

Harish-Chandra Research Institute

Introduction to the circle method of Hardy, Ramanujan and Littlewood

Alessandro Zaccagnini

February-March, 2005

Abstract

In these lectures we give an overview of the circle method introduced by Hardy and Ramanujan at the beginning of the twentieth century, and developed by Hardy, Littlewood and Vinogradov, among others. We also try to explain the main difficulties in proving Goldbach's conjecture and we give a sketch of the proof of Vinogradov's three-prime Theorem.

1 Additive problems

In the last few centuries many additive problems have come to the attention of mathematicians: famous examples are Waring's problem and Goldbach's conjecture. In general, an additive problem can be expressed in the following form: we are given $s \geq 2$ subsets of the set of natural numbers \mathbb{N} , not necessarily distinct, which we call $\mathcal{A}_1, \dots, \mathcal{A}_s$. We would like to determine the number of solutions of the equation

$$n = a_1 + a_2 + \dots + a_s \tag{1.1}$$

for a given $n \in \mathbb{N}$, with the constraint that $a_j \in \mathcal{A}_j$ for $j = 1, \dots, s$, or, failing that, we would like to prove that the same equation has at least one solution for "sufficiently large" n . In fact, we can not expect, in general, that for very small n there will be a solution of equation (1.1). Furthermore, depending on the nature of the sets \mathcal{A}_j , there may be some arithmetical constraints on those n that may be "represented" in the form (1.1).

In Waring's problem we take an integer $k \geq 2$, and all sets \mathcal{A}_j are equal to the set of the k -th powers of the natural numbers: the goal is to prove that there exists an integer $s(k)$ such that *every* natural number has a representation as a sum of at most s k -th powers. This has been proved by Hilbert by means of a very intricate combinatorial argument. Another interesting problem is the determination of the minimal value of s such that equation (1.1) has at least one solution for sufficiently large $n \in \mathbb{N}$, that is, allowing a finite set of exceptions. We recall Lagrange's four square theorem (every non negative integer can be written as the sum of four squares of non negative integers), and also that if we take $k = 2$ and $s = 2$, then the "arithmetical" set of exceptions contains the congruence class $3 \pmod{4}$.

In Goldbach's problem we set $\mathcal{A}_1 = \mathcal{A}_2 = \mathfrak{P}$, the set of all prime numbers, and, of course, we are interested only in even values of n in (1.1).

In both Waring and Goldbach's problems we may say that the difficulties arise from the fact that the sets \mathcal{A} have a simple multiplicative structure, but we are *adding* their elements.

1.1 The circle method

The method that we are going to describe, that has been widely used to tackle and solve many additive problems, has its origin in a 1918 paper of Hardy & Ramanujan [10] on partitions. It has been developed by Hardy & Littlewood [8], [9] in the 1920's, and, because of their success, it is now referred to as the Hardy-Littlewood, or circle, method.

In what follows, we shall describe Hardy, Littlewood & Ramanujan's ideas in some detail. For the sake of simplicity, we begin with the case of a *binary* problem, that is, the case where $s = 2$. As a further simplification, we assume that $\mathcal{A}_1 = \mathcal{A}_2 = \mathcal{A}$. Of course, we also assume that \mathcal{A} is an infinite set. We start by setting

$$f(z) = f_{\mathcal{A}}(z) \stackrel{\text{def}}{=} \sum_{n=0}^{+\infty} a(n)z^n, \quad \text{where} \quad a(n) = \begin{cases} 1 & \text{if } n \in \mathcal{A}, \\ 0 & \text{otherwise.} \end{cases} \quad (1.2)$$

Since \mathcal{A} is infinite, the function f is a power series whose radius of convergence is 1 (it certainly has a singularity at $z = 1$, and it is regular for $|z| < 1$ by comparison with the sum of a geometric series). We are interested in the number of the representations of n in the form $a_1 + a_2$ with $a_j \in \mathcal{A}$, $j = 1, 2$. Therefore, we set

$$r_2(n) \stackrel{\text{def}}{=} |\{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} : n = a_1 + a_2\}|.$$

By the so-called Cauchy rule for the product of two absolutely convergent power

series, when $|z| < 1$ we have

$$f^2(z) = \sum_{n=0}^{+\infty} c(n)z^n \quad \text{where} \quad c(n) = \sum_{\substack{0 \leq h, k \leq n \\ h+k=n}} a(h)a(k). \quad (1.3)$$

Here $a(h)a(k) = 1$ if both $h, k \in \mathcal{A}$, and otherwise $a(h)a(k) = 0$, whence $c(n) = r_2(n)$. The same argument proves more generally that

$$f^s(z) = \sum_{n=0}^{+\infty} r_s(n)z^n \quad \text{where} \quad r_s(n) \stackrel{\text{def}}{=} |\{(a_1, \dots, a_s) \in \mathcal{A}^s : n = a_1 + \dots + a_s\}|.$$

By Cauchy's theorem, for $\rho < 1$ we have

$$r_2(n) = \frac{1}{2\pi i} \oint_{\gamma(\rho)} \frac{f^2(z)}{z^{n+1}} dz, \quad (1.4)$$

where $\gamma(\rho)$ is the circle whose centre is at the origin and whose radius is ρ . For some sets \mathcal{A} it is possible to determine an asymptotic development for f around the singularities it has on the circle $\gamma(1)$, and it is therefore possible to estimate the integral in (1.4) taking ρ as a function of n whose limiting value is 1.

1.2 A simple example

As a simple example, we set up the circle method to solve a trivial combinatorial problem: given $k \in \mathbb{N}^*$, determine the number of possible representations of $n \in \mathbb{N}$ as a sum of exactly k natural numbers. In other words, we want to determine $r_k(n) := |\{(a_1, \dots, a_k) \in \mathbb{N}^k : n = a_1 + \dots + a_k\}|$. It is clearly possible to show directly, in a totally elementary way, that this number is $r_k(n) = \binom{n+k-1}{k-1}$.

