Mathematics Department
Universidad Autónoma de Madrid

Questions of Arithmetic and Harmonic Analysis

Adrián Ubis Martínez

PhD Thesis. Thesis Advisor: Fernando Chamizo Lorente

Madrid, June 2006

To my parents.
To María.

Preface

This memory contains the study of several mathematical problems of diverse character, structured into three chapters, that could be said to belong to the areas of Number Theory and of Harmonic Analysis.

But, what does it mean for a problem to be in one area or another? Perhaps we want to express that it arises in a natural way inside a theory, or maybe that the methods used in the solution belong to a determined kind of reasonings.

As anyone who has worked on mathematics knows, these two ways of understanding the question not always coincide, which is natural, because a theory grows in part due to questions that escape to it. The unique hope of going beyond is using any tool at our disposal. The problems we are going to solve in the following pages are an example of it.

In chapter 1 we treat Fourier series with frequencies in the k-powers, that are functions of chaotic behaviour. Its comprehension will require to work with Gauss sums, Large Sieve inequalities and wavelets, things in principle not related to the regularity of a function.

Class number of a quadratic number field (or equivalently class number of quadratic binary forms), that is the theme of chapter 2, is an amazing quantity that measures how far is the ring of integers of being a unique factorization domain. Nevertheless its behaviour in average can be understood, through some ideas of hyperbolic geometry, as a lattice point problem a thus can be controlled with Harmonic Analysis' tools, or through Dirichlet L functions and the related character sums.

If we are given two small sets A and C of integers, it is easy to decide if there exists another set B such that the sums of the elements of A and B give exactly the elements of C. In chapter 3 we shall show that to study this problem more precisely will require Fourier Analysis in finite fields, as well as combinatorial an geometric arguments.

Most of the results in this memory can be found in the research papers and preprints [CCU, CU1, CU2, GU, Ubi]. But their story, as always happens, has been more involved. I remember very well when, during a research stay in Montreal, I was sat down with Andrew Granville waiting for him to propose me a problem to work for the following four months. Instead, he asked me which questions I was interested in. I told him I wanted to learn things on L functions, and he answered this was too general. After that I said I had been reading some papers of B. Green and I. Ruzsa that Javier Cilleruelo had recommended me, and then he told me the problem on sumsets. For large sets I soon realized that Green-Ruzsa method worked. For small sets,

Granville said it could probably be treated by means of recurrences. From that moment I have been working on this problem, giving only small steps in its understanding.

When I began to research with Fernando Chamizo, he proposed me the question of studying Fourier series with frequencies in polynomials of degree larger than two, extending in that way the work done by S. Jaffard. He said Poisson formula could be used to handle the function near the rationals and besides, the irrationals could be understood from that simpler case. By my clumsiness with these analytic tools it took my some time to understand correctly in which way I had to proceed. In the end we were able to control the function very near of the rationals, but we were very far from the knowledge reached in the quadratic case. In the beginning I did not understand Jaffard's paper completely, in part due to my lack of experience with wavelets. Although in the end I have realized that wavelets are not strictly necessary, they have helped me to understand the real dimension of the problem and to give a partial solution.

In the problem of class number it has been very beautiful to share Gauss' worries, and to understand the methods of Siegel, Shintani and Chamizo-Iwaniec, and to be able to apply them to the positive discriminant case. When finally we obtained the bound for the error term, the natural question was to discover the actual size and behaviour of that term. First I tried to use the summation formulas we had obtained to attack this problem, without success. Later I understood that it was possible (and more natural) to treat the error term directly through Dirichlet class number formula. This second option worked, showing once more the importance of adapting ourselves to the problem we are solving, of using the suitable language and techniques.

Only remains to me the duty of paying the debt I have with the people that have made possible this project, acknowledging its support profoundly: in the first place to my thesis advisor, Fernando Chamizo. To say that Fernando has surpassed the limit of what can be expected of a supervisor, as person as well as mathematician, would be not accurate. He has taught me, with patience and dedication, everything I know on Analytic Number Theory. He has borne my ups and downs, supporting me until the last moment. I think he is an example to follow. In the second place to Andrew, who showed me how to do mathematics, thanks to his enthusiasm and firmness. His ideas made possible chapter 3 of this memory. To Javier Cilleruelo, who guided me in the beginning and made me understand that Additive Number Theory is more involved and beautiful than I thought before. To my office colleagues: Blanca that has taught me so much, Susi, Connie, Nati, Paloma, Jose, Charro and our Thursday's talks. Also to my friends Mari Luz and Elena, and to the rest of graduate students: Ana that cares of everyone of us, Angélica,

Liviu, ... In general I have felt a great atmosphere in this department. To my family and friends for their wholehearted support; to María for his help with programming and for everything else; to Hakima and her family, that treated me as a son; to Manolo for having showed me the amazing world of number theory; to Paulo for those four months of arguments; to Jorge for carrying (brilliantly) the hard duty of being the reviewer of this thesis, and for encouragement.

Contents

Chapter 1

Fourier series with polynomial frequencies

1.1 Introduction

The first published example of a continuous nowhere differentiable function was obtained by Weierstrass:

$$f(x) = \sum_{n=0}^{\infty} a^n \cos(\pi b^n x),$$

with b an odd integer, $0 < a < 1$ and $ab > 1 + 3\pi/2$. But Weierstrass did not think he was the first mathematician in finding such kind of function, because in 1873 he sent a letter to Du Bois-Reymond saying that already in 1861 Riemann had stated that

$$f(x) = \sum_{n=1}^{\infty} \frac{\sin(\pi n^2 x)}{n^2}$$

was not differentiable at any point.

In1916 Hardy [Har] gave a great step in the study of Riemann's function and understood perfectly the smoothness of Weierstrass' function. He did so by associating to any absolutely convergent series

$$f(\theta) = \Re \sum_{n=0}^{\infty} a_n e^{in\theta}$$

the harmonic function

$$F(r, \theta) = \Re \sum_{n=0}^{\infty} a_n r^n e^{in\theta}.$$

He showed that the smoothness of f can be measured through the derivative of F in θ. In a precise way, if for $0 < \delta < 1$

$$f(\theta) - f(\theta_0) = o((\theta - \theta_0)^\delta)$$

holds, then

$$\frac{\partial F(r,\theta)}{\partial \theta}\Big|_{\theta=\theta_0} = o\big((1-r)^{\delta-1}\big) \qquad r \to 1^-.$$

He proved this by writing $F(r,\theta)$ as the integral

$$F(r,\theta) = \Re \frac{1}{2\pi} \int_0^{2\pi} f(t)\left(\frac{2}{1 - re^{i(\theta-t)}} - 1\right), dt$$

that is using Poisson's kernel. These were the beginnings of Hardy's spaces. To see the regularity of Weierstrass' function, Hardy had to study the behaviour of the function

$$\frac{\partial F(r,\theta)}{\partial \theta} = -\pi \sum_{n=0}^{\infty} (ab)^n r^{b^n} \sin(b^n \pi \theta)$$

where r is near to 1. From that he could prove, without any trouble, that whenever $ab > 1$, $0 < a < 1$ Weierstrass' function satisfies

$$f(x) - f(x_0) = \Omega(|x - x_0|^\delta) \qquad \delta = \frac{\log(1/a)}{\log b} < 1$$

for any $x_0 \in \mathbb{R}$, deducing in particular its non-differentiability.

In the case of Riemann's function, all he had to do was to control

$$\pi \sum_{n=1}^{\infty} r^{n^2} \cos(\pi n^2 x)$$

when r approaches 1. But making the change $r = e^{-\pi y}$, this becomes

$$\theta(z) = \sum_{n \in \mathbb{Z}} e^{i\pi n^2 z} \qquad z = x + iy$$

with $y \to 0^+$. This is Jacobi's theta function, whose behaviour could be studied very well due to the functional equation

$$\theta(z) = e^{\pi i/4} z^{-1/2} \theta(-1/z).$$

In fact, combining it with its periodicity we obtain

$$\theta(z) = e^{\pi i m/4} \theta(\gamma(z)) q^{-1/2} (z - \frac{a}{q})^{-1/2}, \tag{1.1}$$

where $\gamma(z) = (rz+s)/(qz-a)$, $r \equiv a \pmod 2$, $s \equiv q \pmod 2$ holding $ra + sq = -1$ and m is an integer that depends on γ.

Hardy and Littlewood [HL] saw that for every x_0 irrational there exist infinitely many convergents a_n/q_n such that we can take $\gamma(z) = (r_n z + s_n)/(q_n z - a_n)$ with $\Im\gamma(x_0 + i|x_0 - a_n/q_n|) > 1/2$. But in this area θ has an stable behaviour, because $|\theta(z) - 1| < 1/2$ if $\Im z \geq 1/2$. So

$$|\theta(x_0 + i|x_0 - a_n/q_n|)| \asymp q_n^{-1/2}|x_0 - a_n/q_n|^{-1/2},$$

and since $|x_0 - a_n/q_n| < 1/q_n^2$ (see [CiCo]), we have

$$\theta(x_0 + iy) = \Omega(y^{-1/4}).$$

Hence Hardy deduced that Riemann's function satisfies

$$f(x) - f(x_0) = \Omega(|x - x_0|^{3/4})$$

for any x_0 irrational.

But there was a great difference between both functions. For Weierstrass' it can be proved directly (as Hardy did) that

$$f(x) - f(x_0) = O(|x - x_0|^\delta) \qquad \delta = \log(1/a)/\log b < 1$$

for any x_0, demonstrating in this way that the regularity is the same at every point. For Riemann's function this was not true, and Hardy knew it. For instance, for some rational numbers

$$f(x) - f(a/q) = \Omega(|x - a/q|^{1/2}),$$

what did not hold for most of the irrationals. This showed that the regularity of this function changed wildly from one point to another. But there remained to answer Riemann's question: what was the behaviour of the fractions in the orbit of 1? For them (the ones a/q with a, q odd integers) we have

$$\theta(a/q + iy) \to 0,$$

what indicates that the function should be quite regular at these points. It seems that Hardy did not worry about these questions, and in general about the regularity of Riemann's function; he was interested only on its irregularity. Strangely, it was not until fifty years later, in 1970, that Joseph Gerver [Ger1, Ger2] while being a student proved that at these rationals the function is indeed differentiable and the derivative is always $-1/2$. He did it by grouping the frequencies in the formula for $f(a/q + h) - f(a/q)$ according to the different residues modulo q, and estimating the main terms

in the resulting functions. One year after this H. Queffelec [Que] analyzed the differentiability of functions

$$f(x) = \sum_{n=1}^{\infty} \frac{\sin(P(n)x)}{P(n)} \qquad P \in \mathbb{Z}[x]$$

but only at some rationals. In 1972 A. Smith [Smi] simplified Gerver's proof by means of Poisson's summation formula.

In 1978 E. Neuenschwander [Neu] undertook the historical study of the actual knowledge Riemann had about this function. From that account we can say that Riemann probably knew the difference of behaviour at rationals and irrationals. After all, it is natural to understand the formal derivative at a/q

$$\pi \sum_{n=1}^{\infty} \cos(\pi n^2 \frac{a}{q})$$

as $\xi(0)$, where $\xi(s)$ is the meromorphic extension of

$$\xi(s) = \pi \sum_{n=1}^{\infty} \cos(\pi n^2 \frac{a}{q}) n^{-s} \qquad \Re s > 1.$$

Indeed, it can be proved (see theorem 1.14) that the value of the derivative is $\xi(0)$ at the rational points for which the derivative exists, and it exists precisely in the ones for which the function $\xi(s)$ does not have a pole at $s = 1$.

In 1991 J. J. Duistermaat [Dui] showed the precise behaviour of f near the rationals and used this result to study the irregularity at the irrationals and the regularity almost everywhere. He began with the expression

$$f(x) - f(x_0) = \int_C \frac{1}{2}(\theta(z) - 1)dz,$$

where C is any smooth curve contained in the hyperbolic plane that goes from $x_0 \in \mathbb{R}$ to $x \in \mathbb{R}$. From that and (1.1) he got a formula that express the self-similarity of Riemann's function:

$$f(x) = f(\frac{a}{q}) + e^{\frac{i\pi}{4}m} q^{\frac{-1}{2}} (x - \frac{a}{q})^{\frac{1}{2}} - \frac{1}{2}(x - \frac{a}{q}) + e^{\frac{i\pi}{4}m} q^{\frac{3}{2}} (x - \frac{a}{q})^{\frac{3}{2}} f(\gamma(x)) + \psi_{a/q}(x)$$

where $\psi_{a/q}(x)$ is a differentiable function and $\psi_{a/q}(a/q) = 0$. From it he could infer the behaviour of f at the rationals, an taking a/q as the convergents (with a, q of different parity) of the point x_0 obtained

$$f(x) - f(x_0) = \Omega(|x - x_0|^{\frac{1}{2} + \frac{1}{2r}}) \tag{1.2}$$

if x_0 satisfies $|x_0 - a_n/q_n| = O(q_n^{-r})$ where a_n/q_n are its convergents. This last point had implicitly been discovered by Hardy and Littlewood in [HL]. Duistermaat also proved from his formula that

$$f(x) - f(x_0) = O(|x - x_0|^{\frac{3}{4}(1-r(r-2))}), \tag{1.3}$$

for any x_0 satisfying $\liminf_n |x_0 - a_n/q_n| q_n^r > 0$. This was the first time that someone showed the regularity at certain irrational points. In particular (1.2) and (1.3) prove that the Hölder exponent is exactly 3/4 almost everywhere, but when $r > 1 + 2/\sqrt{3}$ this bound does not give any information, because we can directly see that $f \in C^{1/2}(\mathbb{R})$. Hence in some ranges we are losing information.

In 1986 P. G. Lemarié and Y. Meyer [LM] characterized for a function $f : \mathbb{R} \to \mathbb{C}$ to be in the space

$$C^\beta(\mathbb{R}) = \{f : \exists C > 0, |f(x) - f(y)| \leq C|x - y|^\beta \, \forall x, y \in \mathbb{R}\} \qquad 0 < \beta < 1$$

through decay conditions on the coefficients of the function with respect to a wavelets basis. Three years later S. Jaffard [Jaf2] used the same techniques to characterize the local regularity of functions, namely the fact of being in the space

$$C^\beta(x_0) = \{f : \exists P \in \mathbb{C}[x], f(x) - P(x - x_0) = O(|x - x_0|^\beta)\} \qquad \beta > 0$$

for $x_0 \in \mathbb{R}$. In 1991 M. Holschneider and Ph. Tchamitchian [HT] used this characterization for Riemann's function, rediscovering in this way the behaviour at the rationals and the irregularity at the irrationals. But they did not used this characterization to study the behaviour of the function near the rest of the points.

In 1993, F. Chamizo and A. Córdoba [CC1] showed that the graph of the function

$$f_\alpha(x) = \sum_{n=1}^{\infty} \frac{\sin(n^2 x)}{n^\alpha} \qquad 1 < \alpha \leq 2$$

is a fractal set of dimension $9/4 - \alpha/2$. They did so by using the approximate functional equation for θ [HL] and properties of Gauss sums.

