application of the Circle Method: **Vinogradov's Three-Primes Theorem** (the Corollary at the end of the section).

Let's define:

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

for  $n$  enough large and  $B > 0$ , constant, let  $P \stackrel{\text{def}}{=} (\log n)^B$ ; then the **major arcs** relative to  $a/q$ , with  $1 \leq a \leq q \leq P$  and  $(a, q) = 1$ , are:

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

and their union  $\mathfrak{M}$  (for  $n$  "large" the arcs are two-by-two disjoint); the **minor arcs** are, then, the complement  $\mathfrak{m} \stackrel{\text{def}}{=} \mathcal{U} \setminus \mathfrak{M}$ .

By remark 3.1:

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

where now:

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

We'll see first how to estimate the integral on the minor arcs by Theorem 3.1, for which we need the following:

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

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

**Theorem 3.1.** (I. M. VINOGRADOV) Let  $(a, q) = 1$ ,  $q \leq n$  and  $|\alpha - a/q| \leq q^{-2}$ ; then:

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

In order to estimate the integral:  $\int_{\mathbf{m}} f(\alpha)^3 e(-n\alpha) d\alpha$  we observe that, by Parseval identity and the Prime Number Theorem (actually, we need even less :  $\psi(x) \ll x$  : see §2.2.1 and §2.2.2), we have:

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

As for the proof of Theorem 2.1 we obtain:

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

whence, by the Remark 2.1 and the Theorem 2.4, we get the:

**Theorem 3.2.** (ESTIMATE OF  $R(n)$  ON THE MINOR ARCS) If  $A > 0$  and  $B \geq 2A + 10$ :

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

In order to complete the estimate of 3.5 we'll deal with major arcs, for which we'll use the theory of primes in the arithmetic progressions (see §2.4.3) and the *Ramanujan sums* (see §2.4.1).

(Since we'll use Siegel-Walfisz Theorem, the constants will not be effective, see Theor. 2.6).

On defining  $v(\beta) \stackrel{def}{=} \sum_{m \leq n} e(m\beta)$ ,  $\forall \beta \in \mathbf{R}$  ed  $\exp(t) \stackrel{def}{=} e^t$ ,  $\forall t \in \mathbf{R}$ , we have the

**LEMMA 3.2.** If  $1 \leq a \leq q \leq P$  and  $(a, q) = 1$  then  $\exists C > 0$  such that  $\forall \alpha \in \mathfrak{M}(q, a)$

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

We define the **singular serie for the ternario Goldbach problem**

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

by 2.14 this is

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

The arithmetic informations in the three-primes problem depend on  $\mathfrak{S}$ ; through Lemma 3.2 we in fact obtain the:

**Theorem 3.3.** (ESTIMATE OF  $R(n)$  ON THE MAJOR ARCS) *If  $A > 0$  and  $B \geq 2A$ , then :*

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

From 3.7 we get:

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

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

The estimate of the integral on all  $\mathcal{U}$  follows by Theorems 3.2 and 3.3:

**theorem 3.4.** (I. M. VINOGRADOV) *Let  $A > 0$  be a constant, with  $R(n)$  defined by 3.5 and 3.5; then:*

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

By partial summation and 3.8 we have the:

**COROLLARY 3.1 (VINOGRADOV’S THREE-PRIMES THEOREM).** *Every enough large odd number is the sum of three primes.*

Notice that, by 3.9, Theorem 3.4 gives no information for the binary Goldbach problem (see next section); while it proves the ternary conjecture, also providing an asymptotic estimate for the number of representations of (enough large) odd numbers (as sums of three primes).

For the proofs of this section, see [Va(1)] (in all of this Chapter we’ll follow its notations, which will differ from the ones of §5.3).

For a survey of the (main) variants of Corollario 3.1 (which is also called **Goldbach–Vinogradov Theorem**), see the recent article by Liu and Zhan [L-Z].

We’ll see, briefly, in the next section how to obtain informations on the Goldbach problem (binary conjecture) using the Circle Method; the resulting estimate proves only that the conjecture holds for **”almost all”** the (enough large) even numbers.

### 3.6 Circle Method and Goldbach Problem

The Circle Method gives, for the binary Goldbach problem, only a non-trivial estimate to:

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

where, for  $m \leq n$ :

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

and:

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

As in the previous section, we have:

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

where:

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

and:

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

Here  $R_3$  is the coefficient Fourier series for the function given by  $f(\alpha)^2$  on  $\mathfrak{m}$  and 0 elsewhere; by Bessel inequality:

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

This, and the arguments of Theorem 3.2, prove the:

**Theorem 3.5.** (ESTIMATE OF  $R_1$  ON THE MINOR ARCS) If  $A > 0$  and  $B \geq A + 9$ , then :

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

By the elementary estimates (see [Va(1)] and [Te]):

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

we have, with:

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

the estimate :

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

but this time:

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

is the number of solutions to the equation:

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

i.e.

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

The (2.4.38) gives  $\phi(n)^{-2}/n^{2\delta-2} \rightarrow 0$  for  $n \rightarrow \infty$ , whence:  $\sum_{q > Z} \phi(q)^{-2} \ll \frac{1}{Z}$ ; this, together with the expression of  $R_2$ , prove the:

**Theorem 3.6.** (ESTIMATE OF  $R_1$  ON THE MAJOR ARCS) If  $A > 0$  and  $B \geq A + 2$ , then :

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

By the previous Theorems we then have the:

**Theorem 3.7 (ESTIMATE OF  $R_1$ ).** For any  $A > 0$  we have

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

This time, as regards the singular series, we have

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

(the first product is over the primes not dividing  $m$ ), whence:

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

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

therefore the binary is proved "for almost all the even  $n \leq N$ ", i.e. for all, except at most  $o(N)$  of them; let's define, then, the **exceptional set for the Goldbach binary problem** :

$$E(n) \stackrel{def}{=} |\{m \leq n : m \text{ even and not a sum of two primes}\}|.$$

Chudakov, Estermann and van der Corput (see [Va(1)]) proved (independently) the following result (which follows from Theorem 3.7 by what we considered about the singular series  $\mathfrak{S}_1$ ):

**COROLLARY 3.2 (ESTIMATE FOR THE EXCEPTIONAL SET IN THE GOLDBACH BINARY CONJECTURE).** For any  $A > 0$  we have

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

The best (up to date) estimate on the exceptional set for Goldbach Problem is due to Montgomery and Vaughan (see their 1975 paper)

**PROPOSITION 3.1 (MONTGOMERY-VAUGHAN).** There exists an absolute constant  $\delta > 0$ , computable, such that

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

## Chapter 4

# Sieves and Exponential Sums

### 4.1 Sieves and Exponential Sums

In this section we give an idea of the Sieve Methods and just the definition of general Exponential sums (see §4.5); we'll give a brief survey of the main Sieve Methods in the next two sections.

Our definition of "**Arithmetic Sieve**" is the one given by Halberstam and Richert in their "Sieve Methods" [H-R].

In the Sieve-Methods outset  $\mathcal{A}$  is no more the set of arithmetic functions, but a finite subset of natural numbers  $\mathcal{A} \subseteq \mathbf{N}$ ; and  $\mathcal{B} \subseteq \mathbf{P}$  indicates any (eventually infinite) subset of the prime numbers. Defining

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

we want to estimate, say,  $S(\mathcal{A}, \mathcal{B}, z)$ , the number of elements of  $\mathcal{A}$  which are left after having "sifted-out" all those divisible by at least one prime of  $\mathcal{B}$  less than  $z$ ; i.e. we define

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

that represents, then, the number of elements of  $\mathcal{A}$  left after this "sieve".

The **Sieve Methods estimate** in fact **the** number  $S(\mathcal{A}; \mathcal{B}, z)$  (which is called **sifting function**), or even weighted quantities linked to it.

We define **exponential sum** a generic sum of  $N \in \mathbf{N}$  complex numbers, depending on  $M \in \mathbf{Z}$ ,  $\alpha \in \mathbf{R}$ , and a sequence  $\{a_n\}_{n \in \mathbf{N}}$  (of complex numbers)

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

## 4.2 Small Sieve

In the present section we give a short survey of the main "Small Sieves", i.e. sieve methods in which the number of prime factors of  $q$ ,  $\omega(q)$ , is "small" w.r.t. the quantities we refer to (usually, the length of the interval:  $x$  for "long" intervals,  $h$  for the "short": see §5.4, §5.5, §5.6); in particular, we'll see the Eratosthenes-Legendre Sieve, the Brun Combinatorial Sieve and Selberg Sieve (in the following,  $\omega(q)$  will indicate both the function "number of primes factors" and a generic arithmetic function; the choice will be clear from the context).

### 4.2.1 Eratosthenes-Legendre Sieve

The first "sieve"-idea is attributed to Eratosthenes (III b.C.), who was aware of the fact that, taking out of the interval  $[z, z^2[$  (here  $z \geq 2$  is an integer) one by one the multiples of the primes  $2, 3, 5, \dots$ , up to  $z$ , the integer left over by this "sieve" were necessarily prime numbers.

This became an algorithm to generate primes, since the XIIIrd century a.C.; then, was written by Legendre as the following formula

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

where (writing, as usual,  $p$  for a prime)

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

More in general, from the definition of sifting function and property (1.1) of Möbius function there follows, in fact, that (now on  $n \equiv 0 \pmod{q}$  will be written as  $n \equiv 0(q)$  for brevity)

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

having set

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

In order to have good estimates on the sifting function, of courif, we must approximate accurately this last quantity.

Thus, we introduce the following quantities:

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

so that  $r_1$  is small (i.e.  $X$  is a good approximation for  $|\mathcal{A}|$ ) and  $\omega_0(p)$  is such that (we write  $\mathbf{P}$  for the set of primes)

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

is small (hence  $\frac{\omega_0(p)}{p} X$  is a good approximation for  $|\mathcal{A}_p|$ ).

Then, after having given our definitions over the primes  $p$ , we define in a natural way  $\omega_0$  on the **square-free**  $d$  (i.e.,  $d$  has no square factors; equivalently,  $\mu(d)^2 = 1$ ):

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

hence,  $\omega_0$  is a multiplicative arithmetic function by definition; in a similar way we define

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

For instance (see example 1, p.16 [H-R]), if

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

we have

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

whence a good approximation is given by the choice

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

since on the square-free we then obtain

$$|r_d| \leq 1.$$

Another example: suppose that  $\mathcal{A}$  is the set of (integer) values of a (given) polynomial  $F : \mathbf{N} \rightarrow \mathbf{N}$ , with degree  $g$

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

(if  $h = o(x)$  then  $[x, x + h]$  is a "short interval" : see §5.5).

Denoting with  $\rho(d) = \rho_F(d)$  the number of distinct solutions (mod  $d$ ) of the congruence

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

we have

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

therefore a good choice is  $X = h$ ,  $\omega_0(d) = \rho(d)$  (in fact also  $\rho$  is multiplicative), whence  $|r_d| \leq \rho(d)$ .

In particular, for

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

and more in general for

$$F(n) = (an + b)(cn + d), \quad \text{with } ac \text{ not zero}$$

we have  $\rho(2) = 1$  and (except for the primes  $p$  dividing  $a$ ,  $c$ , or  $ad - bc$ )  $\rho(p) = 2$  (see §5.4, §5.5 and §5.6).

Also, in the same way, if we chooif a square-free  $q$ , coprime with every prime  $p < z$  in  $\mathcal{B}$  and "factoring in  $\mathcal{B}$ ", i.e. having all its prime factors in  $\mathcal{B}$  (we'll write "q f. in  $\mathcal{B}$ "), theif conditions are equivalent to, respectively to  $\mu^2(q) = 1$ ,  $(q, P(z)) = 1$  and  $(q, p) = 1 \quad \forall p$  prime not in  $\mathcal{B}$ ; we then have

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

whence we can hope to obtain a first estimate for the sifting function of  $\mathcal{A}_q$ , after having supplied a "good" estimate of  $|\mathcal{A}_k|$  (when  $k$  varies among the square-free).

To do this, let's define a function  $\omega$  built from  $\omega_0$ , but depending not only on  $\mathcal{A}$ , but also on  $\mathcal{B}$ : for each prime  $p$

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

and, as for  $\omega_0$ , for all square-free  $d$

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

Again, as for  $\omega_0$ ,  $\omega$  is multiplicative.

The "new" remainders

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

coincide with the "old"  $r_d$ , like for  $\omega(d) = \omega_0(d)$ , when  $\mu^2(d) = 1$  (i.e. when  $d$  is square-free) and  $p|d \Rightarrow p \in \mathcal{B}$  ( $d$  f. in  $\mathcal{B}$ ).

Let's define, also, the following products ( $\forall z \geq 2$  real)

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

If  $q$  satisfies the hypotheses in 4.2, this last gives, by definition of  $\omega$  and by Proposition 1.1

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

where  $|\theta| \leq 1$ .

In particular, for the sifting function, assuming

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

and

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

we then get, putting  $q = 1$  in the previous estimate

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

since, by Proposition 1.1, with  $\omega(n) \stackrel{def}{=} |\{p : p|n\}|$  **number of prime divisors** of  $n$

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

(see Theor. 1.1 [H-R]).

Let's see, in particular, the consequences of formula 4.1. Trivially,  $z = \sqrt{x}$ ,  $\mathcal{B} = \mathbf{P}$ ,

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

i.e., we let  $X = x$  and

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

whence

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

Thanks to Mertens formula (see [Te], p.17)

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

we get as a main term

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

which is different from  $x/\log x$  (as expected by the PNT, see §2.2.3).

This means that there is cancellation between

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

and

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

Furthermore, our estimate of the remainders (see (R) and  $(\Omega_0)$ )  $|R_d| = |\{x/d\}| \leq 2 = A_0$  implies

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

which is clearly a "huge" term w.r.t. the expected  $o(x/\log x)$ .

This last problem is due to the fact that this sum contains too many terms, whence, even if the estimate (R) is improved, we don't get enough information to obtain an acceptable remainder.

The limit of this method, like of all sieve methods, is due to the fact that, at a certain point, in order to get asymptotic formulae, an arithmetic information has to be imported.

This problem is exhaustively explained in the paper by Glyn Harman "Eratosthenes, Legendre, Vinogradov and beyond - The hidden power of the simplest sieve" (see [G-H-H], 9th paper, p.161); here, Harman also gives (in Lemma 1 of the quoted paper) a "simplified" version of the famous Vinogradov method, used by I.M. Vinogradov to bound the exponential sum over the primes (see §3.5) in his famous Three-Primes Theorem, see §3.5).