In this case we obviously have $f(z) = \sum_{n=0}^{+\infty} z^n = (1-z)^{-1}$, so that, for $\rho < 1$,

$$r_k(n) = \frac{1}{2\pi i} \oint_{\gamma(\rho)} \frac{dz}{(1-z)^k z^{n+1}}. \quad (1.5)$$

We remark that the integrand has only one singularity on the circle $\gamma(1)$, which is a pole. In this particular case it is possible to compute exactly the value of the integral on the right hand side of (1.5): in fact, since $\rho < 1$, we have the development

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

The series on the right converges uniformly on all compact sets contained in $\{z \in \mathbb{C} : |z| < 1\}$, and therefore we may substitute into (1.5) and interchange the integral and the series:

$$\begin{aligned} r_k(n) &= \frac{1}{2\pi i} \sum_{m=0}^{+\infty} \binom{-k}{m} (-1)^m \oint_{\gamma(\rho)} z^{m-n-1} dz \\ &= \frac{1}{2\pi i} \sum_{m=0}^{+\infty} (-1)^m \binom{-k}{m} \begin{cases} 2\pi i & \text{if } m = n, \\ 0 & \text{otherwise,} \end{cases} = (-1)^n \binom{-k}{n}. \end{aligned}$$

It is not difficult to check that $(-1)^n \binom{-k}{n} = \binom{n+k-1}{k-1}$. We finally remark that the integrand is fairly small on the whole circle $\gamma(\rho)$, except for a small arc close to the point $z = \rho$, that gives the main contribution to the integral in (1.5). We will make things more precise later in (1.12).

In general, of course, it is not possible to evaluate directly and exactly the integral, and usually the integrand has several singularities on the circle $\gamma(1)$. For instance, in order to compute the number of possible decomposition of an integer $n \in \mathbb{N}$ as a sum of k odd integers, we need the function $g(z) = \sum_{m=0}^{+\infty} z^{2m+1} = z/(1-z^2)$, that has two singularities, namely $z = \pm 1$. In these cases, one needs asymptotic developments near each singularity. It is an interesting exercise to repeat the same computations as above in this case, to see how the arithmetical condition $n \equiv k \pmod{2}$ arises.

We notice a very important feature of (1.3) which we are going to exploit later when dealing with the Goldbach problem: when it is difficult to prove that $r(n) > 0$, it may be helpful to change the definition of the coefficients $a(h)$ in (1.2). Instead of allowing only the values 0 and 1, we may attach a positive weight to each element of the set \mathcal{A} : the resulting function will not count the number of representations anymore as $r_2(n)$, but it will be positive if and only if the weighted version is. The rationale is that it should be easier to bound from below a larger number. This gives the circle method some flexibility.

1.3 Vinogradov's refinement

The method we just roughly sketched has been used extensively by Hardy & Littlewood in the 1920's to prove many results connected to Waring's problem, and to carry out the first real attack on Goldbach's conjecture. In the 1930's Vinogradov introduced a few simplifications that make his method slightly simpler to explain. The basic idea in Hardy, Ramanujan and Littlewood is to have some fixed function, like $f(z)^k$ in the previous section, and to take ρ as a function of n with a limiting value of 1; furthermore, we need suitable asymptotic developments for f around the singularities that it has on the circle $\gamma(1)$. Vinogradov remarked that

only those integers $m \leq n$ give a positive contribution to $r_2(n)$, as clearly shown by (1.3): following him, in the combinatorial problem of the previous section we introduce the function

$$f_N(z) \stackrel{\text{def}}{=} \sum_{m=0}^N z^m = \frac{1-z^{N+1}}{1-z}, \quad (1.6)$$

where the last equality is valid for $z \neq 1$. For $n \leq N$, Cauchy's theorem yields

$$r_k(n) = \frac{1}{2\pi i} \oint_{\gamma(1)} \frac{f_N^k(z)}{z^{n+1}} dz. \quad (1.7)$$

In this case there are *no* singularities of the integrand (f_N is a finite sum, a polynomial): therefore we may fix once and for all the circle of integration. Let's set $e(x) := e^{2\pi i x}$ and perform the change of variable $z = e(\alpha)$ in (1.7):

$$r_k(n) = \int_0^1 f_N^k(e(\alpha)) e(-n\alpha) d\alpha. \quad (1.8)$$

This is the Fourier coefficient formula, that gives the n -th coefficient in the Fourier series expansion of the periodic function $f_N^k(e(\alpha))$, because of the orthogonality property of the complex exponential function:

$$\int_0^1 e(nx) dx = \begin{cases} 1 & \text{if } n = 0, \\ 0 & \text{otherwise.} \end{cases} \quad (1.9)$$

Its importance lies in the fact that it transforms an arithmetical problem into one that can be attacked using standard techniques from real and complex analysis. For simplicity, we set $T_N(\alpha) = T(\alpha) := f_N(e(\alpha))$; from (1.6) we deduce

$$\begin{aligned} T(\alpha) &\stackrel{\text{def}}{=} \sum_{m=0}^N e(m\alpha) \\ &= \begin{cases} \frac{1 - e((N+1)\alpha)}{1 - e(\alpha)} = e(\frac{1}{2}N\alpha) \frac{\sin(\pi(N+1)\alpha)}{\sin(\pi\alpha)} & \text{if } \alpha \notin \mathbb{Z}; \\ N+1 & \text{if } \alpha \in \mathbb{Z}. \end{cases} \end{aligned} \quad (1.10)$$

Figure 1 shows the graph of $|T_{20}(\alpha)|$. The property that we need to conclude our elementary analysis concerns the rate of decay of the function T as α gets away from integers: from (1.10) we easily get

$$|T_N(\alpha)| \leq \min \left(N+1, \frac{1}{|\sin(\pi\alpha)|} \right) \leq \min(N+1, \|\alpha\|^{-1}) \quad (1.11)$$

where $\|\alpha\|$ denotes the distance of α from the nearest integer, that is $\min\{\{\alpha\}, 1 - \{\alpha\}\}$, since T is periodic of period 1, and $\alpha \leq \sin(\pi\alpha)$ for $\alpha \in (0, \frac{1}{2}]$. This inequality shows that if $\delta = \delta(N)$ is not too small, the interval $[\delta, 1 - \delta]$ does not give a large contribution to the integral in (1.8): in fact, if $\delta \geq 1/N$ and $k \geq 2$ we have

$$\left| \int_{\delta}^{1-\delta} T_N^k(\alpha) e(-n\alpha) d\alpha \right| \leq \int_{\delta}^{1-\delta} |T_N^k(\alpha)| d\alpha \leq \int_{\delta}^{1-\delta} \frac{d\alpha}{\|\alpha\|^k} \leq \frac{2}{k-1} \delta^{1-k}, \quad (1.12)$$

and this is $o(N^{k-1})$ as soon as $\delta^{-1} = o(N)$. In other words, it is sufficient that δ is just larger than N^{-1} so that the contribution of the interval $[\delta, 1 - \delta]$ to the integral in (1.8) be smaller than the main term, that we know is $N^{k-1}(k-1)!^{-1}$. This means that the main term arises from a comparatively small interval close to $\alpha = 0$.