In 1996, after having read Duistermaat's paper, Jaffard discovered the regularity at any point of Riemann's function by the use of wavelets. To express correctly her results and our later study we associate to any point x_0 its Hölder exponent

$$\beta_f(x_0) = \sup\{\beta \geq 0 : f \in C^\beta(x_0)\}. \tag{1.4}$$

Jaffard realized that the regularity of any point for Riemann's function only depends on the how this point can be approximated by rationals. Let $(a_n/q_n)_{n\in\mathbb{N}}$ be the convergents of x_0, and define r_n through the formula

$$|x_0 - \frac{a_n}{q_n}| = q_n^{-r_n},$$

then Jaffard considered the spaces

$$E_r = \{x \in \mathbb{R} \setminus \mathbb{Q} : \limsup_n r_n = r\}, \quad 2 \leq r \leq \infty, \tag{1.5}$$

and proved that

$$\beta_f(x_0) = \frac{1}{2} + \frac{1}{2r} \quad \text{if} \quad x_0 \in E_r. \tag{1.6}$$

As

$$\mathbb{R} \setminus \mathbb{Q} = \bigcup_r E_r$$

this gave the Hölder exponent for each point (already known the regularity at any rational). Moreover, since the Hausdorff dimension of E_r is $2/r$ (see [Fal2]), with this she got the spectrum of singularities of the function f, which is defined in general as the function

$$d_{\mathrm{H}}(\beta) = \dim_{\mathrm{H}}\{x \in \mathbb{R} : \beta_f(x) = \beta\}, \tag{1.7}$$

that associates to any β the Hausdorff dimension of the set of points with Hölder exponent equal to β, if it is not the empty set. Whenever $\{x \in \mathbb{R} : \beta_f(x) = \beta\} = \emptyset$ we set $d_{\mathrm{H}}(\beta) = -\infty$. Thus she showed that in the case of Riemann's function

$$d_{\mathrm{H}}(\beta) = \begin{cases} 4\beta - 2 & \text{if } \frac{1}{2} \leq \beta \leq \frac{3}{4}, \\ 0 & \text{if } \beta = \frac{3}{2}, \\ -\infty & \text{otherwise.} \end{cases}$$

In this way we see that f is a multifractal function (the function d_{H} is positive at more than one point) and the irregularity at any point is measured by the approximation of that point by rational numbers.

Once Riemann's function was understood, it was undertaken the study of more general functions. In 1999 Chamizo and Córdoba [CC2] introduced

$$F_{\alpha,k}(x) = \sum_{n=1}^{\infty} \frac{e(n^k x)}{n^\alpha} \qquad k \in \mathbb{N},\ \alpha > 1.$$

We have $F_{\alpha,k} \in C^{(\alpha-1)/k}(\mathbb{R})$, but for most points Hölder exponent is not $(\alpha-1)/k$. For $k > 2$, the function $F_{\alpha,k}$ was not anymore related to an

automorphic form, and that made things more complicated. Through Poisson kernel they were able to characterize the differentiability at any rational point: $F_{k,k}$ is differentiable at a/q, with a and q coprimes, if and only if $\tau(a/q) = 0$ where

$$\tau(\frac{a}{q}) = \sum_{d=1}^{q} e(\frac{ad^k}{q}). \tag{1.8}$$

By studying these sums they were capable of deciding (except for a small set of q) the differentiability at a/q through arithmetical properties of q. They also studied the regularity of the function at other points, by using bounds for the sums

$$\sum_{n \leq N} e(n^k x_0),$$

that came from number theory. These bounds depend on how quickly the convergents of x_0 approach this point. For example, they got

$$\beta(x_0) \geq \frac{\alpha - 1}{k} + 2^{1-k} k^{-1}$$

for any x_0 quadratic irrational. Many other bounds can be deduced from their analysis, as that for any $\epsilon > 0$ there exists a set A_ϵ with positive Hausdorff dimension such that

$$\beta(x_0) \geq \frac{\alpha - 1}{k} + \epsilon$$

for any $x_0 \in A_\epsilon$. In the same paper they generalized their 1993 results about the Minkowski (Box-counting) dimension, by substituting the approximate functional equation by Large Sieve arguments. They demonstrated that

$$\dim_{\mathrm{M}} F_{\alpha,k} = 2 + \frac{1}{2k} - \frac{\alpha}{k} \qquad \frac{k+1}{2} \leq \alpha \leq k + \frac{1}{2}. \tag{1.9}$$

In 2001 F. Chamizo [Cha] noticed that the irregularity of Riemann's function was a general feature of functions

$$\sum_{m=1}^{\infty} m^{-\alpha} a_m e(mx)$$

where $f(z) = \sum_m a_m e(mz)$ is a classical automorphic form. He showed that the behaviour of the function at the cusps changes depending on the related automorphic form being a cusp form, and expressed the derivative through values of L functions attached to f. Moreover he showed that the derivative at any cusp essentially depends on its class under the Fuchsian group attached to the form (for instance, for Riemann's function the derivate at any rational

with odd numerator and denominator equals $-1/2$) . In [MS] S. Miller and W. Schmid generalize part of these results to distributions coming from more general automorphic forms.

Finally, in 2003 Gerver [Ger3] studied the function $F_{\alpha,3}$ near the rationals, proving that $F_{\alpha,3}$ is almost nowhere differentiable for $\alpha < (\sqrt{97}-1)/4 = 2.212\ldots$. He achieved it by using a theorem of Patterson and Heath-Brown about the uniform distribution of the sums $\tau(a/q)$ in the cubic case and also a diophantine approximation result of Erdős.

In this chapter we will generalize part of the knowledge about the function $F_{\alpha,2}$ to the functions $F_{\alpha,k}$, and most results would remain valid for any Fourier series whose frequencies are given by a polynomial and whose coefficients decay monotonically and slower than some polynomial. Part of the stated results in this chapter are contained in [CU2]. To simplify, throughout we will denote

$$F(x) = \sum_{n=1}^{\infty} n^{-\alpha} e(n^k x)$$

whenever there is no danger of confusion.

In the first section we study the sums $\tau(a/q)$ and another related sums that we shall need to control in order to understand the regularity of F.

In the second we shall see in a precise way the behaviour of F very near to the rationals, and in particular we shall deduce the regularity of the function at them through the following result.

Theorem 1.1. *For $1 < \alpha < k+1$, a/q any irreducible fraction and $h > 0$ we have*

$$F(\frac{a}{q}+h) = F(\frac{a}{q}) + Aq^{-1}\tau(\frac{a}{q})h^{\frac{\alpha-1}{k}} + 2\pi i\zeta_{\frac{a}{q}}(\alpha-k)h + T(h^{-\frac{1}{k}})h^{\frac{\alpha-1/2}{k-1}}$$

with A the constant defined in (1.20), T an bounded oscillating function (depending on a, q, α and k) and $\zeta_{a/q}(s)$ the meromorphic continuation of the function defined in $\Re s > 1$ by the formula

$$\sum_{n=1}^{\infty} e(n^k \frac{a}{q}) n^{-s}.$$

From the result of the first section and this theorem we shall infer

Theorem 1.2. *For any rational a/q, a, q coprimes, we have*

$$\beta_F(\frac{a}{q}) = \frac{\alpha-1}{k}$$

if there exists $p^\delta \parallel q$ *such that* $(k, p-1) = 1$ *and* $\delta \equiv 1 \pmod k$. *Otherwise*

$$\beta_F(\frac{a}{q}) = \frac{\alpha - 1/2}{k-1}$$

and F *is differentiable at* a/q *if and only if* $\alpha > k - 1/2$, *with*

$$F'(a/q) = 2\pi i \zeta_{a/q}(\alpha - k).$$

The regularity of the function at the irrationals can be controlled by studying its behaviour near its convergents. This amounts to understand the function T, which depends on sums of the shape

$$S_M(\frac{a}{q}) = \sum_{m \le M} \sum_{d=1}^{q} e(\frac{ad^k + md}{q}),$$

that will be our subject of study in the third section. We shall demonstrate that these sums are bounded by $(Mq)^{1/2+\epsilon}$ uniformly in $M \le q$ for most of a. The precise result (see proposition 1.22) is

$$\frac{1}{q} \sum_{a=1}^{q} \sup_{M \le N} |S_M(\frac{a}{q})|^2 \ll (Nq)^{1+\epsilon} \qquad \epsilon > 0, \tag{1.10}$$

a particular discrete version of the Kolmogorov-Plessner-Seliverstov theorem (see [Zyg]) for Fourier Series in L^2.

In the fourth section we shall expose the local regularity characterization in terms of the continuous wavelet transform and use it to see the relation between the regularity of the functions $F_{\alpha,k}$: for each $x_0 \in \mathbb{R}$ the function

$$\beta_{F_{\alpha,k}}(x_0) - \frac{\alpha}{k} \tag{1.11}$$

increases in α. Besides, we shall give a characterization of the Minkowski dimension of the graph of a continuous function in terms of its continuous wavelet transform. Finally we enlarge the range of validity of the formula (1.9) to

$$\dim_{\mathrm{M}} F = 2 + \frac{1}{2k} - \frac{\alpha}{k} \qquad \frac{k+2}{4} \le \alpha \le k + \frac{1}{2}. \tag{1.12}$$

In the last section we use the results of previous sections in order to study the regularity at the irrationals. First we obtain a uniform result: for any $r \ge 2$ and every point $x \in E_r$ we have (for $\alpha < k-1$ in the case of the upper bound)

$$\frac{\alpha - 1}{k} + 2^{1-k} \min(\frac{1}{k}, \frac{1}{2(r-1)}) \le \beta_F(x) \le \frac{\alpha}{k-1}.$$

After this we shall see the regularity of F in E_r almost everywhere:

Theorem 1.3. *For any $r \geq 2$:*

i) Almost everywhere in E_r (with Hausdorff $\mathcal{H}^{2/r}$ measure) we have

$$\beta_F(x) \geq \min\big(\frac{\alpha-1/2}{k}, \frac{\alpha-1}{k}+\frac{1}{2r}\big).$$

ii) Suppose $r \geq k$. Then there exists a subset $E_{r,0}$ of E_r with positive measure such that for any $x \in E_{r,0}$ we have

$$\beta_F(x) \geq \frac{\alpha-1/2}{k}. \tag{1.13}$$

iii) Suppose $r \geq k$. Then there exists a subset $E_{r,1}$ of E_r with positive measure such that for any $x \in E_{r,1}$ we have

$$\beta_F(x) = \frac{\alpha-1}{k}+\frac{1}{2r}. \tag{1.14}$$

This result is a generalization of what can be obtained by the Fundamental Theorem of Calculus for $r = 2$ and $\alpha > k + 1/2$, and proves also that F is a multifractal function. But we shall see that the regularity at any point, in contrast with the case $k = 2$, not only depends of the convergents' approach speed but above all on what kind of numbers are these convergents. The rationals whose denominators are k-powers represent the extreme case, giving

Theorem 1.4. *For any $r \geq 2$, there exists $D_r \subset E_r$ such that*

$$\beta_F(x) = \frac{\alpha-1}{k}+\frac{1}{kr} \qquad \textit{for every} \quad x \in D_r$$

with

$$1+\frac{1}{2k} \leq \dim_{\mathrm{H}} D_r \leq 1+\frac{1}{k}.$$

This theorem offers a lower bound for the spectrum of singularities

$$d_{\mathrm{H}}(\beta) \geq k(1+\frac{1}{2k})(\beta-\frac{\alpha-1}{k}) \qquad \beta \in (\frac{\alpha-1}{k}, \frac{\alpha-1/2}{k}).$$

If we could prove that actually $\dim_{\mathrm{H}} D_r = (1+k^{-1})/r$ (we have $\dim_{\mathrm{M}} D_r = (1+k^{-1})/r$) that bound would improve to

$$d_{\mathrm{H}}(\beta) \geq k(1+\frac{1}{k})(\beta-\frac{\alpha-1}{k}) \qquad \beta \in (\frac{\alpha-1}{k}, \frac{\alpha-1/2}{k}),$$

what corresponds to what we expect for the function F in that range.

Moreover for the points x at which we have proved that $\beta_F(x) > 1$ we have

$$F'(x) = \lim_{n\to\infty} \zeta_{a_n/q_n}(\alpha-k),$$

where the limit is over the convergents of x.

1.2 Complete sums

We shall see that in the study of the regularity of the function F play an important role the trigonometric sums

$$\tau_m(\frac{a}{q}) = \sum_{d=1}^{q} e(\frac{ad^k + md}{q}) \qquad (a,q) = 1,\ m \in \mathbb{Z}.$$

The special case $\tau_0 = \tau$ is the sum considered in the introduction. We are going to begin explaining some known results (see [Vau]) for these sums. In some places we shall assume that $k \geq 3$, that are the cases in which we are interested.

Lemma 1.5. *Suppose q_1, q_2 are coprime natural numbers. Then*

$$\tau_m(\frac{a}{q_1 q_2}) = \tau_m(\frac{aq_2^{k-1}}{q_1})\tau_m(\frac{aq_1^{k-1}}{q_2}).$$

Proof: By Euclid's algorithm, every integer u with $1 \leq u \leq q$ can be written in a unique way as

$$u = Aq_1 + Bq_2 \qquad 1 \leq A \leq q_2,\ 1 \leq B \leq q_1.$$

In this way, the Lemma follows from the identity

$$e(\frac{au^k + mu}{q_1 q_2}) = e(\frac{aq_2^{k-1}B^k + mB}{q_1})e(\frac{aq_1^{k-1}A^k + mA}{q_2}).$$

□

The sum τ behaves in a special way when q is prime.

Lemma 1.6. *Suppose q is a prime number. Then*

$$\tau(\frac{a}{q}) = \sum_{\chi \in G} \overline{\chi}(a)\tau_\chi. \tag{1.15}$$

where G is the group of Dirichlet characters whose order divide $(k, q-1)$ and τ_χ the Gauss sum

$$\tau_\chi = \sum_{d=1}^{q} \chi(d)e(\frac{d}{q}).$$

Since $|\tau_\chi| \leq q^{1/2}$, then

$$|\tau(a/q)| \leq kq^{\frac{1}{2}}.$$

Proof: We have

$$|\{1 \le n \le q : n^k = m\}| = \sum_{\chi \in G} \chi(m).$$

Therefore

$$\tau(\frac{a}{q}) = \sum_m (\sum_{\chi \in G} \chi(m)) e(\frac{am}{q}) = \sum_{\chi \in G} \sum_{m=1}^{q} \chi(m) e(\frac{am}{q}).$$

Taking into account the bijection $x \mapsto a^{-1}x$ from $\mathbb{F}_q$ to $\mathbb{F}_q$ we get (1.15). Moreover for non-principal character χ we have

$$|\tau_\chi|^2 = \sum_{1 \le d,j \le q-1} \chi(d)\overline{\chi(j)} e(\frac{d-j}{q})$$

and making the change $d \mapsto jd$ we arrive at

$$|\tau_\chi|^2 = \sum_{1 \le d \le q-1} \chi(d) \sum_{1 \le j \le q-1} e(\frac{(d-1)j}{q}) = q.$$

□

If q is a sufficiently high power then the sum $\tau(a/q)$ behaves regularly. In a precise way, we have the following

Lemma 1.7. *Let $q = p^d$, p prime, $p^\delta \parallel k$ and*

$$d \ge \begin{cases} 2 & \text{if } \delta = 0 \\ \delta + 2 & \text{if } \delta > 0,\ p > 2 \\ \delta + 3 & \text{if } \delta > 0,\ p = 2. \end{cases}$$

Then

$$\tau(a/p^d) = \begin{cases} p^{d-1} & \text{if } d \le k \\ p^{k-1}\tau(a/p^{d-k}) & \text{if } d > k. \end{cases}$$

Proof: Every residue modulo p^d can be represented in a unique way as

$$bp^{d-\delta-1} + c \qquad \text{with} \qquad 1 \le b \le p^{\delta+1}, \qquad 1 \le c \le p^{d-\delta-1}.$$

Besides, we have

$$(bp^{d-\delta-1} + c)^k \equiv c^k + kc^{k-1}bp^{d-\delta-1} \pmod{p^d}$$

if d satisfies the hypothesis of the Lemma. Hence

$$\tau(\frac{a}{q}) = \sum_{c=1}^{p^{d-\delta-1}} e(\frac{ac^k}{p^d}) \sum_{b=1}^{p^{\delta+1}} e(\frac{ak}{p^\delta}\frac{c^{k-1}b}{p}) = p^{\delta+1} \sum_{\lambda=1}^{p^{d-\delta-2}} e(a\frac{p^k}{p^d}\lambda^k)$$

which proves the result noticing that $\delta + 2 \leq k$. □

These results give us an optimal upper bound for $\tau(a/q)$.

Lemma 1.8. *We have*

$$\tau(\frac{a}{q}) \ll q^{1-\frac{1}{k}}.$$

for any a coprime to q.