### 4.2.2 Combinatorial Sieve

As shown in the previous section, the originary Eratosthenes-Legendre Sieve is insufficient to obtain the PNT and, also, doesn't give neither good upper-bounds (see the Cebecev estimates in §2.2.1).

The key-idea of Eratosthenes-Legendre Sieve is the arithmetic identity 1.2 :

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

the function  $\mu$ , however, generates the sum

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

which has "too many terms".

The norwegian mathematician Viggo Brun, in the years between 1917 and 1924, invented the **Combinatorial Sieve**, i.e. introduced two auxiliary functions,  $\mu_1$  and  $\mu_2$ , which "approximate  $\mu$  from below and from above" (in a senif which will be clear in a moment), but "vanishing more often than  $\mu$ ".

Let's see them in the **Brun "Pure" Sieve** :

**Theorem 4.1 (Brun Pure Sieve).** *Let  $\chi_t$  be the characteristic function of the set  $\{n \in \mathbf{N} : \omega(n) \leq t\}$  (here  $\omega$  is the "prime-divisors" function).*

*Then  $\forall h \geq 0$  integer the functions*

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

*satisfy the following inequality*

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

We infer immediately the

**Corollary 4.1.** *For any integer  $h \geq 0$*

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

We derive from the Corollary the following lower and upper bound

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

which considerably improve the previous section bounds (even being, however, inferior to the elementary Cebicev estimates 2.2 in §2.2.1).

More in general we have the "Fundamental Lemma for the Combinatorial Sieve", i.e. the

**Theorem 4.2.** *Suppoif that  $\exists X \in \mathbf{R}$  and  $\exists K, A > 0$  such that*

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

and that

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

Then, uniformly w.r.t.  $\mathcal{A}$ ,  $X$ ,  $z$  and  $u \geq 1$ , we have

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

From this result we get now Cebicev-type estimates.

Using Corollary 4.1 we can give a bound for the number of **twin primes**, i.e. those **primes whose difference is 2**, up to  $x$

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

for this quantity Hardy and Littlewood (in 1922, see [H-R]) conjectured the asymptotics

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

the Combinatorial Sieve supplies, instead, the estimate

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

whence, by partial summation, it follows that their reciprocals-series converges

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

From Brun Sieve we also derive good asymptotics for the number of integers (up to  $x$ ) with all their prime divisors greater than (a fixed)  $y$  (see [Te], p.59 or other applications in chap.2 [H-R]).

### 4.2.3 Selberg sieve

The **Selberg sieve**, in its simplest form, is given by the inequality

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

where  $\lambda_1 \stackrel{\text{def}}{=} 1$  and the  $\lambda_d \in \mathbf{R} \quad \forall d \geq 2$  are arbitrary real numbers.

In fact, if  $a \in \mathcal{A}$  and  $(a, P(z)) = 1$ , in the inner sum there is only  $d = 1$  and therefore  $\lambda_1 = 1$ ; if, instead,  $a \in \mathcal{A}$  and  $(a, P(z)) > 1$ , we still have, being the inner sum a real number, that its square contributes a non-negative amount.

Expanding the square and exchanging the three sums

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

having indicated with  $[a, b]$  the least common multiple of  $a$  and  $b$ .

As in the previous sections

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

and hence, say

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

Selberg's original idea is to choose the  $\lambda_d$  ( $d \geq 2$ ) that minimize  $X \Sigma_1 + \Sigma_2$ .

However, even for "simple" sets  $\mathcal{A}$  this is a hard problem. Hence, we have to make assumptions on the  $\lambda_d$  (so to simplify the treatment). For example, we choose them to vanish for  $d \geq z$ :

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

and then choose the other  $\lambda_d$  ( $2 \leq d < z$ ) in order to minimize the quadratic form  $\Sigma_1$ . Also, we assume that

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

is an error term (i.e., negligible w.r.t.  $\Sigma_1$ ). Actually, the  $R_D$  are expected to be negligible and the non-zero  $\lambda_d$  are not too many, due to the choice 4.4.

Supposing that

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

we have that the multiplicative function

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

is well defined and  $g(d) = 0 \Leftrightarrow \omega(d) = 0$ .

Let's define the functions

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

The coefficients

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

respect the constraints  $\lambda_1 = 1$  and 4.4 (by  $G$  and  $G_k$  definitions) and it is possible to prove that they realize, with these constraints, the minimum of  $\Sigma_1$  (which is  $1/G(z)$ ).

We give now the main result regarding the Selberg sieve (for the proofs and further results and details see [H-R], chap.3  $\rightarrow$  7).

**Theorem 4.3.** *Subject to the hypothesis  $(\Omega_1)$  we have*

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

with the estimate (the dash indicates that  $d$  factors in  $\mathcal{B}$ , see §4.2.1;  $\omega(d)$  is the number of prime factors of  $d$ , see §4.2.1)

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

or, also, with the estimate

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

Also, with the further hypothesis (R) we have

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

(See the Theorems 3.1 and 3.2 in [H-R]).

The **Brun-Titchmarsh inequality** (see [H-R]) is a remarkable application of Selberg sieve.

**Theorem 4.4.** *Let  $1 \leq k < y \leq x$ , with  $k$  integer. Then, denoted with  $\pi(x; k, l) \stackrel{\text{def}}{=} |\{p \leq x : p \equiv l(k)\}|$  the number of primes up to  $x$  congruent to  $l$  modulo  $k$ , we have, for  $c > 0$  absolute constant*

$$\pi(x + y; k, l) - \pi(x; k, l) < c \frac{y}{\phi(k) \log x}.$$

As a constant  $c$  we can choose  $c = 2 + o(1)$ , when  $y/k \rightarrow \infty$  (see [Te], p.73 for a proof using Brun sieve), or  $c=2$  (due to Montgomery and Vaughan, cit. in [Te], p.76). In the following, however, we'll use the versione

$$(4.5) \quad \pi(x + y; k, l) - \pi(x; k, l) \ll \frac{y}{\phi(k) \log x}.$$

### 4.3 Large Sieve

We recall that a generic *exponential sum* of coefficients  $a_n$  is

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

and let  $\alpha_1, \alpha_2, \dots, \alpha_R \in \mathbf{R}$  be distinct modulo 1; inoltre, for  $\delta > 0$ , let

$$\|\alpha_r - \alpha_s\| \geq \delta \quad \forall r, s \text{ distinct}$$

(with  $\|\alpha\| \stackrel{\text{def}}{=} \min_{z \in \mathbf{Z}} |\alpha - z|$ ), i.e. are  $\delta$ -**well-spaced**; we define **Large Sieve** an inequality of the type ( $\Delta$  depends only on  $N$  and  $\delta$ ):

$$(4.6) \quad \sum_{r=1}^R |S(\alpha_r)|^2 \leq \Delta \sum_{n=M+1}^{M+N} |a_n|^2.$$

the optimal estimate  $\Delta = \Delta(N, \delta) = N + \delta^{-1} - 1$  has been given by Montgomery and Vaughan and, independently, by Selberg (see [Te] and [B(1)]).

For example, the  $x_j \stackrel{\text{def}}{=} j/n$  ( $j = 1, 2, \dots, n$ ) form a set of numbers  $1/n$ -well-spaced, whence Corollary 1 in [B(1)] (p.13):

**Proposition 4.1.**

$$\sum_{j=1}^R |S(j/q)|^2 \leq (N + n - 1) \sum_{n=M+1}^{M+N} |a_n|^2.$$

Also, choosing the **Farey fractions**  $a/q$ , where  $(a, q) = 1 \quad \forall q \leq Q$ ,

$$\|a/q - a'/q'\| = \|(aq' - a'q)/(qq')\| \geq 1/(qq') \geq (1/Q^2),$$

we obtain Corollary 2 in [B(1)] (p.13):

**Proposition 4.2.**

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^q |S(a/q)|^2 \leq (N + Q^2 - 1) \sum_{n=M+1}^{M+N} |a_n|^2.$$

A short account on the history of the Large Sieve has to include the first work of Linnik (1941), followed by a series of papers by Renyi, who initiated the probabilistic approach, but not yet optimal.

Then, in 1965, Roth gave the subject the nowadays shape, by means of exponential sums; this approach, modulo final adjustments due to Bombieri (see the papers: [B(2)] of the 1965, [Ga(2)] of the 1968 and [B(1)] of the 1974) is optimal. Bombieri, also, applied the Large Sieve to the study of the distribution of primes in the arithmetic progressions: see §2.5.

Renyi considered an extension of Bessel inequality with "quasi-orthogonal" vectors, to apply it directly to arithmetic functions; while Roth, instead, applied it to exponential sums.

This inequality (which can be considered a Large Sieve "ante litteram") is given by

**Proposition 4.3.** *Let  $V$  a  $\mathbf{C}$ -vector space, with inner product  $(\cdot, \cdot)$  and let  $\phi_1, \dots, \phi_R$  and  $\xi$  the vectors of  $V$ . Then*

$$\sum_{r=1}^R |(\xi, \phi_r)|^2 \leq A \|\xi\|^2,$$

where

$$A \stackrel{\text{def}}{=} \max_{r \leq R} \sum_{s=1}^R |(\phi_r, \phi_s)|.$$

In 1967 P. X. Gallagher [Ga(1)] found an alternative proof different from the previous, based on what now is known as "**Gallagher-Sobolev inequality**" (see [M(1)]).

Let's see more in detail the "probabilistic" approach of Renyi (see the Dispersion Method in §4.4).

Let  $\mathcal{N}$  be a set of  $Z$  integers in the interval  $[M+1, M+N]$  ( $M \in \mathbf{Z}$  and  $N \in \mathbf{N}$ ), with

$$Z(q, h) \stackrel{\text{def}}{=} |\{n \in \mathcal{N} : n \equiv h \pmod{q}\}|.$$

Of course,

$$\sum_{h=1}^q Z(q, h) = Z,$$

so that the **mean value** (or expected value) of  $Z(q, h)$  is  $Z/q$ .

Renyi considered the "variance"

$$V(q) \stackrel{\text{def}}{=} \sum_{h=1}^q \left( Z(q, h) - \frac{Z}{q} \right)^2$$

(here we should normalize dividing by  $q$ ).

From the orthogonality of the additive characters (see §2.4.1) and Proposition 4.2 it follows that

$$\sum_{p \leq Q} pV(p) \leq (N + 3Q^2)Z.$$

This, in turn, implies the

**Proposition 4.4.** *Let  $\mathcal{N}$  be a set of  $Z$  integers in  $[M + 1, M + N]$ . Let  $\mathcal{P}$  be a set of  $P$  prime numbers  $p$ , with  $p \leq Q$ ,  $\forall p \in \mathcal{P}$ . Let  $\tau \in ]0, 1[$  and suppose that  $Z(p, h) = 0$  for at least  $\tau p$  values of  $h \pmod{p}$ ,  $\forall p \in \mathcal{P}$ . Then*

$$Z \leq \frac{N + 3Q^2}{\tau P}.$$

## 4.4 Dispersion Method

The Dispersion Method has been introduced, in the outset of Additive Theory of Numbers, by Yu. V. Linnik in the second half of this century (see [L]).

It consists of considering, in general, the **mean-square**

$$(4.7) \quad \sum_m \left| \left( \sum_n c_{m,n} - E(m) \right) \right|^2,$$

where  $m$  and  $n$  vary in certain subset of integers, say  $\mathcal{M}$  and  $\mathcal{N}$ , and  $E(m)$  is the "expected value" of the sum  $\sum_n c_{m,n}$ .

Here the  $K$ th-order moments respect to the expected value (better, the **absolute moments** w.r.t. that value, since, in general, we have complex sums) are given by

$$\sum_m \left| \left( \sum_n c_{m,n} - E(m) \right) \right|^K$$

(we should normalize dividing by  $\sum_{m \in \mathcal{M}} 1 = |\mathcal{M}|$ ).

In particular, for  $K = 2$ , we're considering the mean-square of 4.7 above.

It represents a "variance", but in which the probability isn't normalized (can be normalized dividing, as above, by  $|\mathcal{M}|$ ) and the "expected value"  $E(m)$  isn't defined as "mean value" (i.e. as an arithmetic mean), but in such a way that

$$\sum_m \left( \sum_n c_{m,n} - E(m) \right)$$

is "small".

In Probability the variance measures the Dispersion of a stochastic variable around its mean value (also called expected value).

This ideas inspired the work of Yu. V. Linnik (see also the links with the Large Sieve, see §4.3); this was used, then, most of all in the outset of Analytic Number Theory (which, contrary to Probabilistic Theory of Numbers, doesn't use techniques from Probability Theory; see the Introduction of [Te]).

In this context, it is used especially the following (see its applications here and those in §5.5), which is the main point of the method (used also

in [C-S(2)]; i.e. the exchange of the sums over  $m$  and over the variables  $n_1, n_2$  (that come out expanding the square), so to get cancelation:

$$\sum_{n_1, n_2} \sum_m c_{m, n_1} \overline{c_{m, n_2}} - \sum_{n_1} \sum_m c_{m, n_1} \overline{E(m)} - \sum_{n_2} \sum_m \overline{c_{m, n_2}} E(m) + \sum_m |E(m)|^2$$

(see the application in §5.5.2).

In fact, we can evaluate separately the four terms, writing them as a main term plus an error term. Because of the signs, the main terms cancel; then, we are left with the errors, which give the final estimate (often in  $\mathcal{O}$ ) of the initial mean-square 4.7.

This Method has been used (for example) in 1978 by H.Iwaniec [Iw(1)] to show that there exist infinitely many (natural) numbers of the form  $n^2 + 1$  which are also primes or product of two primes (calling " $P_2$ " these type of numbers, we may abbreviate saying that " $n^2 + 1 = P_2$ " infinitely often).

See also the application to the problem of the distribution of  $n(n+2)$  (and, more in general, of quadratic reducible polynomials) in the arithmetic progressions, in the short intervals  $x < n \leq x+h$  (see §5.5 and [C-S(2)]).

## 4.5 Exponential Sums

In general, an exponential sum of coefficients  $a_n$  is

$$\sum_{N < n \leq N+M} a_n e(n\alpha),$$

where  $\alpha \in [0, 1]$ .

The estimate of exponential sums is of fundamental importance in A.N.T.

As an example, we can quote Vinogradov method (see §3.4 and §3.5), in which  $a_n = \log n$  on the primes or  $a_n = \Lambda(n)$ .

More in generale, we call "exponential sum" a sum of the kind

$$\sum_{N < n \leq N+M} a_n e(f(n)\alpha),$$

for a certain  $\alpha \in [0, 1]$  and a certain function  $f$ .

The standard approach (if  $f$  is enough "smooth" and  $a_n = 1$  or is quasi-constant) is to write these sums as integrals of exponentials (see esp. [Ti], chap. 4).