In the case $k = 2$ we push our analysis a step farther: in fact, it is possible to prove (by induction plus some trigonometric identities) the formula

$$\left(\frac{\sin(\pi(N+1)\alpha)}{\sin(\pi\alpha)} \right)^2 = \sum_{|m| \leq N+1} (N+1 - |m|) e(m\alpha). \quad (1.13)$$

Of course, the knowledge of this identity is at least as difficult as the knowledge of the correct answer to the original problem. Indeed, a much more sensible approach would be to prove (1.13) by means of this argument, rather than the other way around. By (1.8) we have

$$\begin{aligned} r_2(n) &= \int_0^1 \left(\frac{\sin(\pi(N+1)\alpha)}{\sin(\pi\alpha)} \right)^2 e((N-n)\alpha) d\alpha \\ &= \sum_{|m| \leq N+1} (N+1 - |m|) \int_0^1 e((N+m-n)\alpha) d\alpha. \end{aligned} \quad (1.14)$$

By (1.9), the only non-vanishing integral occurs for $m = n - N$, so that $r_2(n) = N+1 - |n - N| = n+1$. The point of this example is that one can usually find information on the quantity $r_2(n)$ by using transformations and suitable identities. We develop the subject further in the next section.

2 Goldbach's problem

After this fairly long introduction devoted to the mechanism of the circle method, we now want to set it up in the case of the Goldbach's problem. Henceforward,

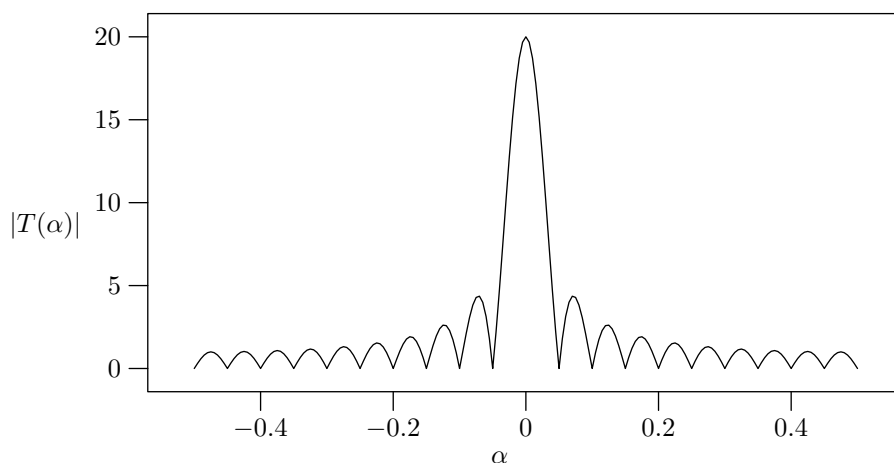


Figure 1: The graph of the function $|T_{20}(\alpha)|$, showing that it has a fairly large peak around integral values of α , and that otherwise it is comparatively small.

the variables p, p_1, p_2, \dots , always denote prime numbers. We are interested in the number of representations of n as a sum of two prime numbers

$$r_2(n) \stackrel{\text{def}}{=} |\{(p_1, p_2) \in \mathfrak{P} \times \mathfrak{P} : n = p_1 + p_2\}|,$$

where p_1 and p_2 are not necessarily distinct, but we consider $p_1 + p_2$ and $p_2 + p_1$ as distinct representations if $p_1 \neq p_2$. For the time being, we do not assume that n is an even integer. Goldbach's conjecture, as stated in a 1742 letter to Euler, is that $r_2(2n) \geq 1$ for all $n \geq 2$.

For technical reasons that will be clarified later (essentially the same reason why it is easier to work with the Chebyshev θ or ψ functions rather than the π function) we prefer to consider a weighted version of the quantity, that is

$$R_2(n) \stackrel{\text{def}}{=} \sum_{p_1+p_2=n} \log p_1 \log p_2.$$

In other words, we count each representation of n as $p_1 + p_2$ with a weight $\log p_1 \log p_2$: this will make things easier, while still retaining the most important feature, that is, $r_2(n) > 0$ if and only if $R_2(n) > 0$. Therefore, the goal of the proof of Goldbach's conjecture in its original form, that $r_2(n) > 0$ for large even n , may be achieved by proving that $R_2(n) > 0$ for large even n . Using the traditional notation we set

$$S(\alpha) = S_N(\alpha) \stackrel{\text{def}}{=} \sum_{p \leq N} (\log p) e(p\alpha) \quad \text{and} \quad \theta(N; q, a) \stackrel{\text{def}}{=} \sum_{\substack{p \leq N \\ p \equiv a \pmod{q}}} \log p.$$

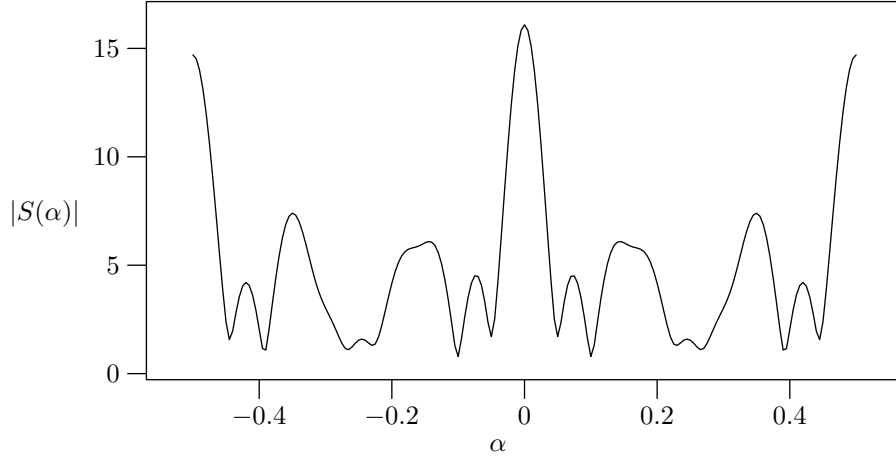


Figure 2: The graph of the function $|S_{20}(\alpha)|$ showing peaks close to the rational values $\alpha = 0, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}$; in $\alpha = \frac{1}{4}, \frac{3}{4}$ there are no peaks because $\mu(4) = 0$.