Proof: By the Lemma 1.5 we can write

$$\tau(\frac{a}{q}) = \tau(\frac{aq_2^{k-1}}{q_1})\tau(\frac{aq_1^{k-1}}{q_2})$$

being q_1 the product of the primes dividing q with exponent greater than one and also dividing k. By the Lemmata 1.6 and 1.7 we deduce that

$$\tau(\frac{aq_1^{k-1}}{q_2}) \ll q_2^{1-\frac{1}{k}}$$

and also

$$\tau(\frac{aq_2^{k-1}}{q_1}) \leq k^2 q_1^{1-\frac{1}{k}}.$$

□

Now, by using the previous Lemmata we are going to study for which values a and q the sum $\tau(a/q)$ vanishes. This proposition completes Lemmata 4.6 and 4.7 in [CC2]:

Proposition 1.9. *$\tau(a/q) = 0$ if and only if there exists p prime such that $p^\delta \parallel q$ with $(k, p-1) = 1$ and $\delta \equiv 1 \pmod k$.*

Proof: By Lemma 1.5 we can write

$$\tau(\frac{a}{q}) = \prod_{p^d \| q} \tau(\frac{a_p}{p^d})$$

with $(a_p, p) = 1$. Thus we reduce the proof of the proposition to the case $q = p^d$. Besides, by Lemma 1.7 we only need to consider the case $1 \leq d \leq k$, since $k \geq \delta + 2$.

If $d = 1$, as $e(a/p)$ is the root of the irreducible polynomial $x^{p-1} + x^{p-2} + \ldots + 1$ the unique possibility for $\tau(a/p)$ to be zero is that the homomorphism

$$\mathbb{F}_p \to \mathbb{F}_p$$

$$n \mapsto n^k$$

will be also automorphism, an this happen only if $(k, p-1) = 1$.

If $1 < d \leq k$ and $\tau(a/p^d) = 0$ for some a, p coprime integers, by using the automorphisms of the Galois group of $\mathbb{Q}(e(1/p^d))$ we deduce that

$$\tau(a/p^d) = 0 \qquad \text{for every } a, (a,p) = 1.$$

On the other hand

$$\sum_{(a,p)=1} \tau(\frac{a}{p^d}) = \sum_{n=1}^{p^d} \sum_{(a,p)=1} e(\frac{n^k a}{p^d}) = p^{2d-2},$$

contradiction. Hence $\tau(a/p^d) \neq 0$ whenever $1 < d \leq k$. $\square$

Let us see some special cases in which τ_m is very simple:

Lemma 1.10. *Suppose p is a prime not dividing k and a an integer coprime to p. Suppose also that $j, d \in \mathbb{Z}$, $j \geq 0$, $1 \leq d \leq k$ and $p^{j(k-1)+d-1} \mid m$. Then*

$$\tau_m(\frac{a}{p^{jk+d}}) = p^{j(k-1)+d-1}.$$

Proof:

$$\tau_m(\frac{a}{p^{jk+d}}) = \sum_{u=1}^{p^{jk+d}} e(\frac{au^k + mu}{p^{jk+d}})$$

We can represent each residue modulo p^{jk+d} as

$$u = Ap^{jk+d-1} + B \qquad 1 \leq A \leq p,\ 1 \leq B \leq p^{jk+d-1}$$

hence

$$\begin{aligned} \tau_m(\frac{a}{p^{jk+d}}) &= \sum_B e(\frac{mB}{p^{jk+d}}) e(\frac{aB^k}{p^{jk+d}}) \sum_A e(\frac{kB^{k-1}A}{p}) \\ &= p \sum_{C=1}^{p^{jk+d-2}} e(\frac{mC}{p^{jk+d-1}}) e(\frac{ap^k C^k}{p^{jk+d}}). \end{aligned}$$

If $j = 0$ this equals p^{d-1}, and if $j > 0$ equals

$$p^{k-1}\tau_{mp^{-k+1}}(\frac{a}{p^{(j-1)k+d}}).$$

This allows us to prove the Lemma by induction. □

For our subsequent study, in the third section, of the sums $\sum_{m\leq M}\tau_m$ we need to handle a special double sum.

Lemma 1.11. *Let $n \in \mathbb{N}$ and*

$$\varrho_n(q) = \sum_{m=1}^{q} |\sum_{a=1}^{q} \tau_n(\frac{a}{q})\overline{\tau_m(\frac{a}{q})}|.$$

The function ϱ_n is multiplicative. Moreover, let $q = p^v$ with p a prime not dividing k and $v = jk + d$ for some positive $j \in \mathbb{Z}$, $1 \leq d \leq k$. We have

$$\varrho_n(p^v) = \begin{cases} 2(k, p-1)(p^{2v} - p^{2v-j-1}) & \text{if } p^{v-j-1} \nmid n \\ 2(k, p-1)(p^{2v} - p^{2v-j-1}) + p^{3v-j-1} & \text{otherwise.} \end{cases}$$

Proof: By Lemma 1.5 we see that

$$\varrho_n(q) = \sum_{m=1}^{q}\prod_{p^v\|q} |\sum_{a=1}^{p^v} \tau_n(\frac{a}{p^v})\overline{\tau_m(\frac{a}{p^v})}| = \prod_{p^v\|q}\big(\sum_{m=1}^{p^v} |\sum_{a=1}^{p^v} \tau_n(\frac{a}{p^v})\overline{\tau_m(\frac{a}{p^v})}|\big),$$

which proves the multiplicativity of ϱ_n. On the other hand

$$\varrho_n(q) = q\sum_{m=1}^{q} |\sum_{\substack{1\leq c,d\leq q \\ c^k\equiv d^k \pmod q}} e(\frac{nc-md}{q})|.$$

If $q = p^v$ we divide the sum into two parts $\varrho_n(p^v) = S_1 + S_2$ where

$$\begin{aligned} S_1 &= p^v \sum_{\Omega^k\equiv 1 \pmod{p^v}} \sum_{m=1}^{p^v} |\sum_{\substack{1\leq c\leq p^v \\ (c,p)=1}} e(\frac{(n-\Omega m)c}{p^v})| \\ &= p^v(k, p-1)\sum_{N=1}^{p^v} |\sum_{\substack{1\leq c\leq p^v \\ (c,p)=1}} e(\frac{Nc}{p^v})| \\ &= p^v(k, p-1)(\phi(p^v) + (p-1)\frac{\phi(p^{jk+d})}{p-1}) \\ &= 2(k, p-1)\phi(p^v)p^v \end{aligned}$$

and

$$S_2 = p^v \sum_{m=1}^{p^v} | \sum_{\substack{1\le c,d\le p^{v-1} \\ c^k\equiv d^k \pmod{p^{v-k}}}} e(\frac{nc-md}{p^{v-1}})|.$$

Repeating this process j times, we arrive at

$$\tau_n(p^v) = p^v\big[2(k,p-1)\big(\sum_{i=0}^{j}\phi(p^{v-i})\big) + \sum_{m=1}^{p^v}|\sum_{1\le c,d\le p^{v-j-1}} e(\frac{nc-md}{p^{v-j-1}})|\big],$$

and this gives the result. □

1.3 Regularity at the rationals

We are going to see that Poisson summation formula allows us to understand quite well $F(x)$ whenever

$$|x-\frac{a}{q}| < q^{-k},$$

for some rational a/q, and helps us in order to understand the behaviour of F in the range $|x-a/q| < q^{-1-\epsilon}$, $\epsilon > 0$. By applying it there will appear the sums τ_m studied in the previous section, as well as the zeta function defined by

$$\zeta_{a/q}(s) = \sum_{n=1}^{\infty} e(\frac{a}{q}n^k)n^{-s} \tag{1.16}$$

in the half plane $\Re s > 1$. By splitting it into the different residues modulo q and using Poisson formula in arithmetic progressions we can write

$$\zeta_{a/q}(s) = \frac{\tau}{q}(\int_0^1 \phi(x)x^{-s} + \frac{1}{s-1}) + \sum_{m\neq 0}\frac{\tau_m}{q}\int_0^\infty \phi(x)x^{-s}e(-\frac{m}{q}x)dx \tag{1.17}$$

where ϕ is any function in $C_0^\infty((0,\infty])$ which takes the value 1 inside the interval $[1,\infty]$, and inner integrals are understood as oscillatory integrals (see [Hör]). Moreover this representation holds for every $s\in\mathbb{C}$, providing the meromorphic continuation of $\zeta_{a/q}(s)$. We see that $\zeta_{a/q}$ has a pole at $s=1$ precisely when $\tau(a/q)\neq 0$.

After applying Poisson formula to the function F near the rational point a/q we shall have to deal with the Fourier transform of the distribution (see [Hör])

$$g(x) = \frac{e(x^k)-1-2\pi i x^k}{x^\alpha}\,\mathbb{I}_{(0,\infty)}(x).$$

So we proceed to study it in the following

Lemma 1.12. *There exists a sequence $(c_j)_{j=0}^{\infty}$ of complex numbers depending on α and k such that for $\lambda > 1$ and $n \in \mathbb{N}$ we have*

$$\widehat{g}(\lambda) = \lambda^{\alpha-1} \sum_{j=2}^{n} a_j \lambda^{-jk} + i^{1/2} \lambda^{-\frac{1}{2}-\frac{\alpha-1/2}{k-1}} e(-C\lambda^{\frac{k}{k-1}}) \sum_{j=0}^{n} c_j \lambda^{-j\frac{k}{k-1}} + O_n(\lambda^{\alpha-n-1})$$

with $C = (1-1/k)k^{-1/(k-1)}$ and

$$a_j = \Gamma(jk - \alpha + 1)(2\pi i)^{\alpha-1+(1-k)j}(j!)^{-1}.$$

Moreover

$$\widehat{g}(-\lambda) = \lambda^{\alpha-1} \sum_{j=2}^{n} \overline{a_j} \lambda^{-jk} + O(\lambda^{\alpha-n}).$$

Proof: We divide the integral into two parts

$$\widehat{g}(\lambda) = I(\psi) + I(\eta),$$

where $\psi \in C_0^{\infty}([0,\infty))$, $\psi(x) = 1$ for $0 \le x \le 1$, $\eta = 1 - \psi$ and $I(f) = \widehat{gf}(\lambda)$. Expanding $u^{\alpha} g(u)$ in power series we have

$$I(\psi) = \sum_{j=2}^{n} \frac{(2\pi i)^j}{j!} I_{kj-\alpha}(\psi) + \int_0^{\infty} u^{n+1-\alpha} g_n(u) \psi(u) e(-\lambda u) du,$$

where $g_n(u)$ is an entire function and

$$I_{\beta}(\psi) = \int_0^{\infty} x^{\beta} \psi(x) e(-\lambda x) dx = (2\pi\lambda)^{-\beta-1} \int_0^{\infty} x^{\beta} e^{-ix} dx - I_{\beta}(\eta).$$

Integrating by parts we see that $I_{\beta}(\eta) \ll_{\beta,n} \lambda^{-n}$. By Cauchy's theorem and the definition of the Γ function we can calculate the first integral, obtaining

$$I_{\beta}(\psi) = (2\pi i\lambda)^{-\beta-1}\Gamma(\beta+1) + O(\lambda^{-n}).$$

Finally integrating by parts $n + 1 - [\alpha]$ times we get

$$\int_0^{\infty} u^{n+1-\alpha} g_n(u) \psi(u) e(-\lambda u) du \ll \lambda^{\alpha-n-1}.$$

On the other hand, another time integrating by parts

$$I(\eta) = \int_0^{\infty} \eta(x) x^{-\alpha} e(x^k - \lambda x) dx + O(\lambda^{-n}).$$

Making the change $x \to \lambda^{1/(k-1)}x$ we arrive at

$$I(\eta) = \lambda^{-\frac{\alpha-1}{k-1}} \int u(x) e(\lambda^{\frac{k}{k-1}}(x^k - x))dx + O(\lambda^{-n})$$

with $u(x) = \eta(\lambda^{1/(k-1)}x)x^{-\alpha}$. Writing u as a sum of three functions of $C_0^\infty((0,\infty))$ it is clear that we can substitute u in the integral by a function $u_0 \in C_0^\infty((0,\infty))$ with support contained in the interval $(1/2k, 2)$ and $u_0 = u$ inside $(1/k, 1)$, and in such a way that the change in the integral is $O(\lambda^{-n})$. Now, applying stationary phase (see Theorem 7.7.5 in [Hör]) we have

$$I(\eta) = \lambda^{-\frac{\alpha-1}{k-1}} \frac{e(-C\lambda^{\frac{k}{k-1}})}{(-ik^2C\lambda^{\frac{k}{k-1}})^{1/2}} \sum_{j\le n} \widetilde{c_j}(\lambda^{\frac{k}{k-1}})^{-j} + O(\lambda^{-n-1})$$

where $C = (1-1/k)k^{-1/(k-1)}$ and $\widetilde{c_j}$ are real numbers only depending on α and k. In particular $\widetilde{c_0} = u(k^{-1/(k-1)}) = k^{\alpha/(k-1)}$.

In the same way we calculate $\widehat{g}(-\lambda)$, taking into account that in this case $\widehat{g\eta}(-\lambda) \ll \lambda^{-n}$, due to the non-vanishing of the derivative of $x^k - (-\lambda)x$ in $[0,\infty)$.

□

When using this result in the proof of the following Lemma we shall need to know that a certain sum converges. This will be assured by the inequality

$$\sum_{m\le N} e(b(m+\theta)^{\frac{k}{k-1}}) \ll b^{\frac{1}{2}} N^{\frac{1}{2}+\frac{1}{2(k-1)}} \tag{1.18}$$

uniform in $0 \le \theta \le 1$ and $b \ge 1$, which is deduced from van der Corput's lemma (see [GK]). Now we are going to see two results concerning the behaviour of $F(a/q+h) - F(a/q)$ for $h > 0$. We get the equivalent ones for $h < 0$ through the formula

$$F(a/q+h) - F(a/q) = \overline{F(-a/q-h) - F(-a/q)}. \tag{1.19}$$

Proposition 1.13. *Let $x \in \mathbb{R}$. For any pair of coprime integer a, q we have*

$$F(x) = F(\frac{a}{q}) + 2\pi i\zeta_{\frac{a}{q}}(\alpha-k)h + A\frac{\tau}{q}h^{\frac{\alpha-1}{k}} + h^{\frac{\alpha-1}{k}} \sum_{m\neq 0} \frac{\tau_m}{q}\, \widehat{g}\big(\frac{m}{qh^{1/k}}\big)$$

where $h = x - a/q > 0$ and

$$A = \big(\frac{i}{2\pi}\big)^{\frac{1-\alpha}{k}} \frac{1}{k}\Gamma(\frac{1-\alpha}{k}). \tag{1.20}$$

Proof: Let $\phi \in C_0^\infty((0,\infty])$ with $\phi = 1$ in $[1,\infty)$. We write

$$F(x) - F(\frac{a}{q}) = \lim_{N\to\infty} S_N$$

$$S_N = \sum_{n\in\mathbb{Z}} \phi_N(n) e(\frac{an^k}{q}) \frac{e(n^k h) - 1}{n^\alpha}.$$

with $\phi_N \in C_0^\infty((0,\infty))$, $\phi_N(t) = \phi(t)$ if $0 < t < N$ and $\phi_N^{(j)}(t) \ll N^{-j}$ for $j \in \mathbb{N}$ and $t \geq N$. Applying Poisson formula in arithmetic progressions

$$S_N = \sum_{m\in\mathbb{Z}} \frac{\tau_m}{q} \int_0^\infty \phi_N(t) t^{-\alpha} (e(ht^k) - 1) e(-\frac{m}{q}t) dt$$

which we can express as

$$S_N = D_N + \frac{\tau}{q} \int_0^\infty \phi_N(t) \frac{e(ht^k) - 1}{t^\alpha} + \sum_{m\neq 0} h^{\frac{\alpha-1}{k}} \frac{\tau_m}{q} \int_0^\infty \phi_N(h^{-\frac{1}{k}}t) g(t) e(-\frac{m}{qh^{1/k}}t) dt$$

where

$$D_N = 2\pi i h \sum_{m\neq 0} \frac{\tau_m}{q} \int \phi_N(t) t^{k-\alpha} e(-\frac{m}{q}t) dt.$$

Lemma 1.12 and (1.18) allow to take the limit $N \to +\infty$. Appealing to (1.17) we obtain

$$\lim_N D_N = 2\pi i h \zeta_{\frac{a}{q}}(\alpha - k) - 2\pi i h \frac{\tau}{q} (\frac{1}{\alpha - k - 1} + \int_0^1 \phi(t) t^{k-\alpha} dt).$$

Finally, for $\phi \to 1$ and considering that

$$\int_0^\infty t^{-\alpha} (e(t^k) - 1) dt = A$$

the result is proven. □

The following theorem is a direct consequence of the two previous results (taking into account (1.18)).