Sometimes, it may happen that  $f$  has an arithmetical meaning, but is not a "regular" function; in fact, chosen  $q \in \mathbf{N}$ , and  $\alpha = j/q$ , with  $j$  integer, we may put  $f(n) \stackrel{def}{=} \bar{n}(\bmod q)$ , i.e. **the inverse of  $n(\bmod q)$** , so to get, for  $a_n = 1$ , (a particular case of) Kloosterman sums (see §4.7).

An analogue case is given by (with  $f(n) = n$ )  $a_n = \Lambda(n)$ , which is "about" the characteristic function of the primes times a logarithm (see §2.2.2). In this case, I.M. Vinogradov (in 1937) used divisor-type functions and bilinear forms (see §4.6), in order to prove the estimate (see Theorem 3.1) from which there follows his famuos Three Primes Theorem (see §3.5).

Another remarkable example of exponential sum is (with  $a_n = 1$ )  $f(n) = n^K$ , for which we have the estimates of H. Weyl; these allow to use the Circle Method in the Waring problem (see §3.1 and [Va(1)], especially chap. 1 and 2).

Weyl estimates are based on the idea to apply to  $f$  the method of the finite differences; in fact, the Method is calles "Weyl differencing" (given in 1916) and has been refined by J.G. Van der Corput in the '20s (see [G-K], especially chap. 1 and 2).

## 4.6 Bilinear Forms

The estimate of bilinear forms of the kind

$$\sum_m \sum_n \alpha_m \beta_n f(m, n),$$

where we may suppose that the range of  $m$  and  $n$  are of the type  $]M, 2M]$  and  $]N, 2N]$  (resp.) and  $f$  is a given function, allows to obtain non-trivial results in various areas of A.N.T.

For example, to improve the level of distribution of a sequence in the arithmetic progressions (see [Iw(1)] and see §5.4).

Or, using Vaughan's Identity, to get the Vinogradov estimates for exponential sums over primes (see §2.5).

We may also give bounds for sums which can be evaluated only on average, as for example in the case of bilinear forms with Kloosterman fractions (see [D-F-I] and §5.6).

Furthermore, H.Iwaniec introduced them in order to give a more flexible form to the remainder in the "**Linear Sieve**" (see [Iw(2)] and [H-R]).

## 4.7 Kloosterman Sums

The general **Kloosterman sum** is a sum of the type ( $a, b \in \mathbf{Z}$ )

$$(4.8) \quad S(q; a, b) \stackrel{\text{def}}{=} \sum_{\substack{n \leq N \\ (n, q) = 1}} e_q(an + b\bar{n})$$

where  $n\bar{n} \equiv 1 \pmod{q}$ , i.e.  $\bar{n}$  is the inverse of  $n \pmod{q}$  (here  $q, N \in \mathbf{N}$  are fixed and  $N \leq q$ ).

In the applications it often appears also the **incomplete Kloosterman sum**

$$(4.9) \quad S(q; b) \stackrel{\text{def}}{=} \sum_{\substack{n \leq N \\ (n, q) = 1}} e_q(b\bar{n})$$

for which we have the **Weil estimate** [W] when the modulo  $q$  is prime (and, of course,  $q$  doesn't divide  $b$ , otherwise it's  $\phi(q)$ ):

$$(4.10) \quad |S(q; b)| \leq 2q^{1/2}.$$

From the properties of Kloosterman sums, there follows the estimate of Estermann [Es]

$$(4.11) \quad |S(q; a, b)| \leq d(q)q^{1/2}(q, a, b)^{1/2},$$

where we indicate with  $d(q)$  the number of divisors of  $q$  and with  $(q, a, b)$  the greatest common divisor of  $q, a$ , and  $b$ .

In particular, from the estimate  $d(q) \ll q^\epsilon$  (v. [H-W], p.260), we have the following bound for the incomplete Kloosterman sums:

$$(4.12) \quad |S(q; b)| \ll q^{1/2+\epsilon}(q, b)^{1/2}.$$

More in general, there holds the following estimate (Lemma 8 in [D-F-I])

**Proposition 4.4.** *Let  $I$  be a "segment of an arithmetic progression", i.e.*

$$I \stackrel{\text{def}}{=} \{n \in ]M, M + N] : n \equiv l \pmod{k}\},$$

$\chi$  is a Dirichlet character  $\pmod{c}$  with  $(c, k) = 1$  and  $a, b \in \mathbf{Z}$ . Then (indicating with  $\tau$  the divisor function)

$$\left| \sum_{n \in I} \bar{\chi}(n) e\left(\frac{a\bar{n} + bn}{c}\right) \right| \leq \left(\frac{X}{ck} + 2 \log 3c\right) (a, c)^{1/2} c^{1/2} \tau(c).$$

## Chapter 5

# Short Intervals Problems

### 5.1 Short Intervals Problems

This Chapter is dedicated to the original results of the Author regarding particular problems (both multiplicative and additive) in short intervals.

The first problem in this chapter (§5.2) studied by the Author is the estimate of the Selberg integral, which is a quantity checking the number of primes in "almost all" the short intervals; in particular, we get a link between this integral and the (discrete) mean-square of a remainder term in the Riemann-von Mangoldt Explicit Formula, that depends on the symmetry of distribution, around  $x$ , of the primes in the short intervals of the type  $[x - h, x + h]$  (here we may assume that  $x \in \mathbf{N}$ ).

This symmetry of distribution is linked in a natural way to the Goldbach numbers  $2x = p_1 + p_2$ , with  $p_1, p_2 \in [x - h, x + h]$ ; because of this connection the Author has successively studied the Goldbach problem with almost equal primes (§5.3).

Then, the Autore has turned to the problem of the distribution of the polynomial sequence  $n(n + 2)$  in the arithmetic progressions in short intervals, i.e. when  $n \in [x, x + h]$  (in particular, the estimate, on average over  $q \in ]Q, 2Q]$  and  $r \in ]R, 2R]$ , of the number of elements of the type  $n(n + 2)$ , with  $n \in [x, x + h]$ , which are multiples of  $qr$ ); this problem has application to the study of the primi twins (see §4.2).

For this problem, we got results (substantially independent among them) through the following three techniques :

- in §5.4 we use the Large Sieve (see §4.3);
- in §5.5 we apply the Dispersion Method (see §4.4);
- in §5.6 we employ Kloosterman sums (see §4.7).

## 5.2 Primes in almost all the Short Intervals

In this section we follow [C-V].

### 5.2.1 Introduction and statement of the results

The problem of primes in almost all the short intervals has been exposed in §2.3.

In order to get 2.10 in almost all short intervals  $[x, x + h]$  (we'll also write a.a.) we study the Selberg integral

$$J(N, H) \stackrel{def}{=} \int_N^{2N} |\psi(x + H) - \psi(x) - H|^2 dx$$

(see §1.1.2 and §2.2.2).

Of course

$$J(N, H) = o(NH^2) \Leftrightarrow \psi(x + H) - \psi(x) \sim H \quad a.a. \ x \in [N, 2N]$$

and the result quoted before can be obtained by the estimate  $J(N, H) = o(NH^2)$ , which holds in the case  $H \geq N^{1/6+\epsilon}$  and  $\epsilon > 0$  (see §2.3).

The techniques used in literature to estimate the Selberg integral are based on the classic Riemann-von Mangoldt explicit formula 1.41.

Using the Huxley estimate (see §1.2.5) A. Perelli [P] has proved that, defining

$$I'(N, T) \stackrel{def}{=} \int_N^{2N} |E(x, T)|^2 dx,$$

where  $E(x, T)$  is the remainder term in the Riemann-von Mangoldt explicit formula 1.41, we have:

$$I'(N, T) = o\left(\frac{N^3}{T^2 L}\right), T \leq N^{1-\vartheta} \Rightarrow J(N, H) = o(NH^2), H \geq N^\vartheta$$

(here  $0 < \vartheta < 1$  and  $L = \log N$  in the following).

In order to obtain the reverse implication J. Kaczorowski and A. Perelli have introduced a new form of the Riemann-von Mangoldt explicit formula, i.e. Theorem 1 in [K-P(2)] (with the choices  $q = 1$  and  $\chi = \chi_0$ ).

As in the quoted paper, let's define

$$w(u) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{if } 0 \leq u \leq 1/2 \\ 2(1-u) & \text{if } 1/2 \leq u \leq 1 \end{cases}, \quad \text{sgn}(u) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{if } u > 0 \\ 0 & \text{if } u = 0 \\ -1 & \text{if } u < 0 \end{cases}$$

$$G(x, T, n) \stackrel{\text{def}}{=} \frac{2}{T} \int_{T/2}^T \int_{\tau|\log \frac{x}{n}}^{\infty} \frac{\sin u}{u} du dt$$

to derive (in the same way as the proof of the Corollary in [K-P(2)]) the following result (see the classic explicit formula 1.41)

Let  $16 \leq N \leq x \leq 2N$ ,  $4 \leq T \leq N/4$  and  $1 \leq M \leq \frac{\min(N^{1/16}, T^{1/5})}{L^9}$ ; then

$$(5.1) \quad \psi(x) = x - \sum_{|\gamma| \leq T} w\left(\frac{|\gamma|}{T}\right) \frac{x^\rho}{\rho} + R(x, T)$$

where

$$(5.2) \quad R(x, T) = \frac{1}{\pi} \sum_{x - \frac{MN}{T} < n \leq x + \frac{MN}{T}} \Lambda(n) \text{sgn}(x-n) G(x, T, n) + \mathcal{O}\left(\frac{NL}{TM \log \frac{N}{T}} + \Lambda([x]) + 1\right).$$

In [K-P(1)] Kaczorowski and Perelli then give a link between  $J(N, H)$  and the mean-square of  $R(x, T)$ , defined by

$$I(N, T) \stackrel{\text{def}}{=} \int_N^{2N} |R(x, T)|^2 dx,$$

in the case in which  $N^\epsilon \leq H \leq N^{1-\epsilon}$ ,  $0 < \epsilon < 1/4$  and  $T$  around  $N/H$ .

Instead, we'll treat the analogue of this relation in the case  $H = \log^A N$ , with  $A$  suitable (see the following).

As regards the conditional results, Selberg proved that  $J(N, H) = o(NH^2)$ , for  $H = \infty(\log^2 N)$ , under Riemann Hypotesis and, recently, some authors have shown the same for  $H = \infty(\log N)$ , under a stronger hypothesis (the Montgomery "pair correlation" Conjecture).

In Theorem 1 of [K-P(1)] we have a non-trivial estimate for  $I(N, T)$  through a non-trivial estimate of  $J(N, H)$ ; since we deal with powers of the logarithm of  $N$ , instead of powers of  $N$ , we obtain a logarithmic factor in excess (due to the Brun-Titchmarsh inequality 4.5) in the remainder of 5.2; this gives, at last, an additional square of the logarithm in our

**Theorem 5.1** *Let  $B > 1/2$ ,  $0 < \delta < 1/4$ ,  $N^\delta \leq T \leq NL^{-2B}$  and  $1 \leq M \leq L^B$ . Then*

$$I(N, T) \ll M^2 J(N, H) + \frac{N^3}{T^2} \left( \frac{L \log(M+1)}{M \log \frac{N}{TM}} \right)^2,$$

where  $H = \frac{N}{TM}$ .

Since our proof is essentially the same of that for Theorem 1 in [K-P(1)] (but this time we use 5.1 and 5.2 instead of the Corollary of [K-P(2)]), we'll omit it.

The opposite bound, of  $J(N, H)$  through  $I(N, T)$ , given in Theorem 2 of [K-P(1)], requires a better estimate for the remainder of  $R(x, T)$ , since now  $T$  varies in a much larger range.

The main novelty of our paper is then the estimate of the difference  $R(x, T) - R([x], T)$ ; which is given by the Lemma in the next section, in which we bound the main term of the remainders in 5.2 to get a non-trivial estimate.

Let  $0 < \delta < 1/8$ ,  $K \geq 1$ ,

$$J \stackrel{def}{=} \log_2 \left( \frac{L^{1/2} K N^{1-\delta}}{H} \right)$$

(here the logarithm is in base 2) and for  $j = 1, \dots, J$  we define

$$H_j \stackrel{def}{=} \frac{2^j H}{2L^{1/2} K} \quad \text{e} \quad T_j \stackrel{def}{=} \frac{N}{100H_j},$$

whence

$$\frac{H}{L^{1/2} K} \leq H_j \leq \frac{N^{1-\delta}}{2} \quad \text{e} \quad \frac{N^\delta}{50} \leq T_j \leq \frac{NL^{1/2} K}{100H}.$$

We have the following

**Theorem 5.2.** *Let  $\epsilon > 0$ ,  $H \geq L^{311+\epsilon}$  and  $1 \leq K \leq L^{1/2}$ . Then*

$$J(N, H) \ll H^2 \sum_{j=1}^J H_j^{-2} I(N, T_j) + \\ + NH^2 \left( \frac{1}{K^2} + \left( \frac{KL^{1/2}}{H} \right)^{\frac{6}{155}} + \frac{HL^2}{N \log^2 H} \right).$$

If we choose  $B = 1 + \epsilon$ ,  $\epsilon > 0$  and  $M = L^B$  in Theorem 5.1 we easily obtain the following

**Corollary 5.1.** *If  $\epsilon > 0$ ,  $0 < \delta < 1/4$  and  $L^{1+\epsilon} \leq H \leq N^{1-\delta}$  then*

$$J(N, H) = o(NH^2) \Rightarrow I(N, T) = o\left(\frac{N^3}{T^2}\right), \forall T : N^\delta \leq T \leq \frac{N}{L^{2+2\epsilon}}.$$

Theorem 5.2 gives the converse of the last result, if  $K \rightarrow \infty$  and  $K = o(L^\epsilon)$ , thanks to the following

**Corollary 5.2.** *Let  $\epsilon > 0$ ,  $0 < \delta < 1/8$ ; then, for  $H \geq L^{311+\epsilon}$  and  $H = o(N)$  we have*

$$I(N, T) = o\left(\frac{N^3}{T^2 L}\right), \forall T \in \left[ \frac{N^\delta}{50}, \frac{NL^{1/2}K}{100H} \right] \Rightarrow J(N, H) = o(NH^2),$$

where  $K \rightarrow \infty$  and  $K = o(L^\epsilon)$  (for  $N \rightarrow \infty$ ).

We remark that, for our short intervals, the requirement on the mean square of  $R(x, T)$  to obtain  $J(N, H) = o(NH^2)$  is extended to a much larger set of values of  $T$ .

We'll see, in the next section, the Proof of Lemma 1 of [C-V].