By the orthogonality relation (1.9), for $n \leq N$ we have

$$\int_0^1 S(\alpha)^2 e(-n\alpha) d\alpha = \sum_{p_1 \leq N} \sum_{p_2 \leq N} \log p_1 \log p_2 \int_0^1 e((p_1 + p_2 - n)\alpha) d\alpha = R_2(n). \quad (2.1)$$

Once again, this is the Fourier coefficient formula for the function S^2 : compare (1.8). Since there are no singularities whatsoever on the circle of integration (though, strictly speaking, the circle has now been replaced by the interval $[0, 1]$) we may wonder what plays the role of the major arcs: the distribution of prime numbers in arithmetic progressions enters the picture, and we recall a basic result from analytic number theory.

Theorem 2.1 *For any fixed $A > 0$, there exists a constant $C = C(A) > 0$ such that for $N \rightarrow +\infty$ and uniformly for all $q \leq (\log N)^A$ and for all integers a such that $(a, q) = 1$ we have*

$$\theta(N; q, a) = \frac{N}{\phi(q)} + E_1(N; q, a),$$

where

$$E_1(N; q, a) = O_A\left(N \exp\{-C(A) \sqrt{\log N}\}\right).$$

Before working it out in general, we compute $S(0)$, $S(\frac{1}{2})$, $S(\frac{1}{3})$, $S(\frac{1}{4})$, and compare our result with the graph shown in Figure 2. It is quite straightforward that $S(0) = \theta(N; 1, 1) \sim N$ by Theorem 2.1; if we compute $S(\frac{1}{2})$ we see that

$$S\left(\frac{1}{2}\right) = \sum_{p \leq N} (\log p) e^{i\pi p} = \log 2 - \sum_{\substack{p \leq N \\ p \equiv 1 \pmod{2}}} \log p = \log 2 - \theta(N; 2, 1) \sim -N,$$

since all primes $p \geq 3$ are odd so that $e^{i\pi p} = -1$. A quite similar thing happens if we compute $S(\frac{1}{3})$:

$$\begin{aligned}
S\left(\frac{1}{3}\right) &= \log 3 + \sum_{\substack{p \leq N \\ p \equiv 1 \pmod{3}}} (\log p) e^{2i\pi p/3} + \sum_{\substack{p \leq N \\ p \equiv 2 \pmod{3}}} (\log p) e^{2i\pi p/3} \\
&= \log 3 + e^{2i\pi/3} \sum_{\substack{p \leq N \\ p \equiv 1 \pmod{3}}} \log p + e^{4i\pi/3} \sum_{\substack{p \leq N \\ p \equiv 2 \pmod{3}}} \log p \\
&= e^{2i\pi/3} \theta(N; 3, 1) + e^{4i\pi/3} \theta(N; 3, 2) + \log 3 \\
&= (e^{2i\pi/3} + e^{4i\pi/3}) \frac{N}{2} + O\left(N \exp\{-C\sqrt{\log N}\}\right) \\
&= -\frac{N}{2} + O\left(N \exp\{-C\sqrt{\log N}\}\right),
\end{aligned} \tag{2.2}$$

by Theorem 2.1. We leave the computation of $S(\frac{1}{4})$ as an exercise to the reader: the most important difference lies in the fact that the sum of roots of unity that occurs in (2.2) is replaced by $i - i = 0$, so that $S(\frac{1}{4}) = O(N \exp\{-C\sqrt{\log N}\})$.

More generally, we now compute S at a rational number a/q , for $1 \leq a \leq q$ and $(a, q) = 1$:

$$\begin{aligned}
S\left(\frac{a}{q}\right) &= \sum_{h=1}^q \sum_{\substack{p \leq N \\ p \equiv h \pmod{q}}} (\log p) e\left(\frac{ap}{q}\right) = \sum_{h=1}^q e\left(\frac{ah}{q}\right) \sum_{\substack{p \leq N \\ p \equiv h \pmod{q}}} \log p \\
&= \sum_{h=1}^q e\left(\frac{ah}{q}\right) \theta(N; q, h) = \sum_{h=1}^q e\left(\frac{ah}{q}\right) \theta(N; q, h) + O(\log q),
\end{aligned} \tag{2.3}$$

where the $*$ means that we have attached the condition $(h, q) = 1$ to the corresponding sum. By Theorem A.1 and (2.3) we have

$$\begin{aligned}
S\left(\frac{a}{q}\right) &= \frac{N}{\phi(q)} \sum_{h=1}^q e\left(\frac{ah}{q}\right) + \sum_{h=1}^q e\left(\frac{ah}{q}\right) E_1(N; q, h) + O(\log q) \\
&= \frac{\mu(q)}{\phi(q)} N + O\left(N \exp\{-C\sqrt{\log N}\}\right),
\end{aligned} \tag{2.4}$$

where μ denotes the Möbius function. This formula suggests that $|S(\alpha)|$ is fairly large when α is a rational number a/q , and that the size of $|S(a/q)|$ decreases essentially as q^{-1} . Since S is a continuous function, we may expect that $|S|$ be large in a neighbourhood of a/q , and we will exploit this fact to find an approximate formula for $R_2(n)$. We begin by extending the influence of the peak near a/q as much as possible: the simplest tool to use in this context is partial summation.

Lemma 2.2 *For any choice of $A > 0$, there exists a positive constant $C = C(A)$ such that for $1 \leq a \leq q \leq P := (\log N)^A$, with $(a, q) = 1$ and for $|\eta| \leq PN^{-1}$ we have*

$$S\left(\frac{a}{q} + \eta\right) = \frac{\mu(q)}{\phi(q)} T(\eta) + E_2(N; q, a, \eta) \quad (2.5)$$

where

$$E_2(N; q, a, \eta) = O_A\left(N \exp\{-C(A)\sqrt{\log N}\}\right).$$

This is Lemma 3.1 of Vaughan [19]: the main ingredients for the proof are Theorem 2.1, partial summation, equation (2.4) and Theorem A.1. In a sense, the peak of S at a/q can be approximated fairly well by means of the peak of T at 0, after a suitable rescaling. Theorem 2.1 implies that the coefficient in $S(\alpha)$ is 1 on average, as the coefficient in $T(\alpha)$, which is a much easier function to study.

For $q \leq P$, we denote by $\mathfrak{M}(q, a) := \left[\frac{a}{q} - \frac{P}{N}, \frac{a}{q} + \frac{P}{N}\right]$ the *major arc* pertaining to the rational number with “small” denominator a/q , and write

$$\mathfrak{M} \stackrel{\text{def}}{=} \bigcup_{q \leq P} \bigcup_{a=1}^q \mathfrak{M}(q, a) \quad \text{and} \quad \mathfrak{m} \stackrel{\text{def}}{=} \left[\frac{P}{N}, 1 + \frac{P}{N}\right] \setminus \mathfrak{M},$$

where, once again, $*$ means that we attach the condition $(a, q) = 1$. Therefore, \mathfrak{M} is the set of the major arcs, and Lemma 2.2 suggests that it is the set where $|S|$ is fairly large. Its complement \mathfrak{m} is the set of the *minor arcs*. We translated the integration interval from $[0, 1]$ to $\left[\frac{P}{N}, 1 + \frac{P}{N}\right]$ in order to avoid two “half arcs” at 0 and 1, but this is legitimate since all functions involved have period 1.