Theorem 1.14. *Let $x \in \mathbb{R}$, $a, q \in \mathbb{Z}$ coprimes, $1 < \alpha < k+1$. If $h = x - a/q$, then for $0 < h < q^{-k}$ and $n > \alpha$*

$$F(x) = F(\frac{a}{q}) + h^{\frac{\alpha-1}{k}} \frac{A\tau}{q} + \sum_{j=1}^{n} (2\pi i h)^j \zeta_{\frac{a}{q}}(\alpha - kj) + (qh)^\beta \sum_{j=0}^{n} c_j T_j(qh^{\frac{1}{k}}) + O((qh^{\frac{1}{k}})^n)$$

with

$$T_j(y) = y^{\frac{jk}{k-1}} \sum_{m=1}^{\infty} \frac{\tau_m}{q^{1/2}}\, e((my^{-1})^{\frac{k}{k-1}}) m^{-\frac{1}{2}-\beta-j\frac{k}{k-1}}$$

and

$$\beta = (\alpha - 1/2)/(k-1).$$

This theorem permits to measure the regularity of the function at any rational.

Corollary 1.15. *Let α, k and a/q as in the previous theorem. Then:*

i) If $\tau \neq 0$ then $F \in C^{\frac{\alpha-1}{k}}(a/q)$ and $F \notin C^{\delta}(a/q)$ for $\delta > (\alpha-1)/k$.

ii) If $\tau = 0$ then $F \in C^{\frac{\alpha-1/2}{k-1}}(a/q)$ and $F \notin C^{\delta}(a/q)$ for $\delta > \frac{\alpha-1/2}{k-1}$.

iii) F is differentiable at a/q if and only if $\tau = 0$ and $\alpha > k - 1/2$. In this case

$$F'(\frac{a}{q}) = 2\pi i \zeta_{\frac{a}{q}}(\alpha - k).$$

Proof: By 1.14 we only have to demonstrate that F is not differentiable at a/q when $\alpha = k - 1/2$, $\tau = 0$. This is due to the fact that T_0 oscillates. In order to prove it, we take $m_0 \neq 0$ such that $\tau_{m_0} \neq 0$ (it is always possible because $\sum_{m=0}^{q} \tau_m = q$). Then

$$\int_{Y}^{2Y} T_0(y^{-1}) e(C(m_0 y)^{\frac{k}{k-1}}) dy = q^{-\frac{1}{2}} \tau_{m_0} m_0^{-\frac{1}{2}-\beta} Y + O(1).$$

Hence $\lim_{y\to\infty} T(y^{-1})$ does not exist. □

We see that the smoothness of the function at a/q depends on the vanishing of the sum $\tau(a/q)$. This vanishing can be fully characterized in terms of arithmetical properties of q. By the previous corollary and Proposition 1.9 we conclude:

Theorem 1.16. *For any rational a/q, a, q coprime integers, we have*

$$\beta_F(x_0) = \frac{\alpha - 1}{k}$$

if there exists a prime p such that $p^{\delta} \parallel q$, $(k, p-1) = 1$ and $\delta \equiv 1 \pmod{k}$. Otherwise

$$\beta_F(x_0) = \frac{\alpha - 1/2}{k-1}.$$

As in Proposition 1.13, but in a simpler way, the following result can be proved.

Proposition 1.17. *Let $h = x - a/q > 0$ and $1 < \alpha < k$. Then*

$$F(x) = F(\frac{a}{q}) + A\frac{\tau}{q}h^{\frac{\alpha-1}{k}} + q^{-1}h^{\frac{\alpha-1}{k}}\sum_{m\neq 0}\tau_m\widehat{g}_0(\frac{m}{h^{1/k}q})$$

where $g_0(x) = x^{-\alpha}(e(x^k) - 1)$.

Let us see that whenever h is small with respect to q^{-1}, actually the term $Aq^{-1}h^{(\alpha-1)/k}$ is the main one in $F(a/q + h) - F(a/q)$.

Proposition 1.18. *Let $k/2 < \alpha < k$ and $h > 0$. Then*

$$F(x) - F(\frac{a}{q}) = \frac{A\tau}{q}h^{\frac{\alpha-1}{k}} + O(h^{\frac{\alpha}{k}}q^{\frac{1}{2}+\epsilon})$$

for any $\epsilon > 0$.

Proof: By Lemma 1.12 we get $\widehat{g}_0(\lambda) \ll \lambda^{-\delta}$ with $\delta > 1$, and applying Proposition 1.13 we arrive at

$$F(x) - F(\frac{a}{q}) = \frac{A\tau}{q}h^{\frac{\alpha-1}{k}} + \frac{h^{\frac{\alpha-1}{k}}}{q}O(\sum_{m\neq 0}|\tau_m|\min(1, (\frac{|m|}{h^{1/k}q})^{-\delta}))$$

From Riemann hypothesis for curves over finite fields it can be deduced (see [Vau]) the bound

$$\tau_m \ll (m, q)q^{\frac{1}{2}+\epsilon},$$

for any $\epsilon > 0$, whence the proposition follows. □

From this proposition we could proved Jaffard's result regarding the regularity of the function F in the case $k = 2$ (see (1.6)). However it is not true anymore for any $k \geq 3$. In this case is not enough to bound the sum $\sum_{m\leq M}\tau_m$ by controlling the size of τ_m. In the following section we are going to prove hat in that sum there is a lot of cancelation, at least for most of the rationals a/q.

1.4 Incomplete sums

As we have just seen, the term $\tau(a/q)$ determines in part the behaviour of the function F. Whenever q is prime, this sum behaves in a complicated way. We are going to show that for most of the residues a the size of $\tau(a/q)$ is near $q^{1/2}$ except in the case $(k, q-1) = 1$, in which τ vanishes.

Proposition 1.19. *Let $1 \leq N \leq q$, q prime and $l = (k, q-1) > 1$. Then*

$$\sum_{a \leq N} |\tau(\frac{a}{q})|^2 = l(q-1)N + O(l^2 q^{3/2} \log q).$$

Proof: We start completing the sum:

$$\begin{aligned} \sum_{a \leq N} |\tau(\frac{a}{q})|^2 &= \sum_{a=1}^{q} |\tau(\frac{a}{q})|^2 \sum_{s \leq N} \frac{1}{q} \sum_{r=1}^{q} e(\frac{(a-s)r}{q}) \\ &= \frac{1}{q} \sum_{r=1}^{q} \sum_{s \leq N} e(\frac{-sr}{q}) \sum_{a=1}^{q} e(\frac{ra}{q}) |\tau(\frac{a}{q})|^2. \end{aligned}$$

By using (1.15) follows that

$$\sum_{a=1}^{q} |\tau(\frac{a}{q})|^2 = \sum_{\chi, \psi \in G} \tau_\chi \overline{\tau_\psi} \sum_{a=1}^{q} \overline{\chi(a)} \psi(a) = q(q-1)l$$

and for any $r \neq q$

$$\begin{aligned} \sum_{a=1}^{q} e(\frac{ra}{q}) |\tau(\frac{a}{q})|^2 &= \sum_{\chi, \psi \in G} \tau_\chi \overline{\tau_\psi} \sum_{a=1}^{q} \overline{\chi(a)} \psi(a) e(\frac{ra}{q}) \\ &= \sum_{\chi, \psi \in G} \chi(r) \overline{\psi(r)} \tau_\chi \overline{\tau_\psi} \tau_{\overline{\chi}\psi} \end{aligned}$$

Therefore

$$\begin{aligned} |\sum_{a \leq N} |\tau(\frac{a}{q})|^2 - N(q-1)l| &\leq l^2 q^{1/2} \sum_{r=1}^{q-1} |\sum_{s \leq N} e(\frac{-sr}{q})| \\ &\leq l^2 q^{1/2} \sum_{r=1}^{q-1} |\sin(\pi \frac{r}{q})|^{-1} \end{aligned}$$

and the result follows from the equivalence $\sin x \sim x$. $\square$

As an outcome of this proposition and Lemma 1.6 we have the following

Proposition 1.20. *Let $I \subset \mathbb{R}$ be a closed interval with $|I| < 1$. For any $\epsilon > 0$ there exists $C = C(\epsilon, k) > 0$ such that for every prime $q > C|I|^{-2-\epsilon}$ holding $(q-1, k) \neq 1$ we have*

$$|\{1 \leq a \leq q : \frac{a}{q} \in I, |\tau(\frac{a}{q})| \geq \frac{q^{1/2}}{2}\}| \geq \frac{q}{2k^2} |I|.$$

We have already understood (see 1.17) that the sums $\sum_m \tau_m f(m/Y)$ have a great importance in order to understand the irregularity of the function F. We are going to see that in that sums there is much cancelation for most of the residues a. In the proof of this fact we shall use a Large Sieve-Type inequality, widely used in number theory. It is a generalization of Bessel's inequality (see [Dav2])

Lemma 1.21. *Let u a vector in an euclidean space. For any set of l vectors $v_1, v_2, \dots, v_l$ in this space we have the inequality*

$$\sum_{i=1}^{l} |\langle u, v_i\rangle|^2 \leq \left(\max_{1\leq i\leq l} \sum_{j\leq l} |\langle v_i, v_j\rangle| \right) \|u\|^2.$$

We proceed to prove the main result of this section.

Proposition 1.22. *Let $f : [0,\infty] \to \mathbb{C}$ continuous function such that its Mellin transform is in L^1 and represents f through the inversion formula in the line $\Re s = 1/2$. Defining*

$$S^*_{a/q}(x) = \sup_{Y\in[x,2x]} |\sum_{m=1}^{q} \tau_m(\frac{a}{q}) f(\frac{m}{Y})|$$

we have

$$\frac{1}{q}\sum_{a=1}^{q} |S^*_{a/q}(x)|^2 \ll xqk^{\omega(q)}d(q)^2 \log q.$$

Proof: We write

$$\sum_{m=1}^{q} \tau_m(\frac{a}{q}) f(\frac{m}{Y}) = \sum_{q_0|q} \sum_{\substack{m=1 \\ (m,q)=q_0}}^{q} \tau_m(\frac{a}{q}) f(\frac{m}{Y})$$

and by Cauchy's inequality

$$\sum_{a=1}^{q} |S^*_{a/q}(x)|^2 \leq d(q)^2 \max_{q_0|q} \sum_{a=1}^{q} |S^*_{a/q}(x,q_0)|^2$$

with

$$S^*_{a/q}(x,q_0) = \sup_{Y\in[x,2x]} |\sum_{\substack{m=1 \\ (m,q)=q_0}}^{q} \tau_m(\frac{a}{q}) f(\frac{m}{Y})|.$$

Let

$$B = \bigcup_{d=1}^{k} \bigcup_{j=0}^{\infty} \{(jk+d, n) \in \mathbb{N}^2 : n \geq jk + d - j - 1\},$$

and A its complementary set in $\mathbb{N}^2$. Let $q_0 = q_A q_B q_C$ and $q = q_0 l_A l_B l_C$, with $q_C l_C \mid k$, $(q_A l_A, q_B l_B) = (q_A l_A, k) = (q_B l_B, k) = 1$, with $q_A l_A = \prod_p p^{v_p}$, $q_A = \prod_p p^{u_p}$ with $(v_p, u_p) \in A$ for any $p \mid q_A l_A$ y $q_B l_B = \prod_p p^{m_p}$, $q_B = \prod_p p^{n_p}$ with $(m_p, n_p) \in B$ for every $p \mid q_B l_B$.

Then

$$\tau_m(\frac{a}{q}) = \tau_m(\frac{a(q_B l_B)^{k-1}}{\Delta})\tau_m(\frac{a\Delta^{k-1}}{q_B l_B}) = \tau_m(\frac{a(q_B l_B)^{k-1}}{\Delta})\eta(q_B l_B)$$

with $\Delta = q_A l_A q_C l_C$ and η the multiplicative function satisfying $\eta(p^v) = p^{v-j-1}$. In this way we have

$$\sum_{a=1}^{q} |S^*_{a/q}(x, q_0)|^2 \leq \eta(q_B l_B)^2 q \Delta^{-1} \|w^*\|^2 \tag{1.21}$$

where $\|w^*\|^2 = \sum_{a=1}^{\Delta} |w^*(a)|^2$, $w^*(a) = \sup_{Y \in [x,2x]} |w_Y(a)|$ and

$$w_Y(a) = \sum_{\substack{\lambda=1 \\ (\lambda, qq_0^{-1})=1}}^{qq_0^{-1}} \tau_{\lambda q_0}(\frac{a}{\Delta}) f(\frac{\lambda q_0}{Y}).$$

We can write

$$\|w^*\| = \langle w^*, g \rangle$$

where g a vector with $\|g\| = 1$. Besides, as f is continuous, for each a we have $w^*(a) = |w_{Y(a)}(a)|$ for a certain $Y(a)$. Thus

$$\|w^*\| = \sum_{a=1}^{\Delta} w_{Y(a)}(a)\overline{g(a)}.$$

By using Mellin inversion formula

$$f(u) = \frac{1}{2\pi i} \int_{1/2-i\infty}^{1/2+i\infty} u^{-s} \mathcal{M}_f(s) ds$$

we can write

$$w_{Y(a)}(a) = \frac{1}{2\pi i} \int_{1/2-i\infty}^{1/2+i\infty} \mathcal{M}_f(s) \sum_{\substack{\lambda=1 \\ (\lambda, qq_0^{-1})=1}}^{qq_0^{-1}} \frac{Y(a)^s}{(\lambda q_0)^s} \tau_{\lambda q_0}(\frac{a}{\Delta}) ds.$$

Therefore

$$\|w^*\| = \frac{1}{2\pi i}\int_{1/2-i\infty}^{1/2+i\infty} \mathcal{M}_f(s) \sum_{\substack{\lambda=1\\(\lambda,qq_0^{-1})=1}}^{qq_0^{-1}} T_s(\lambda)(\lambda q_0)^{-s} ds, \tag{1.22}$$

where

$$T_s(\lambda) = \sum_{a=1}^{\Delta} Y(a)^s \overline{g(a)} \tau_{\lambda q_0}(\frac{a}{\Delta}).$$

But by Cauchy's inequality

$$|\sum_{\substack{\lambda=1\\(\lambda,qq_0^{-1})=1}}^{qq_0^{-1}} T_s(\lambda)(\lambda q_0)^{-s}|^2 \le q_0^{-1}\log q \sum_{\substack{\lambda=1\\(\lambda,qq_0^{-1})=1}}^{qq_0^{-1}} |T_s(\lambda)|^2$$

Now we apply Lemma 1.21 to deduce that

$$\sum_{\substack{\lambda=1\\(\lambda,qq_0^{-1})=1}}^{qq_0^{-1}} |T_s(\lambda)|^2 \le x\|g\|^2 \max_{(n,q)=q_0} \sum_{\substack{\lambda=1\\(\lambda,qq_0^{-1})=1}}^{qq_0^{-1}} |\sum_{a=1}^{\Delta} \overline{\tau_n(\frac{a}{\Delta})}\tau_{\lambda q_0}(\frac{a}{\Delta})|.$$