For the complete Proof of Theorem 5.2 see [C-V] and the correction:

G. Coppola, A. Vitolo - CORRIGENDUM TO OUR PAPER "ON THE DISTRIBUTION OF PRIMES IN INTERVALS OF LENGTH  $\log^\theta N$ " - Acta Math. Hungar. **78(4)** (1998), 359-361.

### 5.2.2 Statement and Proof of Lemma 1

**Lemma 5.1.** *Let  $\{a_n\}_{n \in \mathbf{N}}$  be a sequence of complex numbers,  $x \geq 4$ ,  $c = 1 + \frac{1}{\log x}$ ,  $A_0(x) = \sum_{n < x} a_n + \frac{a_x}{2}$  (here  $a_x = 0$  if  $x$  is not in  $\mathbf{N}$ ) and  $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$  be absolutely convergent in  $\sigma = \operatorname{Re}(s) > 1$ ; then for  $\tau \in (T/2, T]$ ,  $T \rightarrow \infty$  and  $T = o(x)$  when  $x \rightarrow \infty$ , we have*

$$A_0(x) = \frac{1}{2\pi i} \int_{c-i\tau}^{c+i\tau} f(s) \frac{x^s}{s} ds + g(x, \tau),$$

where

$$\begin{aligned} \frac{2}{T} \int_{T/2}^T (g(x, \tau) - g([x], \tau)) d\tau &\ll \frac{1}{T^2} \sum_{n \leq \frac{x}{2}} \frac{|a_n|}{\log^2 \frac{x}{n}} + \sum_{x - \frac{x}{T} < n \leq x + \frac{x}{T}} |a_n| + \\ &+ \frac{1}{T} \sum_{n \in I} |a_n| \left( \frac{1}{x \log^2 \frac{x}{n}} + \frac{1}{T} \right) + \frac{x}{T^2} \sum_{n > 2x} \frac{|a_n|}{n^c \log^2 \frac{x}{n}}, \end{aligned}$$

with  $I$  the set of the integers in the intervals  $(x/2, x - \frac{x}{T}]$ ,  $(x + \frac{x}{T}, 2x]$ .

**Proof** By Perron inversion formula and the absolute convergence of  $f(s)$  for  $\sigma > 1$  we have

$$\begin{aligned} (5.3) \quad A_0(y) &= \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} f(s) \frac{y^s}{s} ds = \\ &= \frac{1}{2\pi i} \int_{c-i\tau}^{c+i\tau} f(s) \frac{y^s}{s} ds + \sum_{n=1}^{\infty} a_n \mathcal{I}(n, y, \tau) \end{aligned}$$

with  $y = x$  or  $y = [x]$ ,  $\tau \in (T/2, T]$  and

$$(5.4) \quad \mathcal{I}(n, y, \tau) = \frac{1}{2\pi i} \int_{\substack{\sigma=c \\ |t|>\tau}} \left(\frac{y}{n}\right)^s \frac{ds}{s}.$$

We remark that, in virtue of 5.3 and 5.4, the estimate in the Proof of Theorem 1 in the paper by Dieter Wolke (cit. in [C-V]), combined with

$$\frac{2}{T} \int_{T/2}^T (\mathcal{I}(n, x, \tau) - \mathcal{I}(n, [x], \tau)) d\tau \ll \left| \frac{2}{T} \int_{T/2}^T \mathcal{I}(n, x, \tau) d\tau \right| +$$

$$+ \left| \frac{2}{T} \int_{T/2}^T \mathcal{I}(n, [x], \tau) d\tau \right|,$$

give the Lemma for  $n$  not in  $I$ .

If  $n \in I$  we proceed as follows.

Let  $y = x$  in 5.4 and  $\ell \stackrel{def}{=} \log(x/n)$  to get

$$\begin{aligned} \mathcal{I}(n, x, \tau) &= \frac{1}{\pi} \left(\frac{x}{n}\right)^c \int_{\tau}^{\infty} \frac{c \cos \ell t + t \sin \ell t}{c^2 + t^2} dt \\ &= \frac{1}{\pi} \left(\frac{x}{n}\right)^c \int_{\tau}^{\infty} \frac{c \cos \ell t + t \sin \ell t}{t^2} dt + \mathcal{O} \left( \left(\frac{x}{n}\right)^c \left( \int_{\tau}^{\infty} \frac{1}{t^4} d\tau + \int_{\tau}^{\infty} \frac{1}{t^3} d\tau \right) \right); \end{aligned}$$

since  $\tau \gg T$  and  $(x/n)^c \ll 1 \quad \forall n \in I$ , we obtain

$$(5.5) \quad \mathcal{I}(n, x, \tau) = \frac{1}{\pi} \left(\frac{x}{n}\right)^c \int_{\tau}^{\infty} \frac{c \cos \ell t + t \sin \ell t}{t^2} dt + \mathcal{O} \left( \frac{1}{T^2} \right);$$

in the same way, letting  $y = [x]$  in 5.4 and  $w = \log([x]/n)$  we have

$$(5.6) \quad \mathcal{I}(n, [x], \tau) = \frac{1}{\pi} \left(\frac{[x]}{n}\right)^c \int_{\tau}^{\infty} \frac{c \cos w t + t \sin w t}{t^2} dt + \mathcal{O} \left( \frac{1}{T^2} \right).$$

Also,  $D \stackrel{def}{=} \ell - w = \log \left( 1 + \frac{\{x\}}{[x]} \right) \ll \frac{1}{x}$  and

$$(5.7) \quad n \in I \Rightarrow 1 \ll |\ell|T, |w|T \ll T;$$

in particular,  $T = o(x)$  implies

$$(5.8) \quad \frac{1}{|w|} \ll \frac{1}{|\ell|}.$$

Hence, being  $\left( 1 + \frac{\{x\}}{[x]} \right)^c = 1 + \mathcal{O}(\frac{1}{x})$ , on integrating 5.5 by parts

$$\mathcal{I}(n, x, \tau) = \frac{1}{\pi} \left(\frac{[x]}{n}\right)^c \int_{\tau}^{\infty} \frac{\sin \ell t}{t} + \frac{c \cos \ell t}{t^2} dt + \mathcal{O} \left( \frac{1}{xT|\ell|} + \frac{1}{T^2} \right);$$

in the same way we obtain by 5.6, thanks to 5.7 and 5.8

$$\begin{aligned} & \mathcal{I}(n, x, \tau) - \mathcal{I}(n, [x], \tau) = \\ &= \frac{1}{\pi} \left( \frac{[x]}{n} \right)^c \int_{\tau}^{\infty} \frac{\sin \ell t - \sin w t}{t} + c \frac{\cos \ell t - \cos w t}{t^2} dt + \mathcal{O} \left( \frac{1}{xT|\ell|} + \frac{1}{T^2} \right). \end{aligned}$$

Since  $([x]/n)^c \ll 1 \quad \forall n \in I$ , we only have to prove, say, that

$$(5.9) \quad \frac{2}{T} \int_{T/2}^T \int_{\tau}^{\infty} \frac{\sin \ell t - \sin w t}{t} dt d\tau \ll \frac{1}{xT\ell^2}$$

and that

$$(5.10) \quad \frac{2}{T} \int_{T/2}^T \int_{\tau}^{\infty} \frac{\cos \ell t - \cos w t}{t^2} dt d\tau \ll \frac{1}{xT\ell^2}$$

to get the Lemma.

Integrating twice by parts 5.9 and 5.10, since for  $x$  enough large  $1/D > [x] > T$ , we can bound the integrals on  $(\tau, 1/D)$  and  $(1/D, \infty)$  to obtain the required estimate.

### 5.3 Goldbach Problem with almost equal primes

In this section we give the generalization of the Chudakov-van der Corput-Estermann Theorem (cit. in [Va(1)]) on the exceptional set in the binary Goldbach problem to a problem with "almost equal" primes; i.e. we prove that the equation  $p_1 + p_2 = 2n$  is satisfied by almost all the  $2n \in [N, 2N]$  when the primes  $p_1$  and  $p_2$  are in the interval  $[n-U, n+U]$ , with  $U = n^{5/8+\epsilon}$ . Furthermore, we explicitly estimate the number of representations of these  $2n$  as a sum of such primes (see Theorem 5.3).

(The section will be structured as [C-L(2)]; the notation doesn't follow the one in Chapter 3, but is independent, see also §5.3.1).

In the (binary) Goldbach problem, the Chudakov-van der Corput-Estermann Theorem [Va(1), chap.3] gives that the number  $E(N)$  of even numbers  $n \leq N$  for which  $n$  is not the sum of 2 primes satisfies  $E(N) \ll NL^{-A}$ , where  $L = \log N$  and  $A > 0$  is an absolute constant.

The Vinogradov Three Primes Theorem [Vi] asserts that every enough large odd integer  $N$  can be represented as  $N = p_1 + p_2 + p_3$ , with  $p_i$  ( $i = 1, 2, 3$ ) primes (see §3.5 and §3.6). Many authors have proved that this Theorem still holds under the further restriction  $|p_i - N/3| \ll N^{\theta+\epsilon}$  ( $\theta < 1$ ),  $i = 1, 2, 3$  ( $\theta = 63/64, 160/183, 2/3, 91/96$  : cit. in [C-L(2)]).

Assuming G.R.H. (see §1.3.3), Wolke (cit. in [C-L(2)]) obtained the same result with  $|p_i - N/3| \leq N^{1/2}(\log N)^{7+\epsilon}$ ,  $i = 1, 2, 3$ .

Then, improving previous unconditional results, Zhan Tao [Z] gave the Theorem for  $\theta = 5/8$ . Also, his method gives an asymptotic formula for the number of representations  $R(N)$ . Using the Circle Method (see §3.3), the problem in [Z] is reduced to obtain non-trivial estimates for exponential sums over primes in short intervals.

In some cases the estimates depend on density theorems in short intervals. In other cases are applied Heath-Brown identity (see §2.5) and standard analytic techniques based on the mean values of Dirichlet  $L$ -functions.

We prove, by using Zhan Tao's techniques, an analogous result for the corresponding binary problem

$$(5.11) \quad 2n = p_1 + p_2, \quad n - U \leq p_1, p_2 \leq n + U.$$

More precisely, let (these notations and the following in the section are different from those of Chapter 3)

$$R(2n) = R(2n, U) \stackrel{def}{=} \sum_{\substack{h+k=2n \\ n-U < h, k \leq n+U}} \Lambda(h)\Lambda(k),$$

$$\mathfrak{S}(2n) \stackrel{def}{=} 2 \prod_{\substack{p|n \\ p>2}} \left( \frac{p-1}{p-2} \right) \prod_{p>2} \left( 1 - \frac{1}{(p-1)^2} \right),$$

where  $\Lambda$  is von-Mangoldt function (see §1.1.2).

We have the

**Theorem 5.3.** *Let  $\varepsilon, A > 0$  be arbitrary constants and  $N^{5/8+\varepsilon} \leq U \leq N$ . Then*

$$\sum_{N \leq 2n \leq 2N} |R(2n) - 2U\mathfrak{S}(2n)|^2 \ll_{\varepsilon, A} NU^2 L^{-A}.$$

Theorem 5.3 implies the

**Corollary 5.3.** *Let  $\varepsilon > 0$  and  $A > 0$  be arbitrary constants. Then  $\forall 2n \in [N, 2N]$ , save  $\mathcal{O}(NL^{-A})$  exceptions, the equation 5.11 is soluble for  $U = n^{5/8+\varepsilon}$  and we have*

$$R(2n) = 2U\mathfrak{S}(2n) + \mathcal{O}(UL^{-A}).$$

Further improvings of Zhan Tao's results have been obtained by Jia, with  $U = n^{7/12+\varepsilon}$  (cit. in [C-L(2)] and [C-L(3)]). However, he uses Sieve methods (see §4.2 and §4.3), which give only a lower bound for the number of representations. Jia deduces his result proving that for an even  $n$  such that  $2P < n \leq 2P + U$ , with  $\mathcal{O}(U \log^{-2} P)$  exceptions, we have

$$(5.12) \{ (p_1, p_2) : n = p_1 + p_2, P < p_1 \leq P + U, P - U < p_2 \leq P + U \}$$

$$\gg \mathfrak{S}(n) \frac{U}{\log^2 P},$$

where  $P$  is a sufficiently large integer,  $\varepsilon$  is a sufficiently small positive constant, and  $U = P^{7/12+40\varepsilon}$ . Recently, Mikawa has established independently the same result of Jia without using a Theorem of the form 5.12 (cit. in [C-L(2)] and [C-L(3)]). See also [C-L(3)], as regards the applications of Sieve methods to this problem.