The proof of this Lemma shows clearly that the major arcs can not be too numerous or too wide if we want to keep the resulting error term under control. We will use this result to find a quantitative version of Goldbach’s conjecture, that was first justified along these lines by Hardy & Littlewood [8, 9].

For $n \leq N$, from Equation (2.1) we deduce

$$\begin{aligned} R_2(n) &= \int_0^1 S(\alpha)^2 e(-n\alpha) d\alpha = \left(\int_{\mathfrak{M}} + \int_{\mathfrak{m}} \right) S(\alpha)^2 e(-n\alpha) d\alpha \\ &= \sum_{q \leq P} \sum_{a=1}^q \int_{-P/N}^{P/N} S\left(\frac{a}{q} + \eta\right)^2 e\left(-n\left(\frac{a}{q} + \eta\right)\right) d\eta + \int_{\mathfrak{m}} S(\alpha)^2 e(-n\alpha) d\alpha \\ &= R_{\mathfrak{M}}(n) + R_{\mathfrak{m}}(n), \end{aligned}$$

say. From now on we write \approx to indicate an expected asymptotic equality. For the time being we neglect the contribution of the minor arcs $R_{\mathfrak{m}}(n)$ and all the error terms that have arisen so far. By Equation (2.5) we have

$$R_{\mathfrak{M}}(n) \approx \sum_{q \leq P} \sum_{a=1}^q \int_{-P/N}^{P/N} \frac{\mu(q)^2}{\phi(q)^2} T(\eta)^2 e\left(-n\left(\frac{a}{q} + \eta\right)\right) d\eta$$

$$= \sum_{q \leq P} \frac{\mu(q)^2}{\phi(q)^2} \sum_{a=1}^q e(-n \frac{a}{q}) \int_{-P/N}^{P/N} T(\eta)^2 e(-n\eta) d\eta. \quad (2.6)$$

We extend the integral to the whole interval $[0, 1]$ and recall the result from the previous section:

$$\int_0^1 T(\eta)^2 e(-n\eta) d\eta = \sum_{\substack{m_1+m_2=n \\ m_1 \geq 0, m_2 \geq 0}} 1 = n+1 \sim n. \quad (2.7)$$

Since $(P/N) \cdot N \rightarrow \infty$, we see that (1.12) implies that the interval $[P/N, 1 - P/N]$ gives a contribution $o(n)$. Therefore we expect that

$$R_{\mathfrak{M}}(n) \approx n \sum_{q \leq P} \frac{\mu(q)^2}{\phi(q)^2} \sum_{a=1}^q e(-n \frac{a}{q}) = n \sum_{q \leq P} \frac{\mu(q)^2}{\phi(q)^2} c_q(n), \quad (2.8)$$

where c_q is the Ramanujan sum defined in Theorem A.1. The next step is to extend the summation to $q \geq 1$, with the idea of using Theorem A.2, since the summand is a multiplicative function of q by Theorem A.1: we skip the detailed proof that the error term arising from this operation is of lower order of magnitude.¹ Now, by Theorem A.2, the right hand side of Equation (2.8) becomes

$$\begin{aligned} R_{\mathfrak{M}}(n) &\approx n \sum_{q \leq P} \frac{\mu(q)^2}{\phi(q)^2} c_q(n) \approx n \sum_{q \geq 1} \frac{\mu(q)^2}{\phi(q)^2} c_q(n) \\ &= n \prod_p (1 + f_n(p) + f_n(p^2) + \dots) \end{aligned} \quad (2.9)$$

where the product is taken over all prime numbers and $f_n(q) = \mu(q)^2 c_q(n) / \phi(q)^2$. Obviously $f_n(p^\alpha) = 0$ for $\alpha \geq 2$, and for $\alpha = 1$ Theorem A.1 implies that

$$f_n(p) = \frac{\mu(p)^2 \mu(p/(p,n))}{\phi(p) \phi(p/(p,n))} = \begin{cases} \frac{1}{p-1} & \text{if } p \mid n, \\ -\frac{1}{(p-1)^2} & \text{if } p \nmid n. \end{cases}$$

If n is odd, the factor $1 + f_n(2)$ vanishes, and Equation (2.9) predicts that we should not expect any representation of n as a sum of two primes. In fact, if n is odd then $R_2(n) = 0$ if $n - 2$ is not a prime number, and $R_2(n) = 2 \log(n - 2)$ if $n - 2$ is a prime number: the result in (2.9) should be understood as $R_2(n) = o(n)$. Conversely, if n is even we may transform Equation (2.9) by means of some easy computation:

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

¹Actually, this is strictly true only on average over n : see Vaughan [19], Chapter 3.

$$\begin{aligned}
&= 2n \prod_{\substack{p|n \\ p>2}} \left(\frac{p}{p-1} \cdot \frac{(p-1)^2}{p(p-2)} \right) \prod_{p>2} \left(1 - \frac{1}{(p-1)^2} \right) \\
&= 2C_0 n \prod_{\substack{p|n \\ p>2}} \frac{p-1}{p-2} = n\mathfrak{S}(n),
\end{aligned} \tag{2.10}$$

where $2C_0$ is the so-called twin-prime constant, and $\mathfrak{S}(n)$ is the *singular series* defined by

$$C_0 \stackrel{\text{def}}{=} \prod_{p>2} \left(1 - \frac{1}{(p-1)^2} \right) \quad \text{and} \quad \mathfrak{S}(n) \stackrel{\text{def}}{=} 2C_0 \prod_{\substack{p|n \\ p>2}} \frac{p-1}{p-2}. \tag{2.11}$$

Equation (2.10) is the asymptotic formula for $R_2(n)$ found by Hardy & Littlewood: of course, it would imply the truth of Goldbach's conjecture, but it is much stronger. In the next paragraph we explain why, in the current state of knowledge, it is impossible to prove it. It is clear from (2.10) that the weighted number of representations depends on the size of n and also on its prime factorization: it is a nice exercise in sieve theory to see why it has to be so.