But

$$\sum_{\substack{\lambda=1\\(\lambda,qq_0^{-1})=1}}^{qq_0^{-1}} |\sum_{a=1}^{\Delta} \overline{\tau_n(\frac{a}{\Delta})}\tau_{\lambda q_0}(\frac{a}{\Delta})| \le l_B \varrho_n(\Delta)$$

hence

$$|\sum_{\substack{\lambda=1\\(\lambda,qq_0^{-1})=1}}^{qq_0^{-1}} T_s(\lambda)(\lambda q_0)^{-s}|^2 \le x q_0^{-1}(\log q) l_B \varrho_n(\Delta). \tag{1.23}$$

As $(n,q) = q_0$, by Lemma 1.11 we have

$$\varrho_n(\Delta) = \varrho_n(q_C l_C)\varrho_n(q_A l_A) \le (q_C l_C)^4 k^{\omega(q_A l_A)}(q_A l_A)^2 \ll k^{\omega(q)}(q_A l_A)^2.$$

So substituting into (1.22) we conclude

$$\|w^*\|^2 \ll x q_0^{-1}(\log q) l_B k^{\omega(q)}(q_A l_A)^2$$

and by (1.21) we get

$$\sum_{a=1}^{q} |S^*_{a/q}(x,q_0)|^2 \ll \eta(q_B l_B)^2 q\Delta^{-1}(\log q) x q_0^{-1} l_B k^{\omega(q)}(q_A l_A)^2.$$

It always holds $\eta(q_B l_B) \leq q_B$, hence

$$\sum_{a=1}^{q} |S^*_{a/q}(x, q_0)|^2 \ll x q_B^2 l_B^2 q_A l_A^2 k^{\omega(q)} (\log q) \leq x q^2 (\log q) k^{\omega(q)}$$

and the result follows. □

In a similar way we demonstrate the following statement:

Proposition 1.23. *Let $D \in \mathbb{Z}, D \geq 1$, $1/2 \leq c < 1$ and $f : [0, \infty] \to \mathbb{C}$ a continuous function such that its Mellin transform is in L^1 and represents f through the inversion formula in the line $\Re s = c$. Defining*

$$S^*_{a/q}(x) = \sup_{Y \in [x, 2x]} |\sum_{m=1}^{q} \tau_m(\frac{a}{q}) f(\frac{m + Dq}{Y})|$$

we have

$$\frac{1}{q} \sum_{a=1}^{q} |S^*_{a/q}(x)|^2 \ll D^{-2c} x q k^{\omega(q)} d(q)^2.$$

Proof: Proceeding as in the proof of Proposition 1.22, but using the Mellin inversion formula in $\Re s = c$ we arrive at

$$\|w^*\| = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \mathcal{M}_f(s) \sum_{\substack{\lambda=1 \\ (\lambda, q q_0^{-1})=1}}^{q q_0^{-1}} T_s(\lambda)(\lambda q_0 + Dq)^{-s} ds, \tag{1.24}$$

which is the substitute of equation (1.22). Now when applying Cauchy's inequality we obtain

$$|\sum_{\substack{\lambda=1 \\ (\lambda, q q_0^{-1})=1}}^{q q_0^{-1}} T_s(\lambda)(\lambda q_0 + Dq)^{-s}|^2 \leq q_0^{-1} q (Dq)^{-2c} \sum_{\substack{\lambda=1 \\ (\lambda, q q_0^{-1})=1}}^{q q_0^{-1}} |T_s(\lambda)|^2$$

$$\sum_{\substack{\lambda=1 \\ (\lambda, q q_0^{-1})=1}}^{q q_0^{-1}} |T_s(\lambda)|^2 \leq x^{2c} l_B \varrho_n(\Delta).$$

Since $x \leq q$ we infer that $q_0^{-1} q (Dq)^{-2c} x^{2c} \leq D^{-2c} q_0^{-1} x$ and thus

$$|\sum_{\substack{\lambda=1 \\ (\lambda, q q_0^{-1})=1}}^{q q_0^{-1}} T_s(\lambda)(\lambda q_0 + Dq)^{-s}|^2 \leq D^{-2c} q_0^{-1} x l_B \varrho_n(\Delta),$$

that substitutes equation (1.23) and proves the result by ending as in the proof of Proposition 1.22. □

Corollary 1.24. *Let $J \in \mathbb{N}$. Let $f : [0,\infty] \to \mathbb{C}$ be a continuous function such that its Mellin transform is in L^1 and represents f through the inversion formula in the line $\Re s = c$ for any $1/2 \le c < 1$. Defining*

$$S^*_{a/q}(x) = \sup_{Y\in[x,2x]} |\sum_{m=1}^{Jq} \tau_m(\frac{a}{q}) f(\frac{m}{Y})|$$

we have

$$\frac{1}{q}\sum_{a=1}^{q} |S^*_{a/q}(x)|^2 \ll xqk^{\omega(q)}d(q)^2\log(Jq).$$

Proof: By Cauchy's inequality

$$|S^*_{a/q}(x)|^2 \le \sup_{Y\in[x,2x]} (|\sum_{m=1}^{q} \tau_m(\frac{a}{q}) f(\frac{m}{Y})|^2 + (\log J) \max_{1\le L\le J} |\sum_{m=Lq}^{2Lq} \tau_m(\frac{a}{q}) f(\frac{m}{Y})|^2).$$

Also

$$|\sum_{m=Lq}^{2Lq} \tau_m(\frac{a}{q}) f(\frac{m}{Y})|^2 \le L\sum_{D=L}^{2L} |\sum_{m=1}^{q} \tau_m(\frac{a}{q}) f(\frac{m+Dq}{Y})|^2.$$

Thus, by using Propositions 1.22 and 1.23 we deduce

$$\frac{1}{q}\sum_{a=1}^{q} |S^*_{a/q}(x)|^2 \ll xqk^{\omega(q)}d(q)^2(\log(q) + \log(J)J^{2(1-c)}),$$

and choosing $c = 1 - (\log J)^{-1}$ the corollary is proved. □

In order to apply this result to the functions $\widehat{g}$ and $\widehat{g_0}$ of the previous section, first we need to handle its Mellin transform. For this purpose we shall use these two lemmata:

Lemma 1.25. *Let $0 < c < 1$, $f \in L^1([0,\infty])$, $f(u)u^{-c} \in L^1([0,\infty])$. Then*

$$\mathcal{M}_{\widehat{f}}(s) = (2\pi i)^{-s}\Gamma(s)\mathcal{M}_f(1-s)$$

on the line $\Re s = c$.

Proof: For any $L > 0$ we have

$$\int_0^L \widehat{f}(x)x^{s-1}dx = \int_0^\infty f(u)\int_0^L e(-xu)x^{s-1}dx = \int_0^\infty f(u)u^{-s}du\int_0^{Lu} e(-x)x^{s-1}dx.$$

Since the inner integral is uniformly bounded in the region $L \geq 0$, by the dominated convergence theorem we have

$$\int_0^\infty \widehat{f}(x)x^{s-1}dx = \int_0^\infty e(-x)x^{s-1}dx \int_0^\infty f(u)u^{-s}du.$$

But deforming the integration domain into the complex plane we notice that

$$\int_0^\infty e(-x)x^{s-1}dx = (2\pi i)^{-s}\Gamma(s).$$

□

Lemma 1.26. *Let $0 < c < 1$, $f \in L^1([0,\infty])$, $f(u)u^{-c} \in L^1([0,\infty])$. Then we can write*

$$\widehat{f}(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \mathcal{M}_{\widehat{f}}(s)x^{-s}ds$$

with $\mathcal{M}_{\widehat{f}}(s) = (2\pi i)^{-s}\Gamma(s)\mathcal{M}_f(1-s)$.

Proof: Let $\rho \in C_0^\infty(\mathbb{R})$ with $\int \rho = 1$. We define $\rho_M(u) = M\rho(Mu)$. By Mellin inversion formula

$$\widehat{f}(x) = \lim_{M\to\infty} \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \mathcal{M}_{\widehat{f}*\rho_M}(s)x^{-s}ds.$$

Since $f \in L^1$ and $\rho \in C_0^\infty$ then $\widehat{f} * \rho_M(x) = (f\check{\rho}_M)\widehat{\ }(x)$. Applying Lemma 1.25 we deduce that

$$\mathcal{M}_{\widehat{f}*\rho_M}(s) = (2\pi i)^{-s}\Gamma(s)\mathcal{M}_{f\check{\rho}_M}(1-s).$$

Moreover $\check{\rho}_M(u) = \widehat{\rho}(-uM^{-1})$ and

$$\int_0^\infty |u^{-c-it}f(u)\widehat{\rho}(-\frac{u}{M})|du \ll \int_0^\infty |f(u)|u^{-c}du < \infty,$$

whence by dominated convergence we complete the proof, due to the decay of $\Gamma(s)$. □

Corollary 1.24 allow us to understand the behaviour of the function F near most of the rational numbers.

Proposition 1.27. *Let $q \in \mathbb{N}$, $0 < H < 1$ and $\delta > 1$. Let $1 < \alpha_1 < k$ and $k + 1/2 < \alpha_2 < k$. There exists a set $B = B(\delta, q, H)$ contained in*

$$\{a \in \mathbb{Z} : 1 \leq a \leq q, (a, q) = 1\}$$

with $|B| \ll q\delta^{-2}d(q)^2k^{\omega(q)}\log(qH^{-1})$, such that for any $a \notin B$ and every $H < h < 2H$ we have

$$F_{\alpha_1}(\frac{a}{q} + h) - F_{\alpha_1}(\frac{a}{q}) = A\frac{\tau}{q}h^{\frac{\alpha_1 - 1}{k}} + O(\delta h^{\frac{\alpha_1 - 1/2}{k}}) \tag{1.25}$$

and

$$F_{\alpha_2}(\frac{a}{q} + h) - F_{\alpha_2}(\frac{a}{q}) = A\frac{\tau}{q}h^{\frac{\alpha_2 - 1}{k}} + 2\pi i\zeta_{a/q}(\alpha - k)h + O(\delta h^{\frac{\alpha_2 - 1/2}{k}}). \tag{1.26}$$

Proof: Let $J = (H^{-1}q)^{(k-1)/(\alpha_1 - 1)}$, and B the set of a such that

$$\sup_{Y \in [H^{1/k}q, 2H^{1/k}q]} |\sum_{1 \leq |m| \leq qJ} \tau_m(\frac{a}{q})\widehat{g}_0(\frac{m}{Y})| + |\sum_{1 \leq |m| \leq qJ} \tau_m(\frac{a}{q})\widehat{g}(\frac{m}{Y})| \geq \delta(H^{\frac{1}{k}}q)^{\frac{1}{2}}q^{\frac{1}{2}}.$$

with $g_0(x) = x^{-\alpha_1}(e(x^k) - 1)$ and $g(x) = x^{-\alpha_2}(e(x^k) - 1 - 2\pi i x^k)$. By Lemma 1.26 it is plain that we can apply Corollary 1.24 to the functions $\widehat{g}_0(x)$ and $\widehat{g}_0(-x)$. In the case of g we split this function as

$$g(x) = g(x)\mathbb{I}_{[0,1]}(x) + x^{-\alpha_2}(e(x^k) - 1)\mathbb{I}_{(1,\infty)}(x) - \eta(x),$$

where $\eta(x) = 2\pi i x^{k-\alpha_2}\mathbb{I}_{(1,\infty)}(x)$. Lemma 1.26 can be applied to the first two functions. Moreover writing

$$\widehat{\eta}(y) = \lim_{N \to \infty} \widehat{\eta_N}(y)$$

with $\eta_N = \eta\mathbb{I}_{[0,N]}$ and using Lemma 1.26 for η_N we see that it is possible to apply Corollary 1.24 to $\widehat{g}(x)$ and to $\widehat{g}(-x)$. Thus

$$|B| \ll q\delta^{-2}d(q)^2k^{\omega(q)}\log(qH^{-1}).$$

If $a \notin B$, by appealing to Propositions 1.13 and 1.17 and to the inequality (1.18) we prove (1.26) and (1.25) respectively. □

1.5 Wavelets

As in Hardy's work [Har], Poisson's integral has been frequently employed in the study of the global regularity of functions (see [Ste]). Certain generalizations of this tools were already known by A. P. Calderón [Cal] but were not

rediscovered until twenty years later, with the name of wavelet transform, by A. Grossmann and J. Morlet [GM]. Later this was used in order to build orthonormal basis of smooth well-localized functions for the space $L^2(\mathbb{R}^n)$ (see [Mey, HW]).

This transform has proven to be a convenient tool for the study of the local regularity of functions [JM]. We shall use it in order to find out the precise smoothness of the function F, although not in a direct way as Jaffard does in [Jaf1] but to extend results when varying α.

We define wavelet as a function $\varphi : \mathbb{R} \to \mathbb{C}$ differentiable and with some decay

$$|\varphi(t)| + |\varphi'(t)| = O(\frac{1}{1+|t|^{1+\delta}}) \qquad \text{for some } \delta > 0 \tag{1.27}$$

and oscillation

$$\int_{-\infty}^{\infty} \varphi(t)dt = 0. \tag{1.28}$$

From it we can build up a family of wavelets

$$\frac{1}{a}\varphi(\frac{t-b}{a}) \qquad a > 0,\ b \in \mathbb{R}$$

that are going to be used to express a lot of different functions. For that we consider the continuous wavelet transform of a function $f \in L^\infty(\mathbb{R})$ with respect to φ

$$T(b,a) = \int_{-\infty}^{+\infty} f(t)\overline{\varphi}(\frac{t-b}{a})\frac{dt}{a}. \tag{1.29}$$

The function f can be recovered from the transform T: we choose a function g such that $g(t)\log(2+|t|) \in L^1(\mathbb{R})$, $a^{-1}\hat{\varphi}(a)\hat{g}(a) \in L^1(\mathbb{R})$ and

$$\int_0^{\infty} \overline{\hat{\varphi}}(a)\hat{g}(a)\frac{da}{a} = 1 \quad \text{if} \quad \text{supp}\varphi \cap (0,\infty) \neq \emptyset \tag{1.30}$$

$$\int_0^{\infty} \overline{\hat{\varphi}}(-a)\hat{g}(-a)\frac{da}{a} = 1 \quad \text{if} \quad \text{supp}\varphi \cap (-\infty,0) \neq \emptyset. \tag{1.31}$$

Any function g holding this requirements is called reconstruction wavelet for φ. There always exists such a function, and we can even take $g \in C_0^\infty(\mathbb{R})$ which is what we do throughout. We have (see [HT]) the following inversion formula.

Theorem 1.28. *Let f be a bounded and weakly oscillating function around 0, which means that*

$$\lim_{u\to\infty} \frac{1}{2u}\int_{t-u}^{t+u} f(y)dy = 0 \qquad \textit{uniformly in } t.$$

Then

$$f(t) = \lim_{\substack{\epsilon\to 0\\ \rho\to\infty}} \int_{\epsilon}^{\rho} \frac{da}{a} \int_{-\infty}^{+\infty} T(b,a)\frac{1}{a} g(\frac{t-b}{a})db.$$

for each t where f is continuous.

In order to study the local regularity until exponent $n \in \mathbb{N}$ we shall require $t^n\varphi(t) \in L^1(\mathbb{R})$ and moreover that

$$\int_{-\infty}^{\infty} t^m \varphi(t)dt = 0 \qquad m = 0, 1, \ldots, n-1 \tag{1.32}$$

the first n moments vanish (is an "atom "). In this way the local regularity of f can be characterized by the decay of the transform T (see [HT], [Jaf1]):

Theorem 1.29. *Let f be a bounded function satisfying*

$$f \in C^{\beta}(x_0) \qquad \beta \in (0, n)$$

for every $x_0 \in \mathbb{R}$. Then

$$T(b,a) \ll a^{\beta}(1 + \frac{|b-x_0|}{a})^{\beta},$$

where T is the transform of f with respect to a wavelet holding (1.32).