### 5.3.1 Notations

$A$  - an arbitrary positive constant,  
 $B, C, D$  - positive constants depending on  $A$ ,  
 $\varepsilon$  - an arbitrarily small positive constant,  
 $V, Y$  - positive integers such that  $N^{7/12+\varepsilon} \leq Y \leq V$ ,  
 $N, U$  - positive integers such that  $N^{5/8+\varepsilon} \leq U \leq N$ ,  
 $H = UL^{-B}$ ,  
 $T \sim \frac{N}{4H}$ ,  
 $\omega = N^{-1}U^2L^{-D}$ ,  
 $P = L^C$ ,  
 $n_1, n_2, \dots, n_T$  - integers such that  $N/2 \leq n_1 < n_2 < \dots < n_T \leq N$ ,

$$S(\alpha; V, Y) \stackrel{def}{=} \sum_{V-Y < h \leq V} \Lambda(h)e(h\alpha),$$

$$S_n(\alpha) \stackrel{def}{=} S(\alpha; n+U, 2U), \quad T_n(\eta) \stackrel{def}{=} \sum_{n-U < h \leq n+U} e(h\eta).$$

$$I_{q,a} \stackrel{def}{=} \left\{ \frac{a}{q} + \eta, \eta \in \xi_q \right\}, \quad \text{con } \xi_q = \left( -\frac{L^D}{U}, \frac{L^D}{U} \right).$$

$$\mathfrak{M} \stackrel{def}{=} \bigcup_{q \leq P} \bigcup_{\substack{a=1 \\ (a,q)=1}}^q I_{q,a}, \quad \text{ed } \mathfrak{m} \stackrel{def}{=} \left[ \frac{1}{\omega}, 1 + \frac{1}{\omega} \right] \setminus \mathfrak{M}.$$

$$\sum_{a=1}^q \stackrel{*}{def} \sum_{\substack{a=1 \\ (a,q)=1}}^q, \quad \delta_\chi \stackrel{def}{=} \begin{cases} 1 & \text{if } \chi = \chi_o \\ 0 & \text{otherwise} \end{cases}, \quad \|\beta\| \stackrel{def}{=} \min_{n \in \mathbf{Z}} |\beta - n|.$$

$$\tau(\chi) \stackrel{def}{=} \sum_{a=1}^q \chi(a) e\left(\frac{a}{q}\right), \quad \text{Gauss sum (see §2.4.2)}$$

$$\psi(x, \chi) \stackrel{def}{=} \sum_{n \leq x} \Lambda(n) \chi(n) \quad (\text{see §1.4.3}).$$

### 5.3.2 Sketch of the Proof

We have

$$R(2n) = \int_0^1 S_n(\alpha)^2 e(-2n\alpha) d\alpha.$$

Hence

$$\sum_{N \leq 2n \leq 2N} |R(2n) - 2U \mathfrak{S}(2n)|^2 \ll \sum_{\mathfrak{m}} + \sum_{\mathfrak{M}},$$

where

$$\begin{aligned} \sum_{\mathfrak{m}} &= \sum_{N \leq 2n \leq 2N} \left| \int_{\mathfrak{m}} S_n(\alpha)^2 e(-2n\alpha) d\alpha \right|^2, \\ \sum_{\mathfrak{M}} &= \sum_{N \leq 2n \leq 2N} \left| \int_{\mathfrak{M}} S_n(\alpha)^2 e(-2n\alpha) d\alpha - 2U \mathfrak{S}(2n) \right|^2. \end{aligned}$$

In order to prove Theorem 5.3 it is sufficient to prove that

$$(5.13) \quad \sum_{\mathfrak{M}} \ll NU^2 L^{-A},$$

$$(5.14) \quad \sum_{\mathfrak{m}} \ll NU^2 L^{-A}.$$

### 5.3.3 Major Arcs Estimates

Let  $\alpha \in I_{q,a}$ . Then

$$\begin{aligned} S_n(\alpha) &= \sum_{n-U < h \leq n+U} \Lambda(h) e(h\alpha) = \\ &= \sum_{\substack{n-U < h \leq n+U \\ (h,q)=1}} \Lambda(h) e\left(\frac{ah}{q}\right) e(h\eta) + \mathcal{O}(L^2) = \\ &= \sum_{b=1}^q e\left(\frac{ab}{q}\right) \sum_{\substack{n-U < h \leq n+U \\ h \equiv b \pmod{q}}} \Lambda(h) e(h\eta) + \mathcal{O}(L^2) = \end{aligned}$$

$$\begin{aligned} \frac{1}{\varphi(q)} \sum_{\chi} \sum_{n-U < h \leq n+U} \Lambda(h) \chi(h) e(h\eta) \sum_{b=1}^q \bar{\chi}(b) e\left(\frac{ab}{q}\right) + \mathcal{O}(L^2) = \\ \frac{1}{\varphi(q)} \sum_{\chi} \chi(a) \tau(\bar{\chi}) W_n(\chi, \eta) + \frac{\mu(q)}{\varphi(q)} T_n(\eta) + \mathcal{O}(L^2), \end{aligned}$$

where

$$W_n(\chi, \eta) \stackrel{def}{=} \sum_{n-U < h \leq n+U} \Lambda(h) \chi(h) e(h\eta) - \delta_{\chi} T_n(\eta).$$

We use now the following version of Siegel-Walfisz Theorem for short intervals (see [P-P-S(1)], [P-P-S(2)] and §2.4.3).

If  $V^{7/12+\varepsilon} \leq Y \leq V$  and  $q \leq P = L^C$ , then

$$\psi(V, \chi) - \psi(V - Y, \chi) = \delta_{\chi} Y + \mathcal{O}_{\varepsilon, C, C_1}(Y L^{-C_1}), \quad \forall \chi \pmod{q}, \forall C_1 > 0.$$

If  $U \geq n^{5/8+\varepsilon}$ , then by partial summation (see Lemma 2.1, §2.2.2), from the previous result above and the estimate  $\tau(\chi) \ll q^{1/2}$  (see §2.4.2),

$$S_n(\alpha) = \frac{\mu(q)}{\varphi(q)} T_n(\eta) + \mathcal{O}(U P^{1/2} L^{D-C_1}),$$

uniformly for  $\eta \in \xi_q$ ,  $q \leq P$  and  $(a, q) = 1$ .

Thus, write

$$\begin{aligned} \int_{I_{a,q}} S_n(\alpha)^2 e(-2n\alpha) d\alpha &= \frac{\mu(q)^2}{\varphi(q)^2} e\left(-\frac{2na}{q}\right) \int_{\xi_q} T_n(\eta)^2 e(-2n\eta) d\eta \\ &+ \mathcal{O}(U P L^{-2C_1+3D}) = \frac{\mu(q)^2}{\varphi(q)^2} e\left(-\frac{2na}{q}\right) \int_0^1 T_n(\eta)^2 e(-2n\eta) d\eta \\ &+ \mathcal{O}(U P L^{-2C_1+3D}) + \mathcal{O}\left(\frac{U L^{-D}}{\varphi(q)^2}\right). \end{aligned}$$

Then, we have

$$\int_{\mathfrak{M}} S_n(\alpha)^2 e(-2n\alpha) d\alpha = 2U \mathfrak{S}(2n, P) + \mathcal{O}(T_1) + \mathcal{O}(T_2),$$

where

$$\mathfrak{S}(2n, P) = \sum_{q \leq P} \sum_{a=1}^q \frac{\mu(q)^2}{\varphi(q)^2} e\left(-\frac{2na}{q}\right),$$

$$T_1 = UP^3L^{-2C_1+3D}, \quad T_2 = UL^{-D+1}.$$

By classic arguments ([Va], chap.3), we obtain

$$\sum_{N \leq 2n \leq 2N} |\mathfrak{S}(2n, P) - \mathfrak{S}(2n)|^2 \ll NP^{-1}L^2,$$

where

$$\mathfrak{S}(2n) = \sum_{q=1}^{\infty} \sum_{a=1}^q \frac{\mu(q)^2}{\varphi(q)^2} e\left(-\frac{2na}{q}\right).$$

We therefore get

$$\begin{aligned} \sum_{\mathfrak{M}} &= \sum_{N \leq 2n \leq 2N} \left| \int_{\mathfrak{M}} S_n(\alpha)^2 e(-2n\alpha) d\alpha - 2U \mathfrak{S}(2n) \right|^2 \ll \\ &U^2 \sum_{N \leq 2n \leq 2N} |\mathfrak{S}(2n, P) - \mathfrak{S}(2n)|^2 + \\ &+ \sum_{N \leq 2n \leq 2N} \left| \int_{\mathfrak{M}} S_n(\alpha)^2 e(-2n\alpha) d\alpha - 2U \mathfrak{S}(2n, P) \right|^2 \ll \\ &\ll NU^2 P^{-1} L^2 + NU^2 P^6 L^{-4C_1+6D} + NU^2 L^{-2D+2} \ll NU^2 L^{-A}, \end{aligned}$$

i.e. 5.13, in the hypothesis

$$C > A + 2, \quad 2D > A + 2, \quad 4C_1 > A + 6(C + D).$$

### 5.3.4 Minor Arcs Estimates

We prove now 5.14.

Let's consider the integers  $n_1, n_2, \dots, n_T$  such that

$$N/2 \leq n_1 < n_2 < \dots < n_T \leq N \quad \text{and} \quad \left[ \frac{N}{2}, N \right] \subset \bigcup_{i=1}^T I_i,$$

with  $I_i \stackrel{\text{def}}{=} [n_i - H, n_i + H]$ . For every  $n \in I_i$ , we put

$$S_n(\alpha) - S_{n_i}(\alpha) = S^+(\alpha) + S^-(\alpha),$$

where

$$S^+(\alpha) \stackrel{def}{=} \begin{cases} S(\alpha; n_i - U, n_i - n), & \text{se } n < n_i, \\ 0, & \text{se } n = n_i, \\ S(\alpha; n + U, n - n_i), & \text{se } n_i < n, \end{cases}$$

$$S^-(\alpha) \stackrel{def}{=} \begin{cases} -S(\alpha; n_i + U, n_i - n), & \text{se } n < n_i, \\ 0, & \text{se } n = n_i, \\ -S(\alpha; n - U, n - n_i), & \text{se } n_i < n. \end{cases}$$

Then, write

$$\begin{aligned} & \left| \int_{\mathbf{m}} S_n(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 \ll \left| \int_{\mathbf{m}} S_{n_i}(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 + \\ & \quad + \left| \int_{\mathbf{m}} S^+(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 + \\ & + \left| \int_{\mathbf{m}} S^-(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 + \left| \int_{\mathbf{m}} S^+(\alpha) S^-(\alpha) e(-2n\alpha) d\alpha \right|^2 + \\ & + \left| \int_{\mathbf{m}} S_{n_i}(\alpha) S^+(\alpha) e(-2n\alpha) d\alpha \right|^2 + \left| \int_{\mathbf{m}} S_{n_i}(\alpha) S^-(\alpha) e(-2n\alpha) d\alpha \right|^2. \end{aligned}$$

Using Cauchy-Schwarz inequality and Parseval identity, we obtain

$$\begin{aligned} & \left| \int_{\mathbf{m}} S^+(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 \ll H^2 L^4, \\ & \left| \int_{\mathbf{m}} S^-(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 \ll H^2 L^4, \\ & \left| \int_{\mathbf{m}} S^+(\alpha) S^-(\alpha) e(-2n\alpha) d\alpha \right|^2 \ll H^2 L^4, \\ & \left| \int_{\mathbf{m}} S_{n_i}(\alpha) S^+(\alpha) e(-2n\alpha) d\alpha \right|^2 \ll UHL^4, \\ & \left| \int_{\mathbf{m}} S_{n_i}(\alpha) S^-(\alpha) e(-2n\alpha) d\alpha \right|^2 \ll UHL^4. \end{aligned}$$

Thus, we get

$$(5.15) \quad \sum_{\mathbf{m}} \ll \sum_{i=1}^T \sum_{n \in I_i} \left| \int_{\mathbf{m}} S_n(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 \ll \\ \sum_{i=1}^T \sum_{n \in I_i} \left| \int_{\mathbf{m}} S_{n_i}(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 + NUHL^4.$$

Since  $N^{5/8+\varepsilon} \leq U \leq N$ , we obtain from Theorems 2 and 3 of [Z] that  $\forall B' > 0$ ,

$$S_{n_i}(\alpha) = S(\alpha; n_i + U, 2U) \ll UL^{-B'}, \quad \forall \alpha \in \mathbf{m}.$$

Hence, by Bessel inequality and Parseval identity, we conclude that

$$(5.16) \quad \sum_{n \in I_i} \left| \int_{\mathbf{m}} S_{n_i}(\alpha)^2 e(-2n\alpha) d\alpha \right|^2 \ll \int_{\mathbf{m}} |S_{n_i}(\alpha)|^4 d\alpha \\ \ll U^3 L^{-2(B'-1)}.$$

The 5.14 follows from 5.15 and 5.16 if  $A + 4 < B < 2B' - A - 2$ , whence Theorem 5.3 is completely proved.

## 5.4 Large Sieve and $n(n+2)$ in short intervals

In this section we display the results in [C-S(1)] on the distribution in the arithmetic progressions of the polynomial  $n(n+2)$ , and, also, of quadratic reducible polynomials, in short intervals  $n \in [x, x+h]$ .

### 5.4.1 Statement of the results

We expect that, on average on the odd square-free moduli  $d$ , the following estimate holds (now on we write  $m \equiv 0(q)$  to mean  $m \equiv 0(\text{mod } q)$ )

$$\sum_{\substack{x < n \leq x+h \\ n(n+2) \equiv 0(d)}} 1 = \frac{h}{d} \sum_{\substack{t|d \\ \frac{d}{x+n} < t < x+h}} 1 + R_d(x, h)$$

where  $h = x^\vartheta$  is the length of the short interval and  $R_d(x, h)$  is a "good" error term, on average over  $d \sim D$ , i.e. on  $D < d \leq 2D$ .

If this holds with  $D = x^{\alpha-\varepsilon}$  ( $\varepsilon \in ]0, \alpha[$ ), we say that the **level of distribution** of our sequence (here  $n(n+2)$ ), in the arithmetic progressions, is (at least)  $\alpha$ .

For example, by standard arguments, the level of distribution of  $n(n+2)$  with  $n \in [x, x+x^\vartheta]$  at least  $\vartheta$ . See also [H-R], where the classic Sieve results are applied (see esp. §4.2.1).

A better level of distribution of a sequence in the arithmetic progressions is usually obtained through the use of bilinear forms (see §4.6).

In the bilinear forms we'll consider the coefficients  $\gamma_q$  and  $\delta_r$  (with  $q \sim Q$  and  $r \sim R$ ) are bounded arithmetic functions. Here the level of distribution is obviously  $\log(QR)/\log(x)$ .

An important example of non-trivial treatment is the bilinear form of the remainder term which we quote, relative to the sequence  $n^2+1$ .

Iwaniec proved in 1978 [Iw(1)] that the level of distribution in this case is  $16/15$ . Using this, he was able to prove that  $n^2 + 1 = P_2$  for infinitely many  $n$  (here  $P_k$  denotes **an integer with at most  $k$  prime factors**), while the trivial level of distribution, i.e. 1, allows to get only  $P_3$ .

In our case we study the bilinear form restricted to prime moduli, i.e.

$$\sum_{q \sim Q} \sum_{r \sim R} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n(n+2) \equiv 0(qr)}} 1,$$

where  $q$  and  $r$  are distinct primes (assuming  $QR > 2h + 2$ ).

This restriction is due to the arithmetic nature of the problem and, also, is essential in our proof, as in the results about this problem we'll quote in the following.

We manage to treat, in the future, also the case of general moduli.

We expect that the following estimate holds on average

$$\sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n(n+2) \equiv 0(qr)}} 1 = \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \left( \frac{2h}{qr} + \sum_{\substack{x < n \leq x+h \\ n \equiv 0(qr)}} 1 + \sum_{\substack{x < n \leq x+h \\ n \equiv -2(qr)}} 1 \right),$$

with a "good" error term, i.e.  $\mathcal{O}(h^{1-\varepsilon})$ .

In [S-V] Salerno and Vitolo obtained level of distribution  $4/3$  for long intervals, using the Weil estimate for Kloosterman sums (see Lemma 3 of [Ho]; also, §4.7).

In this section we use the Large Sieve to improve the level of distribution from  $4/3$  to  $3/2$  (when  $h = x$ ) and, also, to generalize the results of [S-V] to short intervals.

The level of distribution reached in this way for short intervals of the kind  $[x, x + x^\vartheta]$  is  $3\vartheta - 3/2$  and hence better than the classical level (i.e.  $\vartheta$ ) when  $\vartheta > 3/4$  (we include the case  $\vartheta = 1$  of "long" intervals).