We conclude this section noticing that Equation (2.1) implies that

$$R_2(n) \leq \int_0^1 |S(\alpha)|^2 d\alpha = \sum_{p \leq N} (\log p)^2 \leq \theta(N) \log N \sim N \log N \tag{2.12}$$

by Theorem 2.1, so that for n close to N the expected asymptotic formula (2.10) does not differ too much from this upper bound.

3 Where are the difficulties?

For the sake of brevity, we only describe the two more important questions that remain to be settled: the approximation of the Chebyshev θ function, and the contribution of the minor arcs.

3.1 Approximation of the Chebyshev theta function

The approximation of θ provided by the Prime Number Theorem for Arithmetic Progressions 2.1 is quite weak for two main reasons: we remarked above that it is only valid in a fairly restricted range of values for q , and this forces a rather small choice of P , the parameter that we use to define the major arcs.

The second reason is that is that the upper bound known today for the error term is too large: in fact, it is conjectured that its true order of magnitude is much

smaller. It is well known that the difference $\theta(N; q, a) - N/\phi(q)$ depends essentially on a sum whose summands have the shape $N^\rho/(\phi(q)\rho)$, where ρ denotes the generic complex zero of suitable Dirichlet L functions. In the simplest case, when $q = a = 1$, the relation referred to can be written in the form

$$\theta(N) = N - \sum_{\substack{\rho \in \mathbb{C} \text{ s. t. } \zeta(\rho)=0 \\ \rho = \beta + i\gamma, \\ |\gamma| \leq T}} \frac{N^\rho}{\rho} + O\left(\frac{N}{T}(\log N)^2 + \sqrt{N} \log N\right) \quad (3.1)$$

where $\rho = \beta + i\gamma$ is the generic zero of the Riemann zeta function with $\beta \in (0, 1)$, and $T \leq N$. This relation is known as the *explicit formula*, and it suggests that it might be a good idea to replace the function $T(\eta)$ defined in (1.10) with a different approximation for $S\left(\frac{a}{q} + \eta\right)$, namely

$$K(\eta) \stackrel{\text{def}}{=} \sum_{n \leq N} \left(1 - \sum_{|\gamma| \leq T} n^{\rho-1}\right) e(n\eta)$$

where the coefficient of $e(n\eta)$ is the derivative with respect to N of the first two terms in (3.1), evaluated at n (since if f is regular, then $\sum f(n) \sim \int f(t) dt$). This approximation for S is valid only in a neighbourhood of 0, but we can find similar approximations valid on each major arc introducing the Dirichlet L functions. Variants of this idea have been successfully used in several problems.

It is well known that the optimal distribution for prime numbers is achieved if *all* real parts β of all zeros $\rho = \beta + i\gamma$ of the ζ function with $\gamma \neq 0$ are equal to $\frac{1}{2}$ (Riemann Conjecture): in this case, $\theta(N) = N + O\left(N^{1/2}(\log N)^2\right)$. Similarly, if *all* zeros $\beta + i\gamma$ of all Dirichlet L functions with $\beta \in (0, 1)$ have real part $\frac{1}{2}$ (Generalized Riemann Conjecture), then for $q \leq x$

$$\theta(N; q, a) = \frac{N}{\phi(q)} + O\left(N^{1/2}(\log N)^2\right). \quad (3.2)$$

The exponent of N in the error term of (3.2) is optimal, and it can not be replaced by a smaller one. In particular, Goldbach's Conjecture *does not* follow from the Generalized Riemann Conjecture (3.2). We finally remark that the general case $q > 1$ is harder than the case $q = 1$: in fact in the present state of knowledge it is not still possible to rule out the existence of a *real* zero $\beta \in (0, 1)$ of some Dirichlet L function, with β very close to 1. This, essentially, is the reason why we had to impose a rather severe limitation for q in Theorem 2.1. In fact, the contribution from this zero would be $\pm N^\beta/(\phi(q)\beta)$, that is, very close to the "main term" $N/\phi(q)$, and it might spoil the asymptotic formula for $\theta(N; q, a)$ for this particular value of q , with consequences on the asymptotic formula for $R_2(n)$.

3.2 The contribution from minor arcs

The main problem concerning minor arcs is that it is not possible to give an individual estimate for their contribution: it is comparatively easy to prove that *on average* over the integers $n \in [1, N]$ the minor arcs give a negligible contribution to $R_2(n)$, but it is not possible to prove the same thing for any single n . By the Fourier coefficient formula, Bessel's inequality and the Prime Number Theorem 2.1 with $q = 1$ we have

$$\begin{aligned} \sum_{n \leq N} \left| \int_{\mathfrak{m}} S(\alpha)^2 e(-n\alpha) d\alpha \right|^2 &\leq \int_{\mathfrak{m}} |S(\alpha)|^4 d\alpha \leq \sup_{\alpha \in \mathfrak{m}} |S(\alpha)|^2 \int_0^1 |S(\alpha)|^2 d\alpha \\ &= O\left(N \log N \sup_{\alpha \in \mathfrak{m}} |S(\alpha)|^2\right). \end{aligned}$$

Equation (2.4) suggests (and the following Lemma proves, albeit in a slightly weaker form) that the supremum in the last formula should be roughly $N^2 P^{-2}$, since if $\alpha \in \mathfrak{m}$ then it is “close” to a rational with denominator $> P$.

Lemma 3.1 *For $1 \leq a \leq q \leq N$, $(a, q) = 1$ and $|\eta| \leq q^{-2}$ we have*

$$S\left(\frac{a}{q} + \eta\right) \ll (\log N)^4 (Nq^{-1/2} + N^{4/5} + N^{1/2} q^{1/2}).$$

This is Theorem 3.1 of Vaughan [19]. It implies that

$$\sum_{n \leq N} |R_{\mathfrak{m}}(n)|^2 = \sum_{n \leq N} \left| \int_{\mathfrak{m}} S(\alpha)^2 e(-n\alpha) d\alpha \right|^2 = O(N^3 (\log N)^9 P^{-1}), \quad (3.3)$$

since every point on $[0, 1]$ is within q^{-2} from a rational a/q (this is an elementary result of Dirichlet), and on the minor arcs $q > P$. In its turn, Equation (3.3) implies that for the majority of values $n \in [1, N]$ we have that $|R_{\mathfrak{m}}(n)|$ is of lower order of magnitude than the contribution from the major arcs provided by (2.9).

We remark that the measure of the minor arcs is $1 + o(1)$, so that the major arcs represent a tiny portion of the interval $[0, 1]$.