Proof: Since $f \in C^{\beta}(x_0)$ there exists a polynomial p of degree $n-1$ such that

$$f(x) - p(x - x_0) \ll |x - x_0|^{\beta}. \tag{1.33}$$

By 1.29 and (1.32) we have

$$|T(b,a)| = |\int_{-\infty}^{\infty} (f(x) - p(x-x_0))\overline{\psi}(\frac{x-b}{a})\frac{dx}{a}|,$$

and by (1.33)

$$T(b,a) \ll \int_{-\infty}^{\infty} |x-b|^{\beta}|\psi(\frac{x-b}{a})|\frac{dx}{a} + |b-x_0|^{\beta} \int_{-\infty}^{\infty} |\psi(\frac{x-b}{a})|\frac{dx}{a}$$

whence we deduce the result, because $t^n\psi(t) \in L^1$. □

Theorem 1.30. *Let f be a bounded weakly oscillating function and $f \in C^{\gamma}(\mathbb{R})$ for some $\gamma > 0$. Let $\beta' < \beta$ and $\beta \in (0, n)$, $\beta \notin \mathbb{Z}$ such that*

$$T(b,a) \ll a^{\beta}(1 + \frac{|b-x_0|}{a})^{\beta'}, \tag{1.34}$$

with T the transform of f with respect to a wavelet satisfying (1.32). Then

$$f \in C^{\beta}(x_0).$$

Besides, if $\beta > 1$ we can express the derivative f at x_0 as

$$f'(x_0) = \int_0^{\infty} \frac{da}{a} \int_0^{\infty} T(b,a) g'(\frac{x_0 - b}{a}) \frac{db}{a^2}$$

Proof: By Theorem 1.28 we have

$$f(x) = \int_0^{\infty} \omega(a,x) \frac{da}{a}$$

with

$$\omega(a,x) = \int_{-\infty}^{\infty} T(b,a) g(\frac{x-b}{a}) \frac{db}{a}.$$

From inequality (1.34) we deduce that

$$\omega(a,x) \ll a^{\beta} + a^{\beta-\beta'} |x - x_0|^{\beta'} + a^{\beta} \int_{-\infty}^{\infty} |\frac{b-x}{a}|^{\beta'} |g(\frac{x-b}{a})| \frac{db}{a} \ll a^{\beta} (1 + \frac{|x-x_0|}{a})^{\beta'}$$

and in the same way for each $j \geq 0$ we have

$$(\frac{\partial}{\partial x})^j \omega(a,x) = a^{-j} \int_{-\infty}^{\infty} T(b,a) g^{(j)}(\frac{x-b}{a}) \frac{db}{a} \ll a^{\beta-j} (1 + \frac{|x-x_0|}{a})^{\beta'}. \quad (1.35)$$

Therefore defining

$$p(t) = \sum_{j=0}^{m-1} \frac{t^j}{j!} \int_0^{\infty} (\frac{\partial}{\partial x})^j \omega(a,x_0) \frac{da}{a} = \int_0^{\infty} \upsilon(a,t) \frac{da}{a}$$

where m is the integer satisfying $m - 1 < \beta < m$, we have

$$f(x) - p(x - x_0) = \int_0^{\infty} (\omega(a,x) - \upsilon(a, x - x_0)) \frac{da}{a},$$

hence by (1.35) and Taylor's formula we see that up to a constant $f(x) - p(x - x_0)$ is bounded by

$$|x - x_0|^{\beta'} \int_0^{|x-x_0|} a^{\beta-\beta'} \frac{da}{a} + \sum_{j=0}^{m-1} |x - x_0|^j \int_0^{|x-x_0|} a^{\beta-j} \frac{da}{a} + |x - x_0|^m \int_{|x-x_0|}^{\infty} a^{\beta-m} \frac{da}{a}$$

and then

$$f(x) - p(x - x_0) \ll |x - x_0|^{\beta}.$$

□

We therefore arrive at the following theorem:

Theorem 1.31. *Let f bounded, $f \in C^\gamma(\mathbb{R})$ for some $\gamma > 0$ and $0 < \beta_f(x_0) < n$. Then*

$$\beta_f(x_0) = \sup\{\beta \in \mathbb{R} : T(x_0 + b, a) = O((a + |b|)^\beta)\}.$$

Let us apply this characterization of regularity to our family of functions

$$F(x) = F_\alpha(x) = \sum_{n=1}^{\infty} n^{-\alpha} e(n^k x).$$

For this purpose we consider a suitable wavelet.

Lemma 1.32. *Let $r > 0$ and*

$$\varphi_r(t) = \frac{1}{(2\pi)^{r+1}} \frac{\Gamma(1+r)}{(1+it)^{r+1}}.$$

If T is the wavelet transform of the function

$$f(x) = \sum_{m=1}^{\infty} a_m e(mx),$$

with $\sum_{m=1}^{\infty} |a_m| < \infty$, with respect to φ_r then

$$T(b, a) = a^r \theta(b + ia)$$

where

$$\theta(z) = \sum_{n=1}^{\infty} a_m m^r e(mz).$$

Proof:

$$T(b, a) = \sum_{m=1}^{\infty} a_m e(mb) \widehat{\varphi}_r(-ma). \tag{1.36}$$

We consider the function

$$G_r(x) = e^{-2\pi x} x^r \mathbb{I}_{[0,\infty]}(x).$$

By deforming the integration domain into $\mathbb{C}$ we realize

$$\widehat{G}_r(u) = \varphi_r(u)$$

and by the wavelet inversion formula

$$\widehat{\varphi}_r(-x) = G_r(x).$$

Substituting this formula in (1.36) we finish the proof. □

By Theorem 1.31 and Lemma 1.32 we get a relation between the regularity of $F_{\alpha,k}$ when varying α:

Corollary 1.33. *Let $x_0 \in \mathbb{R}$, $1 < \alpha$ and $v > 0$. Then*

$$\beta_{F_{\alpha+v,k}}(x_0) \geq \beta_{F_{\alpha,k}}(x_0) + \frac{v}{k}.$$

Proof: Let $T_{\alpha,k}$ be the transform of $F_{\alpha,k}$ with respect to $\varphi_{d+\alpha/k}$, for any $d > 0$. We have

$$T_{\alpha,k}(b,a) = a^{\frac{\alpha}{k}+d}\theta_d(b+ia)$$

where $\theta_d(z) = \sum_{n=1}^{\infty} n^{dk} e(n^k z)$, whence

$$T_{\alpha+v,k}(b,a) = a^{\frac{v}{k}} T_{\alpha,k}(b,a).$$

By Theorem 1.29 we deduce that if $F_{\alpha,k} \in \mathbb{C}^{\beta}(x_0)$ then

$$T_{\alpha+v,k}(b,a) \ll a^{\frac{v}{k}+\beta}(1 + \frac{|b-x_0|}{a})^{\beta}$$

and by Theorem 1.30 we obtain the corollary. □

We have just observed that wavelet transform can be applied to deal with the smoothness of functions. Let us see that we can take advantage of it in order to determine the fractal dimension of graphs of continuous functions.

Let $E \subset \mathbb{R}^2$ be a bounded set and $N_h(E)$ the minimum number of sets with diameter not larger than h that cover E. Then we define the fractal dimension or Minkowski dimension of E as

$$\dim_{\mathrm{M}}(E) = \lim_{h \to 0} \frac{\log N_h(E)}{\log h^{-1}}$$

whenever the limit exists. Anyway we can consider upper dimension $\overline{\dim_{\mathrm{M}}}$ and lower dimension $\underline{\dim_{\mathrm{M}}}$ given by the upper and lower limits respectively. Let $f : [0,1] \to \mathbb{C}$ be continuous. Defining $\Gamma_f = \{(x, f(x)) \in \mathbb{R}^2 : 0 \leq x \leq 1\}$ we have

$$\log N_h(\Gamma_f) \sim \log(h^{-1}(V_h(f) + 1))$$

where

$$V_h(\phi) = \sup\{ \sum_{j < h^{-1}} |\phi(x_j) - \phi(y_j)| : x_j, y_j \in I_j, \forall j < h^{-1}\}$$

and

$$I_j = [(j-1)h, jh] \qquad j \in \mathbb{N}.$$

We are going to learn in which way $V_h(f)$ is related to $S_h(T,a)$ where T is the wavelet transform of f and

$$S_h(T,a) = \sup\{ \sum_{j < h^{-1}} |T(b_j, a)| : b_j \in I_j \, \forall j < h^{-1}\}.$$

We have

$$\lim_{h\to 0} hS_h(T,a) = \int_0^1 |T(b,a)|db$$

and since $tS_t(T,a)$ is decreasing in t we conclude

$$\int_0^1 |T(b,a)|db \le tS_t(T,a) \qquad \text{for any } t>0. \tag{1.37}$$

Lemma 1.34. *Let $f:\mathbb{R}\to\mathbb{C}$ be a periodic function of period one. If $T(b,a)$ is its wavelet transform with respect to the wavelet φ satisfying*

$$\varphi(t) = O(t^{-2-\epsilon}),$$

then

$$S_h(T,a) \ll V_h(f)$$

uniformly in $a<h$.

Proof: We have

$$T(b,a) = \int_{-\infty}^{+\infty} \frac{1}{a}\overline{\varphi}(\frac{u}{a})(f(b+u)-f(b))\,du$$

hence

$$\sum_{j<h^{-1}} |T(b_j,a)| \le \int_{-\infty}^{+\infty} \frac{1}{a}|\varphi(\frac{u}{a})| \sum_{j<h^{-1}} |f(b_j+u)-f(b_j)|\,du$$

But

$$\sum_{j<h^{-1}} |f(b_j+u)-f(b_j)| \ll V_h(f),$$

and therefore

$$\sum_{j<h^{-1}} |T(b_j,a)| \ll V_h(f).$$

□

Lemma 1.35. *Let f be a periodic function of period 1, with $f\in C^\gamma(\mathbb{R})$ for some $\gamma>0$. If $T(b,a)$ is its wavelet transform, then*

$$V_h(f) \ll (\log h^{-1})\big(\sup_{a<h} S_h(T,a) + \sup_{h<a<1} S_a(T,a)\big).$$

Proof: We can assume γ to be small enough. Then

$$T(b,a) \ll a^{\gamma} \qquad a \to 0.$$

Therefore by Theorem 1.28

$$\sum_{j \le h^{-1}} |f(x_j) - f(y_j)| \le \int_{\epsilon}^{h} I_1(a)\frac{da}{a} + \int_{h}^{\rho} I_2(a)\frac{da}{a} + O(h^{-1}\epsilon^{\gamma}),$$

where

$$I_1(a) = \int_{-\infty}^{\infty} |g(\frac{u}{a})|\frac{1}{a}\sum_{j<h^{-1}} (|T(x_j - u, a)| + |T(y_j - u, a)|)\, du,$$

$$I_2(a) = \int_{-\infty}^{\infty} |T(b,a)|\frac{1}{a}\sum_{j<h^{-1}} |g(\frac{x_j - b}{a}) - g(\frac{y_j - b}{a})|\, db.$$

We have $I_1(a) \ll S_h(T,a)$. By the periodicity of T and the Mean Value Theorem we infer

$$I_2(a) \ll \frac{h}{a}\int_0^1 |T(b,a)|\frac{db}{a} \sup\{\sum_{j\in\mathbb{Z}} |g'(\frac{\xi_j}{a})| : h \le |\xi_{j+1} - \xi_j| \le 2h\, \forall j \in \mathbb{Z}\}$$

hence

$$I_2(a) \ll \int_0^1 |T(b,a)|\frac{db}{a}.$$

Taking into account (1.37) follows that

$$\int_0^1 |T(b,a)|\frac{db}{a} \le S_a(T,a), \qquad a < 1$$

and finally taking $\epsilon = h^{-1/\gamma}$ we conclude the proof. □

As outcome of the two last lemmata we deduce:

Proposition 1.36. *Let $f \in C^{\gamma}(\mathbb{R})$, $|\varphi(t)| \ll (1+|t|)^{-2-\epsilon}$ and*

$$L(h) = \sup_{a \le h} S_h(T,a).$$

Then

$$\dim_{\mathrm{M}}(\Gamma_f) = \lim_{h\to 0} \frac{\log\left(h^{-1}(L(h)+1)\right)}{\log h^{-1}}$$

if the limit exists. Moreover the limit exists whenever $\dim_{\mathrm{M}}(\Gamma_f)$ *does.*

In [CC2] it is calculated the fractal dimension of the graph Γ in the interval $[0,1]$ of the function

$$\sum_{n=1}^{\infty} \frac{c_n e(n^k x)}{n^\alpha} \qquad where \qquad 0 < \underline{\lim} c_n \leq \overline{\lim} c_n < \infty$$

for any $\alpha > (k+1)/2$. In fact this proves that the bound for the lower dimension

$$\underline{\dim}_{\mathrm{M}}(\Gamma) \geq 2 + \frac{1}{2k} - \frac{\alpha}{k}$$

holds in the whole range $\alpha > 1$. We are going to extend the calculation of this dimension, although we write the result only in the case $c_n = 1$. Inside the proof we shall use a Large Sieve inequality (see [Dav2]) different from Lemma 1.21.

Lemma 1.37. *Let $S : [0,1] \to \mathbb{R}$ be a function with continuous derivative. If $x_1, x_2, \ldots, x_R$ are h-spaced points, then*

$$\sum_{j=1}^{R} |S(x_j)|^2 \leq \frac{1}{h} \int_0^1 |S(x)|^2 dx + (\int_0^1 |S(x)|^2 dx)^{1/2} (\int_0^1 |S'(x)|^2 dx)^{1/2}.$$

We shall also use, as it was done in [CC2] to prove the lower dimension, that

$$(\int_0^1 |\sum_{n \leq N} c_n e(n^k x)|^4 \, dx)^{1/4} \ll N^{\frac{1}{2}+\epsilon}. \tag{1.38}$$

This inequality is deduced from the fact $r(n) \ll n^\epsilon$, where $r(n)$ is the number of representations of n as a sum of two k-powers, because if $n = a^k + b^k$ then $a+b$ divide n when k is odd and $a^{k/2} + i b^{k/2}$ divide n in the ring $\mathbb{Z}[i]$ whenever k is even.

If we had the same result for the norm in L^{2k} then we would get the fractal dimension in the range $\alpha > 1$. In general, bounds for different norms provide upper bounds for the fractal dimension (see [CU1]). By using (1.38) we arrive at the following statement:

Proposition 1.38. *Suppose $\alpha > (k+2)/4$. Then*

$$\dim_{\mathrm{M}}(\Gamma_F) = \max(1, 2 + \frac{1}{2k} - \frac{\alpha}{k}).$$

Proof: The wavelet transform of F with respect to $\varphi_{1+\alpha/k}$ is $T(b,a) = a^{1+\alpha/k} \theta(b+ia)$ where

$$\theta(b+ia) = \sum_{n=1}^{\infty} n^k e(n^k(b+ia)).$$

We divide the sum into dyadic intervals

$$\theta(b+ia)=\sum_{l=0}^{\infty}P_{2^l}(b),$$

with

$$P_M(b)=\sum_{M\leq n<2M}n^k e^{-2\pi n^k a}e(n^k b).$$

By Hölder's inequality

$$\sum_{j<h^{-1}}|P_M(b_j)|\ll h^{-\frac{3}{4}}(\sum_{j<h^{-1}}|P_M(b_j)|^4)^{1/4}.$$

Applying Lemma 1.37 to $P_M(x)^2$ and inequality (1.38) we realize that whenever b_j are h-spaced

$$\sum_{j<h^{-1}}|P_M(b_j)|^4\ll M^{4k+\epsilon}(h^{-1}+M^k)e^{-M^k a}M^2.$$

Then for $a<h$ we have

$$S_h(T,a)\ll a^{\frac{\alpha}{k}}h^{-\frac{3}{4}}(a^{-1-\frac{2}{k}})^{\frac{1}{4}+\epsilon}=h^{-\frac{3}{4}}a^{\frac{\alpha}{k}-\frac{1}{4}-\frac{1}{2k}-\epsilon},$$

and since $\alpha>(k+2)/4$ we infer

$$\sup_{a<h}S_h(T,a)\ll h^{-1-\frac{1}{2k}+\frac{\alpha}{k}-\epsilon}.$$

Appealing to Lemma 1.35 is enough to conclude. □

The previous proposition could have been demonstrated in much the same way without the use of wavelets. But this tool provides a relation between the dimensions of the graphs of the functions $F_{\alpha,k}$:

Proposition 1.39. *Let $\alpha_2>\alpha_1>1$. Then*

$$\overline{\dim}\Gamma_{F_{\alpha_2}}\leq\overline{\dim}\Gamma_{F_{\alpha_1}}-\frac{\alpha_2-\alpha_1}{k}.$$

Proof: If T_1 and T_2 are the wavelet transforms of F_{α_1} and F_{α_2} with respect to $\varphi_{1+\alpha_1/k}$ and $\varphi_{1+\alpha_2/k}$ respectively, then

$$T_2(b,a)=a^{\frac{\alpha_2-\alpha_1}{k}}T_1(b,a)$$

hence

$$S_h(T_2,a)=a^{\frac{\alpha_2-\alpha_1}{k}}S_h(T_1,a)$$

and taking the supremum on $a<h$ we deduce the result. □

1.6 Regularity at the irrationals

We say that $f : \mathbb{R} \to \mathbb{C}$ is a multifractal function whenever the associated function

$$d_{\mathrm{H}}(\beta) = \dim_{\mathrm{H}}\{x \in \mathbb{R} : \beta_f(x) = \beta\}$$

is positive for more than one point.