Let's give the results.

**Theorem 5.4.** *Let  $x > 4$ ,  $3/4 < \vartheta \leq 1$ ,  $x^\vartheta \leq h \leq x$ ,  $0 < \varepsilon < \frac{4\vartheta-3}{10}$ ; let  $Q, R \in [1, h/2[$  and let  $\gamma_q, \delta_r$  be bounded arithmetic functions with support on the primes in the intervals  $]Q, 2Q], ]R, 2R]$  (resp.). Then for  $(q, r) = 1$*

$$(5.17) \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n(n+2) \equiv 0(qr)}} 1 = \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \left( \frac{2h}{qr} + \sum_{\substack{x < n \leq x+h \\ n \equiv 0(qr)}} 1 + \sum_{\substack{x < n \leq x+h \\ n \equiv -2(qr)}} 1 \right) + \mathcal{O}(h^{1-\varepsilon}),$$

provided  $R \leq h^2/x^{1+3\varepsilon}$ ,  $Q \leq h/x^{1/2+2\varepsilon}$ ,  $QR > 2h + 2$ .

As in the application we get level of distribution  $3(\vartheta - 1/2)$ :

**Corollary 5.4.** *Let  $x, \vartheta, \varepsilon, q, r, \gamma_q, \delta_r$  be as above; let  $h = x^\vartheta$ . Then the estimate 5.17 of Theorem 5.4 holds for  $QR = x^{3\vartheta-3/2-5\varepsilon}$ .*

As in [S-V] we can easily generalize Theorem 5.4 and Corollary 5.4 to quadratic reducible polynomials, proving

**Corollary 5.5.** *Let  $(an + b)(cn + d)$  be a polynomial without fixed divisors. Let  $x, \vartheta, h, \varepsilon, q, r, \gamma_q$  and  $\delta_r$  be as above, with  $qr$  coprime with  $[a, c, ad - bc]$ . Then the same conclusions of Theorem 5.4 and of Corollary 5.4 hold true with  $(an + b)(cn + d)$  instead of  $n(n + 2)$ .*

## 5.4.2 Proof of the Theorem and of the Corollaries

Let  $q$  and  $r$  be distinct primes (as in the following) and define

$$I \stackrel{\text{def}}{=} \sum_{q \sim Q} \sum_{r \sim R} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n(n+2) \equiv 0(qr)}} 1.$$

Since  $q$  and  $r$  are distinct primes

$$I = \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \left( \sum_{\substack{x < n \leq x+h \\ n \equiv 0(r) \\ n \equiv -2(q)}} 1 + \sum_{\substack{x < n \leq x+h \\ n \equiv 0(q) \\ n \equiv -2(r)}} 1 + \sum_{\substack{x < n \leq x+h \\ n \equiv 0(qr)}} 1 + \sum_{\substack{x < n \leq x+h \\ n \equiv -2(qr)}} 1 \right).$$

Hence, to prove 5.17 it will suffice to prove that

$$(5.18) \quad \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n \equiv 0(r) \\ n \equiv -2(q)}} 1 = h \sum_{\substack{q \sim Q \\ r \sim R}} \frac{\gamma_q \delta_r}{qr} + \mathcal{O}(h^{1-\varepsilon}).$$

Clearly, we may prove then

$$(5.19) \quad \Sigma \stackrel{def}{=} \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n \equiv 0(r) \\ n \equiv -2(q)}} 1 - \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n \equiv 0(r)}} \frac{1}{q} \ll h^{1-\varepsilon};$$

in fact, the difference between the main terms of 5.18 and of 5.19 is negligible, because

$$\sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \sum_{\substack{x < n \leq x+h \\ n \equiv 0(r)}} \frac{1}{q} - h \sum_{\substack{q \sim Q \\ r \sim R}} \frac{\gamma_q \delta_r}{qr} = \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \mathcal{O}(1/q) \ll R$$

and  $R \ll h^{1-\varepsilon}$  by hypothesis.

From the orthogonality of the additive characters (see §2.4.1 or [Vi], chap.1, Lemma 5)

$$(5.20) \quad \Sigma = \sum_{r \sim R} \delta_r \sum_{q \sim Q} \frac{\gamma_q}{q} \sum_{j < q} \sum_{x/r < m \leq (x+h)/r} e_q(j(m + 2\bar{r})).$$

We use Mellin transform to choose the integers  $m$  in the interval  $]x/r, (x+h)/r]$  (i.e. to express its characteristic function). In order to do this we use a suitable kernel  $K_r(\tau)$ , with the property

$$\int_{\mathbf{R}} |K_r(\tau)| d\tau \ll \log x;$$

in this way, writing  $m \simeq x/R$  to indicate that  $m \in ]x/2R, 2x/R]$ , we obtain from 5.20

$$\begin{aligned} \Sigma &= \sum_{r \sim R} \delta_r \sum_{q \sim Q} \frac{\gamma_q}{q} \sum_{j < q} \sum_{m \simeq x/R} e_q(j(m + 2\bar{r})) \int_{\mathbf{R}} K_r(\tau) m^{i\tau} d\tau = \\ &= \sum_{r \sim R} \delta_r \int_{\mathbf{R}} K_r(\tau) \sum_{q \sim Q} \frac{\gamma_q}{q} \sum_{j < q} e_q(2j\bar{r}) \sum_{m \simeq x/R} m^{i\tau} e_q(jm) d\tau; \end{aligned}$$

hence, by Hölder inequality (recalling that  $\gamma_q, \delta_r \ll 1$ ) we get (for a certain  $\tau \in \mathbf{R}$ )

$$\begin{aligned} \Sigma &\ll (\log x) \sum_{r \sim R} \left| \sum_{q \sim Q} \frac{\gamma_q}{q} \sum_{j < q} \left( \sum_{m \simeq x/R} m^{i\tau} e_q(jm) \right) e_q(2j\bar{r}) \right| \ll \\ &\ll (\log x) \sum_{r \sim R} \left| \sum_{q \sim Q} \frac{\gamma_q}{q} \sum_{j < q} \left( \sum_{m \simeq x/R} m^{i\tau} e_q(\bar{2}jm) \right) e_q(j\bar{r}) \right|. \end{aligned}$$

Applying Cauchy inequality we obtain ( $q$  prime  $\Rightarrow$  the  $j$ -sum is over the reduced remainders classes mod  $q$ )

$$\Sigma \ll (\log x) \sqrt{R} \sqrt{\sum_{r \sim R} \left| \sum_{q \sim Q} \frac{\gamma_q}{q} \sum_{j \leq q}^* \left( \sum_{m \simeq x/R} m^{i\tau} e_q(\bar{2}jm) \right) e_q(j\bar{r}) \right|^2},$$

whence, by Lemma 5.3 (see next subsection)

$$\begin{aligned} (5.21) \quad \Sigma &\ll (\log x) \sqrt{R} \sqrt{x^{2\delta} (R + Q^2) \sum_{q \sim Q} \frac{1}{q^2} \sum_{j \leq q} \left| \sum_{m \simeq x/R} m^{i\tau} e_q(jm) \right|^2} \\ &\ll x^{2\delta} \sqrt{R} \sqrt{(R + Q^2) \sum_{q \sim Q} \frac{1}{q} \frac{x}{R}} \ll x^{2\delta} \sqrt{(R + Q^2)x}. \end{aligned}$$

We aim to  $\Sigma \ll h^{1-\varepsilon}$  and for this it suffices, by 5.19, to choose in 5.21, for example,  $\delta = \varepsilon/4$  and

$$R \leq (h^2/x)x^{-3\varepsilon}, \quad Q \leq (h/x^{1/2})x^{-2\varepsilon};$$

hence Theorem 5.4.

(This approach, in fact, doesn't impose constraints on  $\vartheta$ , except for the obvious one, i.e.  $\vartheta > 1/2$ ; however, the level of distribution becomes greater than  $\vartheta$ , as already remarked, only for  $\vartheta > 3/4$ ).

The Proof of Corollary 5.4 is immediate, simply choose in Theorem 5.4  $R = (h^2/x)x^{-3\varepsilon}$ ,  $Q = (h/x^{1/2})x^{-2\varepsilon}$ . Corollary 5.5 is proved on the same lines of the proof of Corollary 1.2 in [S-V].

### 5.4.3 A variant of the Large Sieve

**Lemma 5.2.** *Let  $Q, N \in \mathbf{N}$  and  $\{a_n\}$  be a sequence of complex numbers; then*

$$(5.22) \quad \sum_{q \leq Q} \sum_{a \leq q}^* \left| \sum_{n \leq N} a_n e_q(an) \right|^2 \ll (N + Q^2) \sum_{n \leq N} |a_n|^2,$$

where "\*" means (as usual) that the sum is over the reduced classes (mod  $q$ ).

This is the very well known Large Sieve Inequality (for a standard proof see [B(1)], p.13; see also §4.3).

From this Lemma we derive, in an elementary way, a Large Sieve in which we have the inverse remainder classes:

**Lemma 5.3.** *Let  $Q, N \in \mathbf{N}$  and  $\lambda_{a,q} \in \mathbf{C}$  ( $\forall a, q \in N$ ); then  $\forall \delta > 0$  we have*

$$(5.23) \quad \sum_{n \leq N} \left| \sum_{\substack{q \leq Q \\ (q, n)=1}} \sum_{a \leq q}^* \lambda_{a,q} e_q(a\bar{n}) \right|^2 \ll (QN)^\delta (N + Q^2) \sum_{q \leq Q} \sum_{a \leq q}^* |\lambda_{a,q}|^2.$$

**Proof.** We prove that

$$(5.24) \quad \sum_{q \leq Q} \sum_{a \leq q}^* \left| \sum_{\substack{n \leq N \\ (n, q)=1}} a_n e_q(a\bar{n}) \right|^2 \ll (QN)^\delta (N + Q^2) \sum_{n \leq N} |a_n|^2,$$

since 5.23 follows by the Duality Principle (see [M(2)], p.134; see also [Te], Lemma 5.1, p.63).

In order to do this, we expand the square in 5.24 obtaining

$$\sum_{q \leq Q} \sum_{a \leq q}^* \sum_{\substack{n_1 \leq N \\ (n_1, q) = 1}} \sum_{\substack{n_2 \leq N \\ (n_2, q) = 1}} a_{n_1} \overline{a_{n_2}} e_q(a(\overline{n_1} - \overline{n_2})),$$

da cui, ponendo  $b = a\overline{n_1 n_2}$  ricaviamo (dato che  $(n_1, q) = (n_2, q) = 1$ )

$$\sum_{q \leq Q} \sum_{b \leq q}^* \left| \sum_{\substack{n \leq N \\ (n, q) = 1}} a_n e_q(bn) \right|^2,$$

i.e. the LHS of 5.24; hence, it will suffice to prove the following variant of the Large Sieve :

$$(5.25) \quad \sum_{q \leq Q} \sum_{a \leq q}^* \left| \sum_{\substack{n \leq N \\ (n, q) = 1}} a_n e_q(bn) \right|^2 \ll (QN)^\delta (N + Q^2) \sum_{n \leq N} |a_n|^2.$$

Here the LHS is

$$\sum_{q \leq Q} \sum_{a \leq q}^* \left| \sum_{\substack{n \leq N \\ d|n \\ d|q}} \mu(d) a_n e_q(an) \right|^2 = \sum_{q \leq Q} \sum_{a \leq q}^* \left| \sum_{\substack{d \leq N \\ d|q}} \mu(d) \sum_{\substack{m \leq N/d}} a_{md} e_q(amd) \right|^2,$$

whence (by Cauchy inequality and the estimate for the divisor function  $\tau(q) \ll q^\delta$ , see [H-W], p. 260)

$$\sum_{q \leq Q} \sum_{a \leq q}^* \left| \sum_{\substack{n \leq N \\ (n, q) = 1}} a_n e_q(bn) \right|^2 \ll Q^\delta \sum_{d \leq N} d \sum_{\substack{g \leq Q/d \\ c \leq g}}^* \left| \sum_{m \leq N/d} a_{md} e_g(cm) \right|^2.$$

Then, applying the Large Sieve, i.e. by 5.22, we have

$$\sum_{q \leq Q} \sum_{a \leq q}^* \left| \sum_{\substack{n \leq N \\ (n, q) = 1}} a_n e_q(bn) \right|^2 \ll Q^\delta \sum_{d \leq N} d \left( \frac{N}{d} + \frac{Q^2}{d^2} \right) \sum_{m \leq N/d} |a_{md}|^2 \ll$$

$$\begin{aligned} &\ll Q^\delta \left( N \sum_{n \leq N} |a_n|^2 \sum_{\substack{d|n \\ d \leq N}} 1 + Q^2 \sum_{n \leq N} |a_n|^2 \sum_{\substack{d|n \\ d \leq N}} \frac{1}{d} \right) \\ &\ll Q^\delta (N + Q^2) N^\delta \sum_{n \leq N} |a_n|^2, \end{aligned}$$

whence the estimate 5.25, completing the Proof of Lemma 5.3.

## 5.5 Dispersion Method and $n(n+2)$ in short intervals

In this section we continue the study of the distribution in the arithmetic progressions of the polynomial  $n(n+2)$  and, also, of quadratic reducible polynomials, in the short intervals, that we began in the previous section. Here, instead of the Large Sieve (see [B(1)] and [B(2)]; cfr. also §4.3), we use the Dispersion method (see [L]; see also §4.4) in order to have results that are independent (even if from some point of view stronger) w.r.t. the previous.

### 5.5.1 Statement of the results

Applying the Dispersion Method we prove the following results.

**Theorem 5.5.** *Let  $x > 4$ ,  $0 < \vartheta \leq 1$ ,  $x^\vartheta \leq h \leq x$ ,  $0 < \varepsilon \leq \frac{1}{8}$ ; let  $Q, R \in [1, h/2[$  and  $\gamma_q, \delta_r$  be bounded arithmetic functions with support on the primes of  $]Q, 2Q], ]R, 2R]$  (respectively). Then, for  $(q, r) = 1$ , we have 5.17, provided  $R \leq h^{1-2\varepsilon}$ ,  $Q \leq R^{1/2}h^{-\varepsilon}$ ,  $QR > 2h + 2$ .*

As an application we then get level of distribution  $3\vartheta/2$

**Corollary 5.6.** *Let  $x, \vartheta, \varepsilon, q, r, \gamma_q, \delta_r$  be as above. Then the estimate 5.17 of Theorem 5.5 holds for  $QR = h^{3/2-4\varepsilon}$ .*

As in the previous section, we generalize Theorem 5.5 and Corollary 5.6 to obtain

**Corollary 5.7.** *Let  $(an+b)(cn+d)$  be a polynomial without fixed divisors. Let  $x, \vartheta, h, \varepsilon, q, r, \gamma_q$  and  $\delta_r$  be as above, with  $qr$  coprime with  $[a, c, ad-bc]$ . Then the same conclusions of Theorem 5.5 and Corollary 5.6 still hold, with  $(an+b)(cn+d)$  in place of  $n(n+2)$ .*

(This time we'll not prove the Corollaries, because we'll refer to §5.4).