4 Results for “almost all” even integers

The argument sketched in Section 2 is not strong enough to prove Goldbach's Conjecture, but it can still be used to prove some interesting, albeit weaker, results. In particular, we now prove that even integers n such that $R_2(n) = 0$ are comparatively rare: more precisely, let us set $\mathcal{E}(N) := \{n \leq N : n \text{ is even and } R_2(n) = 0\}$. We will prove that, given $B > 0$, we have $|\mathcal{E}(N)| = O_B(N(\log N)^{-B})$.

Theorem 4.1 *Given $B > 0$ we have*

$$\sum_{n \leq N} |R_2(n) - n\mathfrak{S}(n)|^2 \ll_B N^3 (\log N)^{-B}.$$

Sketch of the proof. Using the ideas in §2, it is not too difficult to give a rigorous proof of the fact that for $n \leq N$ we have

$$R_{\mathfrak{M}}(n) = n\mathfrak{S}(n, P) + O_A(n(\log n)P^{-1}) \quad (4.1)$$

using Lemma 2.2 and Equations (1.11), (2.6)–(2.7), where

$$\mathfrak{S}(n, P) \stackrel{\text{def}}{=} \sum_{q \leq P} \frac{\mu(q)^2}{\phi(q)^2} c_q(n). \quad (4.2)$$

Theorems A.2, A.1 and standard estimates concerning Euler’s ϕ function, show that

$$\sum_{n \leq N} |\mathfrak{S}(n, P) - \mathfrak{S}(n)|^2 \ll N(\log N)^2 P^{-1}. \quad (4.3)$$

The elementary inequality $|a + b + c|^2 \leq 3(|a|^2 + |b|^2 + |c|^2)$ implies

$$\begin{aligned} \sum_{n \leq N} |R_2(n) - n\mathfrak{S}(n)|^2 &\ll \sum_{n \leq N} |R_{\mathfrak{M}}(n) - n\mathfrak{S}(n, P)|^2 \\ &\quad + \sum_{n \leq N} |n\mathfrak{S}(n, P) - n\mathfrak{S}(n)|^2 + \sum_{n \leq N} |R_{\mathfrak{m}}(n)|^2 \\ &\ll N^3 (\log N)^{2-2A} + N^3 (\log N)^{2-A} + N^3 (\log N)^{9-A} \\ &\ll N^3 (\log N)^{9-A} \end{aligned}$$

by (3.3), (4.1)–(4.3). Theorem 4.1 follows choosing $A \geq B + 9$. \square

Finally, let $\mathcal{E}'(N) := \{n \in [\frac{1}{2}N, N] : n \text{ is even and } R_2(n) = 0\} = \mathcal{E}(N) \cap [\frac{1}{2}N, N]$. Equation (2.11) implies that $\mathfrak{S}(n) \geq 2C_0$ when n is even, so that

$$\begin{aligned} \sum_{n \leq N} |R_2(n) - n\mathfrak{S}(n)|^2 &\geq \sum_{\substack{n \leq N, 2|n \\ R_2(n)=0}} |2C_0 n|^2 \geq \sum_{\substack{N/2 \leq n \leq N, 2|n \\ R_2(n)=0}} |2C_0 n|^2 \\ &\geq \frac{1}{2} C_0^2 |\mathcal{E}'(N)| N^2, \end{aligned}$$

and $|\mathcal{E}'(N)| = O_B(N(\log N)^{-B})$ for any $B > 0$. The result for $\mathcal{E}(N)$ follows by decomposing the interval $[1, N]$ into $O(\log N)$ intervals of type $[\frac{1}{2}M, M]$.

5 Vinogradov's three-prime theorem

The circle method can be successfully applied to many different problems: for example, using a notation consistent with the one above, we have

$$R_3(n) \stackrel{\text{def}}{=} \sum_{p_1+p_2+p_3=n} \log p_1 \log p_2 \log p_3 = \int_0^1 S(\alpha)^3 e(-n\alpha) d\alpha$$

if $n \leq N$. An argument similar to the one in the previous sections shows that $R_3(n)$ is well approximated by the contribution of the major arcs alone, and this yields

$$R_3(n) = \frac{1}{2} n^2 \mathfrak{S}_3(n) + O_A(n^2 (\log n)^{-A}), \quad (5.1)$$

for any positive A . Here

$$\mathfrak{S}_3(n) \stackrel{\text{def}}{=} \prod_{p|n} \left(1 + \frac{1}{(p-1)^3}\right) \cdot \prod_{p \nmid n} \left(1 - \frac{1}{(p-1)^2}\right).$$

Having three summands in place of two changes radically the nature of the problem: we are content to remark that in this case an individual upper bound for the contribution of the minor arcs is indeed possible. In fact, Lemma 3.1 implies, for $n \leq N$ and $q > P$, that

$$\left| \int_{\mathfrak{m}} S(\alpha)^3 e(-n\alpha) d\alpha \right| \leq \sup_{\alpha \in \mathfrak{m}} |S(\alpha)| \int_0^1 |S(\alpha)|^2 d\alpha = O(n^2 (\log n)^4 P^{-1/2}). \quad (5.2)$$

Finally, we conclude noticing that a very simple computation shows that the twin-prime problem is naturally linked to Goldbach's conjecture: in fact, we have

$$\theta_N(n) \stackrel{\text{def}}{=} \sum_{\substack{p_2 \leq N \\ p_2 - p_1 = n}} \log p_1 \log p_2 = \int_0^1 |S(\alpha)|^2 e(-n\alpha) d\alpha,$$

as a short computation shows. This means that the two problems are strictly related and are of the same degree of difficulty.

A Some useful results

Theorem A.1 (Ramanujan) *The Ramanujan sum $c_q(n)$ defined below is a multiplicative function of q , and*

$$c_q(n) \stackrel{\text{def}}{=} \sum_{h=1}^q e\left(\frac{hn}{q}\right) = \mu\left(\frac{q}{(q,n)}\right) \frac{\phi(q)}{\phi(q/(q,n))}.$$

Theorem A.2 (Euler Product) *Let f be a multiplicative function such that the series $\sum_{n \geq 1} f(n)$ is absolutely convergent. Then the following identity holds*

$$\sum_{n \geq 1} f(n) = \prod_p \left(1 + f(p) + f(p^2) + f(p^3) + \cdots \right),$$

where the product is taken over all prime numbers and is absolutely convergent.