Until now we have only studied the smoothness of the function near the rationals, hence we cannot say that $F_{\alpha,k}$ is a multifractal function. Throughout this section we shall see that, as in the case $k = 2$, any function $F_{\alpha,k}$ is multifractal and in fact its regularity at any point depends on how this point is approached by the rationals. The main difference between the cases $k = 2$ and $k > 2$ is that in the former the irrationals always have the same kind of irregularity whereas in the latter there are infinitely many possible behaviours.

We are going to start obtaining upper and lower bounds for the Hölder exponent at any point. For this aim we recall the following result on the control of trigonometric sums (see [Vau]).

Lemma 1.40. *(Weyl's inequality). If P polynomial of degree k with main coefficient A, and a/q is an irreducible fraction such that*

$$|A - \frac{a}{q}| \leq q^{-2},$$

then

$$\sum_{n \leq N} e(P(n)) \ll (Nq^{-1/K} + N^{1-1/K} + N^{1-k/K}q^{1/K})N^{\epsilon}$$

for each $\epsilon > 0$ with $K = 2^{k-1}$.

This is the upper bound we get for the regularity at a point x_0, which depends on which space E_r is that point.

Proposition 1.41. *For any point x of E_r we have*

$$\beta_F(x) \geq \frac{\alpha - 1}{k} + 2^{1-k} \min(\frac{1}{k}, \frac{1}{2(r-1)}).$$

Proof: By Mean Value Theorem

$$F(x+h) - F(x+\frac{h}{2}) \ll h|\sum_{n \leq h^{-1/k}} 2\pi i n^{k-\alpha} e(n^k \xi_1)| + |\sum_{n > h^{-1/k}} n^{-\alpha} e(n^k \xi_2)| \tag{1.39}$$

for certain $x+h/2 \leq \xi_1, \xi_2 \leq x+h$. We consider the consecutive convergents a_n/q_n and a_{n-1}/q_{n-1} of x such that

$$q_n^{-r_n} = |x - \frac{a_n}{q_n}| \leq |h| \leq |x - \frac{a_{n-1}}{q_{n-1}}| = q_{n-1}^{-r_{n-1}}.$$

Since

$$|\frac{a_n}{q_n} - \frac{a_{n-1}}{q_{n-1}}| = \frac{1}{q_n q_{n-1}}$$

and the convergents are on different sides of x we see that

$$\frac{1}{2} q_{n-1}^{r_{n-1}-1} \leq q_n \leq q_{n-1}^{r_{n-1}-1}. \tag{1.40}$$

There are two cases: the first is when h satisfies

$$q_n^{-r_n} \leq |h| \leq q_n^{-2}$$

which can be transformed into

$$h^{-\frac{1}{r_n}} \leq q_n \leq h^{-\frac{1}{2}}.$$

In this case by dividing the sums in (1.39) into dyadic intervals and summing by parts we can apply Lemma 1.40 with a_n/q_n approximating ξ_j, $j = 1, 2$, obtaining in that way

$$F(x+h) - F(x+\frac{h}{2}) \ll h^{\frac{\alpha-1}{k}} (h^{\frac{1}{kK}} + h^{\frac{1}{r_n K}} + h^{(1-\frac{1}{2})\frac{1}{K}}).$$

The second case is when h is near a_{n-1}/q_{n-1}, namely

$$q_n^{-2} \leq |h| \leq q_{n-1}^{-r_{n-1}},$$

which by (1.40) can be transformed into

$$h^{-\frac{1}{2r_{n-1}-2}} \ll q_{n-1} \leq h^{-\frac{1}{r_{n-1}}}.$$

Proceeding as in the previous case, but using as approximation the rational a_{n-1}/q_{n-1}, we obtain

$$F(x+h) - F(x+\frac{h}{2}) \ll h^{\frac{\alpha-1}{k}} (h^{\frac{1}{kK}} + h^{\frac{1}{(2r_{n-1}-2)K}} + h^{(1-\frac{1}{r_{n-1}})\frac{1}{K}}).$$

Thus, taking the maximum of both of them we arrive at

$$F(x+h) - F(x+\frac{h}{2}) \ll h^{\frac{\alpha-1}{k}} (h^{\frac{1}{kK}} + h^{\frac{1}{(2r_{n-1}-2)K}} + h^{\frac{1}{r_n K}} + h^{(1-\frac{1}{r_{n-1}})\frac{1}{K}}).$$

Taking into account that $\limsup_n r_n = r$ and that

$$F(x+h) - F(x) = \sum_{j=0}^{\infty} \big(F(x+h2^{-j}) - F(x+h2^{-j-1})\big)$$

we conclude the proof. □

We can also see that the function cannot be very smooth at any point.

Proposition 1.42. *Let $\alpha < k-1$. For any x we have*

$$\beta_F(x) \leq \frac{\alpha}{k-1}.$$

Proof: We are going to prove that

$$F(x+h) - F(x) = \Omega(|h|^{\frac{\alpha}{k-1}} |\log|h||^{-2}).$$

Consider Féjer's kernel

$$f_M(x) = \sum_{|n|\leq M} (1 - \frac{|n|}{M}) e(nx) = \frac{1}{M}\Big(\frac{\sin(\pi M x)}{\sin(\pi x)}\Big)^2 \quad \text{with} M = N^{k-1}, N > 1.$$

Note that for $n \neq N$ we have $|N^k - n^k| \geq N^k - (N-1)^k > M$, hence

$$\int_{-1/2}^{1/2} e(N^k t) f_M(t)(F(x-t) - F(x))dt = N^{-\alpha} e(N^k x).$$

If $|F(x-t) - F(x)| = O(t^{\alpha/(k-1)}(\log|t|)^{-2})$, then the previous integral would be $O(\int |t|^{\alpha/(k-1)}(\log|t|)^{-2}|f_M(t)|dt)$. Dividing it into dyadic intervals of length M^{-1} we deduce that the integral is $O(M^{-\alpha/(k-1)}(\log M)^{-1})$ and this is not possible. □

The bounds we have obtained are far from being sharp, at least for most of the points. Since $F'_{1/2+\epsilon,k} \in L^2([0,1])$, by the Fundamental Theorem of Calculus we have $F_{k+1/2+\epsilon,k}$ is differentiable almost everywhere, hence

$$F_{k+1/2+\epsilon,k} \in C^1(x_0)$$

for almost every x_0. By Corollary 1.33 we obtain for $\alpha \geq k + 1/2$ that for almost every $x \in \mathbb{R}$ we have

$$\beta_F(x) \geq \frac{\alpha - 1/2}{k}. \tag{1.41}$$

We shall see this kind of result can be generalized for the function F to every $\alpha > 1$ and E_r with $r \geq 2$. In order to understand it we first need to deal with the Hausdorff measure of these sets.

Definition 1.43. Let $E \subset \mathbb{R}$. For any $s > 0$ define its exterior s-dimensional Hausdorff measure as

$$\mathcal{H}^s(E) = \sup_{\delta>0} \mathcal{H}^s_\delta(E) = \lim_{\delta\to 0+} \mathcal{H}^s_\delta(E)$$

with

$$\mathcal{H}^s_\delta(E) = \inf\{\sum_{i=1}^{\infty} |U_i|^s : E \subset \bigcup_i U_i, |U_i| \leq \delta\}.$$

It can be demonstrated (see [Fal1]) that any Borel set in $\mathbb{R}$ is $\mathcal{H}^s$-measurable, and we shall only deal with these type of sets. For any $\gamma > 0$ and $\delta < 1$ we have

$$\mathcal{H}^{s+\gamma}_\delta(E) \leq \delta^\gamma \mathcal{H}^s_\delta.$$

Hence $\mathcal{H}^s(E)$ is a non-decreasing function and since $\mathcal{H}^s(E) = 0$ for any $s > 1$, it has sense to define the Hausdorff dimension of E as

$$\dim_{\mathrm{H}}(E) = \inf\{s > 0 : \mathcal{H}^s(E) = 0\}.$$

Let us see the basic result for handling the Hausdorff dimension of a set

Lemma 1.44. *(Example 4.6 in [Fal2]) Let $[0,1] = G_0 \supset G_1 \supset G_2 \supset \ldots$, where each G_j is a finite union of intervals (whose maximum length to zero when j tends to infinity) such that each interval of G_{j-1} contains at least $m_j \geq 2$ two intervals of G_j and these are separated by a distance larger than ε_j, with $0 < \varepsilon_j < \varepsilon_{j-1}$. Defining*

$$s_j = \frac{\log(m_1 \ldots m_{j-1})}{-\log(m_j \varepsilon_j)}, \qquad s = \liminf_j s_j$$

we have

$$\dim_{\mathrm{H}}(\bigcap_{j=0}^{\infty} G_j) \geq s.$$

If moreover $s_j \geq s$ for every j sufficiently large then $\mathcal{H}^s(\cap G_j) > 0$.

Lemma 1.45. *For any $r \geq 2$ we have $\dim_{\mathrm{H}} E_r = 2/r$ and*

$$\mathcal{H}^{2/r}(E_r) > 0.$$

Proof: For the upper dimension, observe that for any $r' < r$ holds

$$E_r \subset \bigcap_{N=1}^{\infty} A_N$$

where

$$A_N = \bigcup_{\substack{n\geq N\\ 1\leq a\leq n}} [\frac{a}{n} - \frac{1}{(n\log n)^{r'}}, \frac{a}{n} + \frac{1}{(n\log n)^{r'}}].$$

But

$$\mathcal{H}^{2/r'}(A_N) \ll (\log N)^{-1}$$

hence $\mathcal{H}^{2/r'}(E_r) = 0$ and therefore $\dim_{\mathrm{H}} E_r \leq 2/r$.

For the lower one consider a sequence $(n_j)_{j\in\mathbb{N}}$ defined by $n_j = n_{j-1}^j$ and build the sets

$$G_j = \bigcup_{n_j<p<2n_j} \bigcup_{1\leq a<p} I_r(a,p)$$

with

$$I_r(a,p) = [\frac{a}{p} - \frac{e^{(\log p)^{1/2}}}{p^r}, \frac{a}{p} - \frac{1}{p^r}] \cup [\frac{a}{p} + \frac{1}{p^r}, \frac{a}{p} + \frac{e^{(\log p)^{1/2}}}{p^r}]. \tag{1.42}$$

Then

$$E_r \supset \bigcap_{j=1}^{\infty} G_j$$

and we can use Lemma 1.44 with $m_j \asymp n_j^2(\log n_j)^{-1}\exp((\log n_{j-1})^{1/2})(n_{j-1})^{-r}$ and $\epsilon_j \asymp n_j^{-2}$. Thus for j sufficiently large

$$s_j \geq \frac{2\log n_{j-1} - r\log n_{j-2} - \log\log n_{j-1}}{r\log n_{j-1} - (\log n_{j-1})^{1/2} + \log\log n_j} \geq \frac{2}{r},$$

hence $\mathcal{H}^{2/r}(E_r) > 0$. □

We can already state the following result on the regularity of F almost everywhere in E_r.

Theorem 1.46. *For any $r \geq 2$, we have:*

i) For almost every x in E_r (with the measure $\mathcal{H}^{2/r}$) we have

$$\beta_F(x) \geq \min\big(\frac{\alpha - 1/2}{k}, \frac{\alpha - 1}{k} + \frac{1}{2r}\big).$$

Besides, if $\alpha > k + 1/2$ and $(\alpha-1)/k + 1/(2r) > 1$ then

$$F'(x) = \lim_{n\to\infty} \zeta_{a_n/q_n}(\alpha - k). \tag{1.43}$$

ii) If $r \geq k$, there exists a set $E_{r,0}$ inside E_r of positive measure and such that for any $x \in E_{r,0}$

$$\beta_F(x) \geq \frac{\alpha - 1/2}{k}. \tag{1.44}$$

iii) if $r > k$, there exists a set $E_{r,1}$ inside E_r of positive measure such that for any $x \in E_{r,1}$

$$\beta_F(x) = \frac{\alpha - 1}{k} + \frac{1}{2r}. \tag{1.45}$$

Proof: We begin proving i). Let $1 \leq \alpha_1 < k$ and $k + 1/2 < \alpha_2 < k + 1$ such that $\alpha_1 \leq \alpha \leq \alpha_2$. For any $\epsilon > 0$, take

$$B_\epsilon(q) = \bigcup_{\substack{j \in \mathbb{N} \\ q^{-r-1} \leq 2^{-j} \leq q^{-1}}} B(q^\epsilon, q, 2^{-j})$$

with $B(q^\epsilon, q, 2^{-j})$ the set that appears in the statement of Proposition 1.27. We have

$$|B_\epsilon(q)| \ll q^{1-\epsilon}. \tag{1.46}$$

On the other hand, define

$$C_\epsilon(q) = \{a \in \mathbb{Z} : 1 \leq a \leq q, (a,q) = 1, |\tau(a/q)| \geq q^{1/2+\epsilon}\}.$$

By Lemmata 1.5, 1.6 and 1.7 we get

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} |\tau(\frac{a}{q})| \ll Q^{2+1/2+\epsilon/2}. \tag{1.47}$$

If $(a_n/q_n)_{n \in \mathbb{N}}$ is the sequence of convergents of x, the we define

$$M_{r,\epsilon} = \{x \in E_r : |\{a_n/q_n : a_n \in B_\epsilon(q_n) \cup C_\epsilon(q_n)\}| = \infty\}.$$

For any $Q_0 \in \mathbb{N}$ we have

$$M_{r,\epsilon} \subset \bigcup_{2^j = Q \geq Q_0} \bigcup_{Q \leq q \leq 2Q} \bigcup_{a \in B_\epsilon(q) \cup C_\epsilon(q)} [\frac{a}{q} - \frac{1}{q^{r-\epsilon/2}}, \frac{a}{q} + \frac{1}{q^{r-\epsilon/2}}].$$