We remark that using the Dispersion method we go beyond the level  $\vartheta$  (the "trivial" level of distribution) for every  $\vartheta > 0$ , while by the Large Sieve (see previous section) this is possible only for  $\vartheta > 3/4$ .

In fact, the level of distribution given by the Large Sieve is smaller than the one supplied by the Dispersion.

Nevertheless, the main Theorems (as, also, their Corollaries) are independent each other, because of different ranges of  $Q$  and  $R$  in the two results.

### 5.5.2 Proof of the Theorem

We start, to prove Theorem 5.5, from 5.19 of the previous section and observe that, since  $qr > 2h + 2$  and  $q$  is prime

$$\Sigma = \sum_{\substack{q \sim Q \\ r \sim R}} \gamma_q \delta_r \left( \sum_{\substack{\frac{x}{r} < m \leq \frac{x+h}{r} \\ mr \equiv -2(q)}} 1 - \sum_{\substack{\frac{x}{r} < m \leq \frac{x+h}{r} \\ (m, q) = 1}} \frac{1}{q} \right) + \mathcal{O}(R),$$

$\mathcal{O}(R)$  being negligible, as before; then, by Cauchy inequality

$$\Sigma \ll \sqrt{R} \sqrt{\Delta},$$

where, say,  $\Delta = \Delta(x, h, Q, R)$  equals

$$\Delta \stackrel{def}{=} \sum_{r \sim R} \left| \sum_{q \sim Q} \gamma_q \left( \sum_{\substack{\frac{x}{r} < m \leq \frac{x+h}{r} \\ mr \equiv -2(q)}} 1 - \sum_{\substack{\frac{x}{r} < m \leq \frac{x+h}{r} \\ (m, q) = 1}} \frac{1}{q} \right) \right|^2.$$

Henceforth, we'll prove  $\Sigma \ll h^{1-\varepsilon}$  through the bound

$$(5.26) \quad \Delta \ll h^{2-2\varepsilon}/R.$$

We apply now the Dispersion method to  $\Delta$ ; we expand the square and exchange the sum over  $r$  and the inner sums to have

$$\Delta = \sum_{q_1, q_2 \sim Q} \gamma_{q_1} \overline{\gamma_{q_2}} \sum_{\substack{\frac{x}{2R} < m_1 \leq \frac{x+h}{R} \\ (m_1, q_1) = 1}} \sum_{\substack{\frac{x}{2R} < m_2 \leq \frac{x+h}{R} \\ (m_2, q_2) = 1}} E,$$

where  $E = E(m_1, m_2, q_1, q_2, x, h, R)$  is, say

$$E \stackrel{def}{=} \sum_{\substack{X < r \leq Y \\ rm_1 \equiv -2(q_1) \\ rm_2 \equiv -2(q_2)}} 1 - \sum_{\substack{X < r \leq Y \\ rm_1 \equiv -2(q_1)}} \frac{1}{q_2} - \sum_{\substack{X < r \leq Y \\ rm_2 \equiv -2(q_2)}} \frac{1}{q_1} + \sum_{X < r \leq Y} \frac{1}{q_1 q_2},$$

$X = X(m_1, m_2, x, R) \stackrel{def}{=} \max(R, x/m_1, x/m_2)$ ,  $Y = Y(m_1, m_2, x, h, R) \stackrel{def}{=} \min(2R, (x+h)/m_1, (x+h)/m_2)$ ; here all the sums over  $r$  have  $(r, q_1 q_2) = 1$ .

Hence, by these definitions and our hypothesis on  $R$ , every sum over  $m_1$  and  $m_2$  has length  $\mathcal{O}(h/R)$ .

(This information will be implicit in the following.)

First of all, let's evaluate the diagonal of  $\Delta$ , i.e.  $\Delta'$ , say

$$\Delta' \stackrel{def}{=} \sum_{q \sim Q} |\gamma_q|^2 \sum_{\substack{\frac{x}{2R} < m_1 \leq \frac{x+h}{R} \\ (m_1, q_1)=1}} \sum_{\substack{\frac{x}{2R} < m_2 \leq \frac{x+h}{R} \\ (m_2, q_2)=1}} E,$$

where this time  $E = E(m_1, m_2, q, q, x, h, R)$  equals, say,  $E \stackrel{def}{=} E_1 + E_2 + E_3 + E_4$ , i.e.

$$\sum_{\substack{X < r \leq Y \\ rm_1 \equiv -2(q) \\ rm_2 \equiv -2(q)}} 1 - \sum_{\substack{X < r \leq Y \\ rm_1 \equiv -2(q)}} \frac{1}{q} - \sum_{\substack{X < r \leq Y \\ rm_2 \equiv -2(q)}} \frac{1}{q} + \sum_{X < r \leq Y} \frac{1}{q^2}.$$

The contribute of  $E_1$  in  $\Delta'$  is bounded by

$$\begin{aligned} \sum_{q \sim Q} \sum_{\substack{\frac{x}{2R} < m_1 \leq \frac{x+h}{R} \\ R < r \leq 2R \\ \frac{x}{m_1} < r \leq \frac{x+h}{m_1} \\ rm_1 \equiv -2(q)}} \sum_{\substack{\frac{x}{r} < m_2 \leq \frac{x+h}{r} \\ rm_2 \equiv -2(q)}} 1 &\ll \sum_{q \sim Q} \sum_{\substack{\frac{x}{2R} < m_1 \leq \frac{x+h}{R}}} \left( \frac{h}{m_1 q} + 1 \right) \ll \\ &\ll h \frac{hR}{R^2} + Q \frac{h}{R} \ll h + \frac{Qh}{R} \end{aligned}$$

(having exchanged the sum over  $r$  with the sum over  $m_2$ ), since, by our hypotheses,  $QR > h$  and  $h \leq x$ .

The contribute of  $E_2$  (that of  $E_3$  is analogous) is bounded by (being  $QR > h$ )

$$\sum_{q \sim Q} \frac{1}{q} \sum_{r \sim R} \sum_{\substack{\frac{x}{r} < m_2 \leq \frac{x+h}{r} \\ \frac{x}{m_1} < m_1 \leq \frac{x+h}{r} \\ m_1 r \equiv -2(q)}} 1 \ll \sum_{q \sim Q} \frac{1}{q} \sum_{r \sim R} \frac{h}{R} \ll h,$$

after having exchanged the sum over  $r$  with the double sum over  $m_1, m_2$ .

Finally, the contribute of  $E_4$  is given by

$$\sum_{q \sim Q} \frac{1}{q^2} \sum_{\substack{\frac{x}{2R} < m_1 \leq \frac{x+h}{R} \\ \frac{x}{2R} < m_2 \leq \frac{x+h}{R}}} \sum_{X < r \leq Y} 1 \ll \frac{1}{Q} \sum_{r \sim R} \frac{h^2}{R^2} \ll \frac{h^2}{QR} \ll h.$$

5.5. DISPERSION METHOD AND  $N(N+2)$  IN SHORT INTERVALS 109

Hence

$$\Delta' \ll h + \frac{hQ}{R} \ll \frac{h^{2-2\varepsilon}}{R},$$

as required in 5.26 (our hypotheses on  $Q, R$  imply  $R \leq h^{1-2\varepsilon}$  and  $Q \leq h^{1-2\varepsilon}$ ).

Now we pass to the estimate of  $\Delta - \Delta'$  (the non-diagonal terms of  $\Delta$ ).

We first prove that we can ignore the condition  $(r, q_1 q_2) = 1$  in the last three sums of  $E$  in  $\Delta - \Delta'$ . In fact the sums in  $E$  having  $(r, q_1 q_2) > 1$  are (since  $q_1$  and  $q_2$  are distinct primes), say

$$E' \stackrel{def}{=} - \sum_{\substack{X < r \leq Y \\ r m_1 \equiv -2(q_1) \\ q_2 | r}} \frac{1}{q_2} + \sum_{\substack{X < r \leq Y \\ (r, q_1) = 1 \\ q_2 | r}} \frac{1}{q_1 q_2} - \sum_{\substack{X < r \leq Y \\ r m_2 \equiv -2(q_2) \\ q_1 | r}} \frac{1}{q_1} + \sum_{\substack{X < r \leq Y \\ (r, q_2) = 1 \\ q_1 | r}} \frac{1}{q_1 q_2}$$

and, say,

$$E'' \stackrel{def}{=} \sum_{\substack{X < r \leq Y \\ q_1 q_2 | r}} \frac{1}{q_1 q_2}.$$

Their contribute to  $\Delta - \Delta'$  is negligible, i.e.  $\mathcal{O}(h^{2-2\varepsilon}/R)$ , as required in 5.26; in fact, exchanging back the sums over  $r$  and those over  $m_1, m_2$  obtain

$$\begin{aligned} & \sum_{\substack{\frac{x}{2R} < m_1 \leq \frac{x+h}{R} \\ (m_1, q_1) = 1}} \sum_{\substack{\frac{x}{2R} < m_2 \leq \frac{x+h}{R} \\ (m_2, q_2) = 1}} E' = \\ &= \frac{1}{q_2} \sum_{\substack{r \sim R \\ (r, q_1) = 1 \\ q_2 | r}} \sum_{\substack{\frac{x}{r} < m_2 \leq \frac{x+h}{r}}} \mathcal{O}(1) + \frac{1}{q_1} \sum_{\substack{r \sim R \\ (r, q_2) = 1 \\ q_1 | r}} \sum_{\substack{\frac{x}{r} < m_1 \leq \frac{x+h}{r}}} \mathcal{O}(1), \end{aligned}$$

and this last gives a contribute  $\mathcal{O}(h)$  to  $\Delta - \Delta'$ , which is negligible, as seen before (we use the hypothesis  $QR > h$ ).

In the same way,  $E''$  contributes to  $\Delta - \Delta'$  with (being  $4Q^2 < R$ )

$$\sum_{q_1, q_2 \sim Q} \frac{1}{q_1 q_2} \sum_{\substack{r \sim R \\ q_1 q_2 | r}} \sum_{\substack{\frac{x}{r} < m_1 \leq \frac{x+h}{r} \\ \frac{x}{r} < m_2 \leq \frac{x+h}{r}}} 1 \ll \sum_{q_1, q_2 \sim Q} \frac{1}{q_1^2 q_2^2} \frac{h^2}{R} \ll \frac{h^2}{Q^2 R} \ll h,$$

which is also negligible (again, using  $QR > h$ ).

Hence, by a direct calculation,  $E$  in  $\Delta - \Delta'$  is

$$\begin{aligned} & \left( \left[ \frac{Y-c}{q_1 q_2} \right] - \left[ \frac{X-c}{q_1 q_2} \right] \right) - \frac{1}{q_2} \left( \left[ \frac{Y+2\overline{m}_1}{q_1} \right] - \left[ \frac{X+2\overline{m}_1}{q_1} \right] \right) \\ & - \frac{1}{q_1} \left( \left[ \frac{Y+2\overline{m}_2}{q_2} \right] - \left[ \frac{X+2\overline{m}_2}{q_2} \right] \right) + \frac{Y-X}{q_1 q_2} \end{aligned}$$

(where

$$(5.27) \quad c \equiv -2\overline{m}_2 q_1 \overline{q}_1 - 2\overline{m}_1 q_2 \overline{q}_2 \pmod{q_1 q_2},$$

with  $\overline{m}_1 m_1 \equiv 1 \pmod{q_1}$ ,  $\overline{m}_2 m_2 \equiv 1 \pmod{q_2}$ ,  $\overline{q}_1 q_1 \equiv 1 \pmod{q_2}$   
and  $\overline{q}_2 q_2 \equiv 1 \pmod{q_1}$ ),

which is  $\mathcal{O}(1)$ , because the main term cancel and the fractional parts give  $\mathcal{O}\left(1 + \frac{1}{q_2} + \frac{1}{q_1}\right)$ .

Thus, we get

$$\Delta - \Delta' \ll \sum_{q_1, q_2 \sim Q} \sum_{\frac{x}{2R} < m_1 \leq \frac{x+h}{R}} \sum_{\frac{x}{2R} < m_2 \leq \frac{x+h}{R}} 1 \ll Q^2 \frac{h^2}{R^2}$$

and this last is  $\mathcal{O}(h^{2-2\varepsilon}/R)$ , since  $Q^2 \leq Rh^{-2\varepsilon}$ , as required by the hypotheses of Theorem 5.5.

## 5.6 Kloosterman Sums and $n(n+2)$ in short intervals

In this section we continue the study of the distribution in the arithmetic progressions of  $n(n+2)$  (and, also, of quadratic reducible polynomials) in the short intervals, begun in the previous sections (see [C-S(1)] and [C-S(2)]). Now, instead of the Large Sieve (see [B(1)] and [B(2)]; see also §4.3), we use again the Dispersion Method (see [L]; see also §4.4), but combined with a non-trivial estimate the fractional parts, using estimates for Kloosterman sums bilinear forms (see [D-F-I]); these allow us to prove stronger results than that in §5.5 (even if still independent of those in §5.4). In fact, this time the level of distribution is  $143\vartheta/95$ , i.e.  $143/95$  in the "long" intervals (see the following Corollary 5.8).

We'll assume now on that  $Q > R^{1/2}h^{-\varepsilon/2}$ , otherwise we go to the proof in the previous section.

In the following section we give, of course, only a part of the Proof in [C-S(3)] not already in [C-S(2)] (for which see §5.5).