B Recommended reading

The standard reference for the circle method is Vaughan’s monograph [19]: see in particular Chapter 1. See also Hardy [7] Chapter 8 (in particular §§8.1–8.7), James [13] §5, and Ellison [4] for the history of Waring’s problem. The genesis of the idea of studying the behaviour of the generating function in the neighbourhood of many singularities is clearly explained in Hardy & Ramanujan [10] (in particular §§1.2–1.5) and in Hardy [7] Chapter 8 (in particular §§8.6–8.7). For Waring’s problem see Hardy & Wright [11] Chapters 20–21 for an introduction, and Vaughan [19] for a detailed study. For the relationship between Laurent series and Fourier series see Titchmarsh [18] §13.12. See also the survey by Kumchev & Tolev [14].

Set $\mathcal{E}(N) := \{2n \leq N : r_2(2n) = 0\}$. The complete detailed proof that for any $A > 0$ we have $|\mathcal{E}(N)| = O_A(N(\log N)^{-A})$ is in §3.2 of Vaughan [19]. Montgomery & Vaughan [16] proved the stronger result that $|\mathcal{E}(N)| \ll N^{1-\delta}$ for some $\delta > 0$. A discussion of many problems related to variants of the Goldbach Conjecture can be found in Languasco [15], while Zaccagnini [20] deals with “mixed” problems with primes and powers. A heuristic argument in favour of the twin-prime conjecture can be found in Hardy & Wright [11], §22.20. See the introduction of Halberstam & Richert [6] for the general setting of the Schinzel & Sierpiński’s conjectures and the notes for a quantitative version of the same conjectures due to Bateman & Horn. An upper bound for $r_2(n)$ of the correct order of magnitude is contained in Theorem 3.11. See Zaccagnini [21] for an elementary heuristic argument (based on a variant of Eratosthenes’ sieve) in support of the asymptotic formula (2.10): in particular see Equations (6), (8) and (10), and the “Coda.” Other strategies for the proof of Goldbach’s Conjecture are discussed in Ribenboim [17] §4.VI. See also Guy [5] §C.1 for further references.

For Equations (3.2) and (3.3) see Davenport [2] Chapter 20 and Chapter 25 respectively. Chen proved that every large even integer can be written as a sum of a prime and of an integer with at most 2 prime factors: see Halberstam & Richert [6] Chapter 10, or Bombieri [1] §9 for a comparatively simple proof with 4 in place of 2.

Equation (5.2) is in Davenport [2] Chapter 26. The Ternary Goldbach Problem is discussed in [2] Chapter 26 or [19] §3.1. Deshouillers, Effinger, te Riele & Zinoviev [3] proved that if the Generalized Riemann Conjecture is true then every odd integer $n \geq 7$ is a sum of three primes. Theorem A.1 is Theorem 272 of Hardy & Wright [11]. For useful results on the distribution of primes or the properties of the Riemann zeta function, see [2] Chapters 7–18, or Ivić [12] Chapters 11–12.

References

- [1] E. Bombieri. *Le Grand Crible dans la Théorie Analytique des Nombres*. Societé Mathématique de France, Paris, 1974. Astérisque n. 18.
- [2] H. Davenport. *Multiplicative Number Theory*. Graduate Texts in Mathematics 74. Springer-Verlag, third edition, 2000.
- [3] J.-M. Deshouillers, G. Effinger, H. te Riele, and D. Zinoviev. A complete Vinogradov 3-primes Theorem under the Riemann Hypothesis. *Electr. Res. Announcements American Mathematical Society*, 3:99–104, 1997.
- [4] W. J. Ellison. Waring’s problem. *Amer. Math. Monthly*, 78:10–36, 1971.
- [5] R. K. Guy. *Unsolved Problems in Number Theory*. Springer-Verlag, second edition, 1994.
- [6] H. Halberstam and H.-E. Richert. *Sieve Methods*. Academic Press, London, 1974.
- [7] G. H. Hardy. *Ramanujan, Twelve lectures on subjects suggested by his life and works*. Chelsea, New York, third edition, 1999.
- [8] G. H. Hardy and J. E. Littlewood. Some problems in “Partitio Numerorum”; III. On the expression of a number as a sum of primes. *Acta Mathematica*, 44:1–70, 1923.
- [9] G. H. Hardy and J. E. Littlewood. Some problems of “Partitio Numerorum”; V. A further contribution to the study of Goldbach’s problem. *Proceedings of the London Mathematical Society (2)*, 22:46–56, 1923.
- [10] G. H. Hardy and S. Ramanujan. Asymptotic formulae in combinatory analysis. *Proceedings of the London Mathematical Society (2)*, 17:75–115, 1918. = S. Ramanujan, “Collected papers,” edited by G. H. Hardy, P. V. Seshu Aiyar and B. M. Wilson, Third ed., AMS–Chelsea, 1999; n. 36, 276–309.

- [11] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford Science Publications, Oxford, fifth edition, 1979.
- [12] A. Ivić. *The Theory of the Riemann Zeta-Function*. J. Wiley, New York, 1985.
- [13] R. D. James. Recent progress in the Goldbach problem. *Bulletin American Mathematical Society*, 55:246–260, 1949.
- [14] A. V. Kumchev and D. I. Tolev. An invitation to additive prime number theory, 2004. <http://www.ma.utexas.edu/~kumchev/A19.ps>.
- [15] A. Languasco. Some results on Goldbach’s problem. *Rend. Sem. Mat. Univ. Pol. Torino*, 53 (4):325–337, 1995.
- [16] H. L. Montgomery and R. C. Vaughan. The exceptional set in Goldbach’s problem. *Acta Arithmetica*, 27:353–370, 1975.
- [17] P. Ribenboim. *The New Book of Prime Numbers Records*. Springer-Verlag, New York, 1996.
- [18] E. C. Titchmarsh. *The Theory of Functions*. Oxford University Press, Oxford, second edition, 1988.
- [19] R. C. Vaughan. *The Hardy–Littlewood Method*. Cambridge University Press, Cambridge, second edition, 1997.
- [20] A. Zaccagnini. Additive problems with prime numbers. *Rend. Sem. Mat. Univ. Pol. Torino*, 53 (4):471–486, 1995. Atti del “Primo Incontro Italiano di Teoria dei Numeri,” Roma, 3–5 gennaio 1995.
- [21] A. Zaccagnini. Goldbach Variations: problems with prime numbers. *L’Educazione Matematica, Anno XXI, Serie VI*, 2:47–57, 2000. http://www.math.unipr.it/~zaccagni/psfiles/papers/Goldbach_E.pdf.

Prof. Alessandro Zaccagnini
Dipartimento di Matematica
Università degli Studi di Parma
Parco Area delle Scienze, 53/a
43100 Parma, ITALIA

Tel. 0521 906902 – Telefax 0521 906950

e-mail: alessandro.zaccagnini@unipr.it

web page: <http://www.math.unipr.it/~zaccagni/home.html>