### 5.6.1 Statement of the results

We have the

**Theorem 5.6.** *Let  $x > 4$ ,  $0 < \vartheta \leq 1$ ,  $x^\vartheta \leq h \leq x$ ,  $0 < \varepsilon < \frac{12}{119}$ ; let  $Q, R \in [1, h/2[$  and  $\gamma_q, \delta_r$  be bounded arithmetic functions, with support on the primes of  $]Q, 2Q[$ ,  $]R, 2R[$  (resp.). Then for  $(q, r) = 1$  we have 5.17, provided  $h^{3\varepsilon} \leq R \leq h^{1-3\varepsilon}$ ,  $h^{3\varepsilon} \leq Q \leq R^{48/95}h^{-2\varepsilon}$ ,  $QR > 2h + 2$ .*

As an application, we get level of distribution  $143\vartheta/95$

**Corollary 5.8.** *Let  $x, \vartheta, \varepsilon, q, r, \gamma_q, \delta_r$  be as above. Then the estimate 5.17 of Theorem 5.6 holds for  $QR = h^{143/95-7\varepsilon}$ .*

As in [S-V] we generalize Theorem 5.6 and Corollary 5.8 to quadratic reducible polynomials

**Corollary 5.9.** *Let  $(an+b)(cn+d)$  be a polynomial without fixed divisors. Let  $x, \vartheta, h, \varepsilon, q, r, \gamma_q$  and  $\delta_r$  be as above, with  $qr$  coprime with  $[a, c, ad-bc]$ . Then the same conclusions of Theorem 5.6 and of Corollary 5.8 hold true with  $(an+b)(cn+d)$  instead of  $n(n+2)$ .*

### 5.6.2 Estimates of the fractional parts with Kloosterman sums

We have (see §5.5)

$$(5.28) \quad E - E' - E'' = \sum_{\substack{X < r \leq Y \\ r \equiv c(q_1 q_2)}} 1 - \sum_{X < r \leq Y} \frac{1}{q_1 q_2} + \mathcal{O}\left(\frac{1}{q_2} + \frac{1}{q_1}\right),$$

in which the remainder is acceptable, since (by the hypothesis  $Q \leq Rh^{-2\varepsilon}$ ) it contributes with  $\mathcal{O}(h^{2-2\varepsilon}/R)$  to 5.26.

Before to go on, we have to treat the case in which the 5.28 is summed with  $m_1 = m_2$  in  $\Delta - \Delta'$ , to show that its contribute to 5.26 is negligible, too. Since the condition  $r \equiv c(q_1 q_2)$  in 5.28 is equivalent, in this case, to  $r \equiv -2\bar{m} \pmod{q_1 q_2}$ , we obtain

$$\sum_{\substack{q_1, q_2 \sim Q \\ (q_1, q_2) = 1}} \gamma_{q_1} \bar{\gamma}_{q_2} \sum_{\substack{\frac{x}{2R} < m \leq \frac{x+h}{R} \\ (m, q_1 q_2) = 1}} (E - E' - E'') \ll \sum_{r \sim R} \sum_{\substack{\frac{x}{r} < m \leq \frac{x+h}{r}}} \sum_{\substack{Q^2 < d \leq 4Q^2 \\ d | (mr+2)}} \tau(d)$$

and this last is  $\mathcal{O}(h^{1+\varepsilon})$ , using the estimate  $\tau(d) \ll d^\mu$ ,  $\mu > 0$  "small" (see [H-W], p.260) twice; since  $R \leq h^{1-3\varepsilon}$ , this gives a negligible contribute to 5.26.

Thus, in the following we may assume that  $m_1$  and  $m_2$  are distinct.

Here we require the following (regularized) Fourier expansion of the fractional part.

**Lemma 5.4.** *For every  $0 < \sigma < 1/2$  and for every natural number  $k$  there exist two functions  $f$  and  $g$  periodic of period 1 (depending on  $\sigma$  and  $k$ ) such that ( $e(t)$  is defined, as usual, by  $e^{2\pi it}$ )*

$$\left| \{y\} - \frac{1}{2} - f(y) \right| \leq g(y), \quad f(y) = \sum_{j \in \mathbf{Z}^*} a_j e(jy), \quad g(y) = \sum_{j \in \mathbf{Z}} b_j e(jy),$$

where the Fourier coefficients (depending on  $\sigma$  and  $k$ ) satisfy

$$b_0 \ll_k \sigma \quad \text{and} \quad |a_j|, |b_j| \ll_k \min\left(\frac{1}{|j|}, \frac{1}{|j|} \left(\frac{1}{|j|\sigma}\right)^{k+1}\right) \quad \forall j \in \mathbf{Z}^*.$$

We apply the Lemma 5.4 to write

$$(5.29) \quad \{y\} - \frac{1}{2} = \sum_{j \in \mathbf{Z}^*} c_j e(jy) + \mathcal{O}_k(\sigma),$$

where

$$(5.30) \quad |c_j| \ll_k \min \left( \frac{1}{|j|}, \frac{1}{|j|} \left( \frac{1}{|j|\sigma} \right)^k \right) \quad \forall j \in \mathbf{Z}^*.$$

Then, defining  $\mathcal{F} = \mathcal{F}(q_1, q_2, m_1, m_2, R, x, h)$  as

$$\mathcal{F} \stackrel{def}{=} \sum_{\substack{X < r \leq Y \\ r \equiv c \pmod{q_1 q_2}}} 1 - \sum_{X < r \leq Y} \frac{1}{q_1 q_2} = \left\{ \frac{X-c}{q_1 q_2} \right\} - \left\{ \frac{Y-c}{q_1 q_2} \right\}$$

we obtain

$$(5.31) \quad \mathcal{F} = \sum_{j \in \mathbf{Z}^*} c_j (e_{q_1 q_2}(jX) - e_{q_1 q_2}(jY)) e_{q_1 q_2}(-jc) + \mathcal{O}_k(\sigma),$$

where  $c$  is given by 5.27 (and, as usual,  $e_d(n) \stackrel{def}{=} e(n/d)$ ).

From 5.29 and 5.30 we choose (since, as stated, we may suppose that  $Q^2 > Rh^{-\varepsilon}$ )

$$\sigma \stackrel{def}{=} \frac{R}{Q^2} h^{-2\varepsilon} \quad (\rightarrow 0)$$

in order to render the contribute of  $\sigma$  in 5.31 to 5.26 negligible. Furthermore, choosing

$$J \stackrel{def}{=} \frac{Q^2}{R} h^{3\varepsilon} \quad (\geq h^{2\varepsilon} \rightarrow \infty)$$

we have

$$\sum_{|j| > J} |c_j| \ll_k \frac{1}{\sigma^k} \sum_{|j| > J} |j|^{k+1} \ll_k \left( \frac{1}{\sigma J} \right)^k,$$

which is  $\mathcal{O}_k \left( \frac{R}{Q^2} h^{-2\varepsilon} \right)$ , i.e.  $\mathcal{O}_\varepsilon \left( \frac{R}{Q^2} h^{-2\varepsilon} \right)$  (with the choice of a "large"  $k$  depending on  $\varepsilon$ ); this gives, again, a contribute in 5.26 which is negligible in 5.28.

Of course, in the same way,

$$(5.32) \quad \sum_{|j| > G} |c_j| \ll_\varepsilon \frac{R}{Q^2} h^{-2\varepsilon}, \quad \forall G \geq J.$$

Thus, the series in 5.31 may be substituted (reducing, without loss of generality, to positive  $j$  indices) by the sum :

$$\mathcal{F} = \sum_{j \leq q_1 q_2} c_j (e_{q_1 q_2}(jX) - e_{q_1 q_2}(jY)) e_{q_1}(2j\overline{m_1 q_2}) e_{q_2}(2j\overline{m_2 q_1}),$$

say, and more in general, by any such sum over su  $j \leq G$ , where by 5.32 we can choose any  $G \geq J$ ; in particular, our choice of  $G$  is admissible, being  $q_1 q_2 > Q^2$  and  $Q^2 \geq J$  (by the hypothesis  $R \geq h^{3\varepsilon}$ ). (In the following we'll omit in  $\mathcal{F}$  all the contributes that, by 5.32, constitute in 5.28 negligible terms for the sums in 5.26).

Without loss of generality we estimate (here  $W = X, Y \ll R$ , depends on  $m_1, m_2, R, x, h$ , but not on  $q_1, q_2$ )

$$(5.33) \quad \mathcal{F} = \sum_{j \leq q_1 q_2} c_j e_{q_1 q_2}(jW) e_{q_1}(2j\overline{m_1 q_2}) e_{q_2}(2j\overline{m_2 q_1}).$$

Let  $j = gm_1 m_2 \pmod{q_1 q_2}$ , so that  $\mathcal{F}$  in 5.33 becomes

$$\sum_{g \leq q_1 q_2} d_g e_{q_1 q_2}(gm_1 m_2 W) e_{q_1}(2gm_2 \overline{q_2}) e_{q_2}(2gm_1 \overline{q_1}),$$

where  $d_g$  is the coefficient  $c_v$ , with index  $1 \leq v \leq q_1 q_2$  such that we have  $v \equiv gm_1 m_2 \pmod{q_1 q_2}$ .

Here we want to apply the **reciprocity relation**, i.e.

$$(5.34) \quad \frac{\overline{q_1}}{q_2} \equiv -\frac{\overline{q_2}}{q_1} + \frac{1}{q_1 q_2} \pmod{1},$$

which gives

$$\mathcal{F} = \sum_{g \leq q_1 q_2} d_g e_{q_1 q_2}(gm_1 m_2 W) e_{q_1}(2g(m_2 - m_1)\overline{q_2}) e_{q_1 q_2}(2gm_1)$$

and, going back to  $j = m_1 m_2 g$  and by 5.32

$$(5.35) \quad \mathcal{F} = \sum_{j \leq J} c_j e_{q_1 q_2}(jW) e_{q_1}(2j(\overline{m_1} - \overline{m_2})\overline{q_2}) e_{q_1 q_2}(2j\overline{m_2}).$$

In this way, summing over  $q_2$  we have Kloosterman sums with arbitrary coefficients (i.e.  $\overline{\gamma_{q_2}}$ ) and their estimate can be done only on average over the moduli (i.e.  $q_1$ ); this bound has recently been given by Duke-Friedlander-Iwaniec [D-F-I].

5.6. KLOOSTERMAN SUMS AND  $N(N+2)$  IN SHORT INTERVALS 115

The following Lemma is Theorem 2 in [D-F-I]:

**Lemma 5.5.** *Let  $\alpha$  and  $\beta$  be two arithmetic functions  $\alpha, \beta : \mathbf{N} \rightarrow \mathbf{C}$ , with  $l^2$ -norm  $\|\alpha\|, \|\beta\|$ , (resp.); then  $\forall k \in \mathbf{Z}^*$  and  $\forall \mu > 0$  we have*

$$\sum_{m \sim M} \sum_{\substack{n \sim N \\ (n, m) = 1}} \alpha_m \beta_n e\left(k \frac{\overline{m}}{n}\right) \ll_{\mu} \|\alpha\| \|\beta\| (k + MN)^{\frac{3}{8}} (M + N)^{\frac{11}{48} + \mu}.$$

In order to apply Lemma 5.5, we have first to eliminate the reciprocal remainder classes  $\overline{m_1}$  and  $\overline{m_2}$ , since (even if  $m_1$  and  $m_2$  are constant w.r.t.  $q_1$  and  $q_2$ ) they depend on the moduli.

Then, we regard them as reciprocal residues modulo, say,

$$B \stackrel{def}{=} \prod_{\substack{q \sim Q \\ q \text{ primo}}} q,$$

and this is possible, since  $(m_1 m_2, B) = 1$ .

By 5.32 and the hypothesis  $Q < Rh^{-3\varepsilon}$  we can choose  $j < Q$ , we have (by definition of  $B$ )  $(j, B) = 1$  and we can write, from 5.35,

$$(5.36) \quad \mathcal{F} = \sum_{\substack{j \leq B \\ (j, B) = 1}} c_j e_{q_1 q_2}(j(W + 2\overline{m_2})) e_{q_1}(2j(\overline{m_1} - \overline{m_2})\overline{q_2});$$

letting  $j = gm_1 m_2 \pmod{B}$  the exponentials become

$$e\left(\frac{gm_1(m_2 W + 2)}{q_1 q_2}\right) \text{ and } \left(\frac{2g(m_2 - m_1)\overline{q_2}}{q_1}\right).$$

We want to apply twice Lemma 5.5, so we use Lemma 2.1 (partial summation); but, first, we must change again variables to eliminate the coefficients  $m_1(m_2 W + 2)$ ; hence, let  $k = gm_1(m_2 W + 2) \pmod{B}$ , getting in 5.36

$$\begin{aligned} & \sum_{\substack{q_1, q_2 \sim Q \\ (q_1, q_2) = 1}} \gamma_{q_1} \overline{\gamma_{q_2}} \mathcal{F} = \sum_{\substack{k \leq B \\ (k, B) = 1}} d_k \times \\ & \times \left( \sum_{\substack{q_1, q_2 \sim Q \\ (q_1, q_2) = 1}} \gamma_{q_1} \overline{\gamma_{q_2}} e_{q_1 q_2}(k) e_{q_1}\left(2k(m_2 - m_1)\overline{m_1(m_2 W + 2)q_2}\right) \right), \end{aligned}$$

where now  $d_k \stackrel{def}{=} c_l$ , with  $l \leq B$ ,  $(l, B) = 1$ ,  $l \equiv gm_1(m_2 W + 2) \pmod{B}$ ; again, by partial summation, we write the same equation with coefficients

$\widetilde{d}_k$  instead of  $d_k$ , where  $\widetilde{d}_k = d_k$  or  $\widetilde{d}_k = 0$ ; returning to the variable  $j$  we have (here  $\widetilde{c}_j = c_j$  or  $\widetilde{c}_j = 0$ )

$$\sum_{\substack{q_1, q_2 \sim Q \\ (q_1, q_2) = 1}} \gamma_{q_1} \overline{\gamma_{q_2}} \mathcal{F} \ll \sum_{\substack{j \leq B \\ (j, B) = 1}} |\widetilde{c}_j| \left| \sum_{\substack{q_1, q_2 \sim Q \\ (q_1, q_2) = 1}} \gamma_{q_1} \overline{\gamma_{q_2}} e_{q_1}(2j(m_2 - m_1)\overline{q_2}) \right|.$$

Choosing  $\mu = \varepsilon/2$  in Lemma 5.5 we obtain, gathering the estimates from 5.28 on,

$$\begin{aligned} \Delta &\ll_{\varepsilon} \sum_{\frac{x}{2R} < m_1 < m_2 \leq \frac{x+h}{R}} \left| \sum_{\substack{q_1, q_2 \sim Q \\ (q_1, q_2) = 1}} \gamma_{q_1} \overline{\gamma_{q_2}} \mathcal{F} \right| \ll_{\varepsilon} \\ &\ll_{\varepsilon} \sum_{\frac{x}{2R} < m_1, m_2 \leq \frac{x+h}{R}} \sum_{j \leq B} |c_j| Q^{95/48} h^{\varepsilon/2} \ll_{\varepsilon} \frac{h^2}{R^2} Q^{\frac{95}{48}} h^{\varepsilon} \end{aligned}$$

and last is  $\mathcal{O}_{\varepsilon}(h^{2-2\varepsilon}/R)$ , since  $Q \leq R^{\frac{48}{95}} h^{-2\varepsilon}$ , as required by the hypotheses of Theorem 5.6.