Since the $\mathcal{H}^{2/r}-$measure of each interval is smaller or equal than $q^{\epsilon/2-2}$, by (1.46) and (1.47) we get

$$\mathcal{H}^{2/r}(M_{r,\epsilon}) \ll Q_0^{-\epsilon/2}$$

and thus $\mathcal{H}^{2/r}(M_{r,\epsilon}) = 0$. Defining

$$M_r = \bigcup_{n=1}^{\infty} M_{r,1/n}$$

we also have $\mathcal{H}^{2/r}(M_r) = 0$. If $x \in E_r \setminus M_r$, for any sufficiently small h we can find convergents a_{n-1}/q_{n-1}, a_n/q_n of x satisfying

$$2q_n^{-r_n} < |h| \leq 2q_{n-1}^{-r_{n-1}} \leq q_n^{-1}.$$

In this way, we write

$$F_{\alpha_1,k}(x+h) - F_{\alpha_1,k}(x) = F_{\alpha_1,k}(x+h) - F_{\alpha_1,k}(\frac{a_n}{q_n}) - (F_{\alpha_1,k}(x) - F_{\alpha_1,k}(\frac{a_n}{q_n})).$$

By (1.25), for each $\epsilon > 0$ we obtain

$$F_{\alpha_1,k}(x+h) - F_{\alpha_1,k}(x) \ll \frac{|h|^{\frac{\alpha_1-1}{k}}}{q_n^{\frac{1}{2}-\epsilon}} + q_n^{\epsilon}|h|^{\frac{\alpha_1-1/2}{k}} \ll |h|^{\frac{\alpha_1-1}{k}+\frac{1}{2r_n}-\frac{\epsilon}{r_n}} + |h|^{\frac{\alpha_1-1/2}{k}-\epsilon}.$$

For $h \to 0$ we have

$$\beta_{F_{\alpha_1,k}}(x) \geq \min\big(\frac{\alpha_1-1}{k} + \frac{1}{2r}, \frac{\alpha_1-1/2}{k}\big) - \epsilon.$$

But this holds for any $\epsilon > 0$, hence also for $\epsilon = 0$. By Corollary 1.33 we deduce

$$\beta_{F_{\alpha^*,k}}(x) \geq \min\big(\frac{\alpha^*-1}{k} + \frac{1}{2r}, \frac{\alpha^*-1/2}{k}\big) \tag{1.48}$$

for any $\alpha^* > \alpha_1$, and in particular for $\alpha^* = \alpha$. Moreover if $\alpha > k + 1/2$ and take $\alpha_2 = \alpha$ and by (1.26) we have for $x \in E_r \setminus M_r$, $h = x - a_n/q_n > 0$ the expression

$$F(x) - F(\frac{a_n}{q_n}) = 2\pi i \zeta_{a_n/q_n}(\alpha - k)h + O(|h|^{\frac{\alpha-1}{k}+\frac{1}{2r_n}-\frac{\epsilon}{r_n}} + |h|^{\frac{\alpha-1/2}{k}-\epsilon})$$

but by (1.48) we know that whenever $(\alpha-1)/k + 1/(2r) > 1$

$$F(x) - F(\frac{a_n}{q_n}) = F'(x)h + O(|h|^{\frac{\alpha-1}{k}+\frac{1}{2r}-\epsilon} + |h|^{\frac{\alpha-1/2}{k}-\epsilon})$$

thus

$$(F'(x) - 2\pi i \zeta_{a_n/q_n}(\alpha - k))h = o(|h|)$$

which proves (1.43).

In order to prove ii), define

$$E_{r,0} = (E_r \setminus M_r) \cap \{x : (q_n)_{n\in\mathbb{N}} \subset P_0\},$$

where $P_0 = \{p \in \mathbb{N} : p \text{ prime }, (p, k-1) = 1\}$. In the same way as in Lemma 1.45 can be proved $\mathcal{H}^{2/r}(E_{r,0}) > 0$. Taking into account that $\tau(a/p) = 0$ if $p \in P_0$, as before we have

$$\beta_{F_{\alpha^*,k}}(x) \geq \frac{\alpha^* - 1/2}{k}$$

for any $\alpha^* > \alpha_1$.

For iii), define

$$E_{r,1} = (E_r \setminus M_r) \cap \{x : |(q_n)_{n\in\mathbb{N}} \cap P_1| = \infty, |\tau(a_n/q_n)| \geq q_n^{1/2}/2\}$$

with $P_1 = \{p \in \mathbb{N} : p \text{ prime }, (p, k-1) \neq 1\}$. By using Proposition 1.20 we can prove $\mathcal{H}^{2/r}(E_{r,1}) > 0$ following the proof of Lemma 1.45. If $x \in E_{r,1}$ and $h_n = x - a_n/q_n > 0$ we have

$$F_{\alpha_2,k}(x) - F_{\alpha_2,k}(\frac{a_n}{q_n}) = A\tau(\frac{a_n}{q_n})h_n^{\frac{\alpha_2-1}{k}} + 2\pi i\zeta_{a_n/q_n}(\alpha_2 - k)h_n + O(|h_n|^{\frac{\alpha_2-1/2}{k}-\epsilon})$$

moreover for any $h \in (h_n/2, 2h_n)$

$$F_{\alpha_2,k}(\frac{a_n}{q_n}+h)-F_{\alpha_2,k}(\frac{a_n}{q_n}) = A\tau(\frac{a_n}{q_n})h^{\frac{\alpha_2-1}{k}}+2\pi i\zeta_{a_n/q_n}(\alpha_2-k)h+O(|h_n|^{\frac{\alpha_2-1/2}{k}-\epsilon})$$

hence if $r > k$ there exists $h_n^* \in (h_n/2, 2h_n)$ such that

$$|F_{\alpha_2,k}(x) - F_{\alpha_2,k}(\frac{a_n}{q_n} + h_n^*)| \gg q_n^{-\frac{1}{2}} h_n^{\frac{\alpha_2-1}{k}} \gg h_n^{\frac{\alpha_2-1}{k}+\frac{1}{2r_n}},$$

taking ϵ sufficiently small. By Corollary 1.33 we have

$$\beta_{F_{\alpha^*,k}}(x) = \frac{\alpha^* - 1}{k} + \frac{1}{2r}$$

for every $\alpha^* \in [\alpha_1, \alpha_2]$, and in particular for $\alpha^* = \alpha$. □

In E_r there are points where F behaves much more irregularly than in mean. To the end of studying the quantity of this exceptional points we need this lemma.

Lemma 1.47. *Let I be an interval contained in $[0,1]$ and $N \in \mathbb{N}$, with $|I| \geq N^{-1}$. There exists an integer n with $N \leq n \leq 2N$, a constant $c > 0$ and a subset $B = B_n$ of*

$$\{a/p^k \in I : (a,p) = 1, 1 \leq a \leq p^k, n \leq p \leq n + n^{1/2}\}$$

with $|B| \geq cn^{k+1/2}(\log n)^{-1}$ such that any pair of elements in B are at distance at least n^{-k-1}.

Proof: By Prime Number Theorem we can find an integer n satisfying $N \leq n \leq 2N$ such that the interval $[n, n + n^{1/2}]$ contains more than $n^{1/2}/(4 \log n)$ primes. If $p, p + d$ are any pair of primes in $[n, n + n^{1/2}]$ and

$$\frac{a}{p^k} - \frac{b}{(p+d)^k} = \theta \quad |\theta| \leq n^{-k-1},$$

then

$$\frac{a+j}{p^k} - \frac{b+j}{(p+d)^k} = \theta + \frac{kjd}{p(p+d)^k} + O(jd^2 n^{-k-2}),$$

hence

$$|\frac{a+j}{p^k} - \frac{b+j}{(p+d)^k}| \geq n^{-k-1}$$

for $1 \leq j \leq c_1 n/d$, c_1 a certain constant. This implies

$$|\{1 \leq a \leq p^k : \exists\, b \in \mathbb{N}, |\frac{a}{p^k} - \frac{b}{(p+d)^k}| < n^{-k-1}\}| \ll |I| d n^{k-1}.$$

From this we infer the existence of a set B satisfying the conditions of the statement of the lemma. □

From this we obtain this result:

Theorem 1.48. *For any $r > 2$ there exists $D_r \subset E_r$ such that*

$$\beta_F(x) = \frac{\alpha - 1}{k} + \frac{1}{kr} \tag{1.49}$$

and with

$$1 + \frac{1}{2k} \leq \dim_{\mathrm{H}} D_r \leq 1 + \frac{1}{k}.$$

Proof: Let $1 \leq \alpha_1 < k$ and $k + 1/2 < \alpha_2 < k + 1$ such that $\alpha_1 \leq \alpha \leq \alpha_2$, and let

$$B(q) = \bigcup_{\substack{j \in \mathbb{N} \\ q^{-r-1} \leq 2^{-j} \leq q^{-1}}} B((\log q)^4, q, 2^{-j})$$

where $B((\log q)^4, q, 2^{-j})$ is set in the statement of Proposition 1.27. As in the proof of Theorem 1.46, taking into account that $\tau(a/p^k) = p^{k-1}$ holds for any $p > k$ and that $(\alpha - 1)/k + 1/(kr) < (\alpha - 1/2)/k$, we show that the points in

$$D_r = \{x \in E_r : q_n = p_n^k, p_n \text{ prime }, |\{a_n/q_n : a_n \in B(q_n)\}| < \infty\}$$

have the regularity given by (1.49). The upper bound for the dimension of D_r can be proved as Lemma 1.45. For the lower we observe that

$$D_r \supset \bigcap_{n=1}^{\infty} \bigcup_{p \geq n} \bigcup_{\substack{1 \leq a \leq p^k \\ a \notin B(p^k)}} I_r(a, p^k)$$

with $I_r(a, p^k)$ defined as in (1.42). Therefor we get $D_r^* \subset D_r$ with

$$D_r^* = \bigcap_{n=1}^{\infty} \bigcup_{n \leq p \leq n + n^{1/2}} \bigcup_{\substack{1 \leq a \leq p^k \\ a \notin B(p^k)}} I_r(a, p^k)$$

But $D_r^* = L_r \setminus \Delta$ with

$$L_r = \bigcap_{n=1}^{\infty} \bigcup_{n \leq p \leq n + n^{1/2}} \bigcup_{1 \leq a \leq p^k} I_r(a, p^k)$$

and

$$\Delta = \bigcap_{n=1}^{\infty} \bigcup_{n \leq p \leq n + n^{1/2}} \bigcup_{\substack{1 \leq a \leq p^k \\ a \in B(p^k)}} I_r(a, p^k)$$

In a simple way it can be showed that $\mathcal{H}^{(1+1/(2k))/r}(\Delta) = 0$. For the lower dimension of L_r, by using Lemma 1.47 we consider the set B_n described in its statement and build

$$G_j = \bigcap_{n=1}^{\infty} \bigcup_{a/p^k \in B_{n_j}} I_r(a, p^k)$$

with $n_j = n_{j-1}^j$. By Lemma 1.44 we infer

$$s_j \geq \frac{1 + 1/2k}{r}$$

for j sufficiently large and thus $\mathcal{H}^{(1+1/2k)/r}(L_r) > 0$. $\square$

Remark 1.49. In the same way as in the last two results we could show for any $1/k < v < 1/2$ and $r > k$ that there exists a subset of E_r of positive Hausdorff dimension whose points have Hölder exponent $(\alpha - 1)/k + v/r$.

We know that the subset of E_r approximated by fractions of type a/p^k has Minkowski dimension equal to $(1 + 1/k)/r$. We think this also happens for Hausdorff dimension, which could be proved obtaining the equivalent to Lemma 1.47 with p between n and $2n$. This result follows from the inequality

$$|\{(a, b, p, q) \in \mathbb{Z}^4 : |ap^k - bq^k| \leq N^\epsilon, |a|+|b|+|p|+|q| \leq N, (p, q) = 1\}| \ll N^{2-\epsilon}$$

for some $\epsilon > 0$; nevertheless we do not know to prove it. On the other hand, is natural to suppose that for any continuous integrable function f we have

$$\sum_{m \neq 0} \tau_m(\frac{a}{q}) f(\frac{m}{Y}) \ll Y^{\frac{1}{2}} q^{\frac{1}{2}+\epsilon}$$

for each rational a/q. From this would follow

$$d_{\mathrm{H}}(\beta) = (k + 1)(\beta - \frac{\alpha - 1}{k}) \qquad \beta \in [\frac{\alpha - 1}{k}, \frac{\alpha - 1/2}{k}).$$

Finally, if we think almost every point has Hölder exponent equal to $(\alpha - 1/2)/k$, we can conjecture this shape for the spectrum of singularities of F:

$$d_{\mathrm{H}}(\beta) = \begin{cases} 0 & \text{if } \beta = (\alpha - 1/2)/(k - 1) \\ 1 & \text{if } \beta = (\alpha - 1/2)/k \\ (k + 1)(\beta - (\alpha - 1)/k) & \text{if } (\alpha - 1)/k \leq \beta < (\alpha - 1/2)/k \\ -\infty & \text{otherwise.} \end{cases}$$

Chapter 2

Average measure of classes of quadratic forms

2.1 Introduction

For any $n \in \mathbb{Z}$ we define

$$P_n = \{ax^2+bxy+cy^2 : a,b,c \in \mathbb{Z}, (a,b,c) = 1, b^2-4ac = n, n < 0 \Rightarrow a > 0\}, \tag{2.1}$$

the space of primitive binary quadratic forms of discriminant n. The group $SL(2,\mathbb{Z})$ acts on this space in a natural way (by linear change of variable) and the set $SL(2,\mathbb{Z})\backslash P_n$, that can be equipped (such as Gauss showed) with a natural structure of abelian finite group, plays an important role in the comprehension of the forms and in the representation of numbers by them. In particular, a relevant quantity is its cardinal

$$h(n) = |SL(2,\mathbb{Z})\backslash P_n|,$$

the class number of forms of discriminant n.

In Art. 302 and Art. 304 of *Disquisitiones Arithmeticae* [Gau], Gauss considered the average for the class number when the discriminant varies (with the modern definition he restricted himself to the study of discriminants multiples of 4). In the first of those articles he treated the case of negative discriminants and saw that the class number grows in a regular way as the square root of the absolute value of the discriminant. In a precise way, he claimed to have obtained "through a theoretical investigation" an average formula that can be written as

$$\sum_{n\leq N} h(-4n) = \frac{4\pi}{21\zeta(3)}N^{3/2} - \frac{2}{\pi^2}N + E_2^-(N), \quad \text{with } E_2^-(N) = o(N). \tag{2.2}$$

It is plausible that Gauss proved this statement by using the interpretation of class number in terms of lattice points (Art. 172, Art. 174 [Gau]): $h(-n)$ equals the number of points in the set

$$\{(a,b,c) \in \mathbb{Z}^3 : b^2-4ac = -n, (a,b,c) = 1, -a < b \leq a < c \text{ or } 0 \leq b \leq a = c\} \tag{2.3}$$

In Art. 304 he investigated the case of positive discriminants. Gauss saw that class number behaves very irregularly, but he realized that by multiplying it by the logarithm of the fundamental unit the regularity was recovered, growing as the square root of the discriminant. Gauss wrote: "[...] the mean value of this product is approximately expressed by a formula of the type $m\sqrt{D} - n$. However, we are not yet been capable of determining the values of the constants m, n theoretically. If we are allowed to take some conclusion from the comparison of some hundreds of determinants, m seems to be very near $7/3$". The correct value of m was given by Gauss in one of its handwritten notes (see [Gau] p. 462), where says that the proof "illustrates brilliantly many parts of Higher Arithmetic and Analysis". The value he gives for m is $2\pi^2/(7\zeta(3))$, which is very near to the previously conjectured value ($2\pi^2/(7\zeta(3)) - 7/3 \approx 0.01$). We can write this statement in modern notation as

$$\sum_{n \leq N} h(4n) \log \epsilon_{4n} \sim \frac{4\pi^2}{21\zeta(3)} N^{3/2} \tag{2.4}$$

where $\epsilon_n = (t + u\sqrt{n})/2$, with (t,u) the smallest positive solution of Pell's equation $t^2 - nu^2 = 4$, whenever n is not a square. If it is a square, we define $\epsilon_n = 1$. Later this behaviour was understood through Dirichlet formula (see [Lan]) for the class number:

$$h(d) \log \epsilon_d = d^{\frac{1}{2}} L(1, \chi_d) \qquad \text{if } d > 0 \tag{2.5}$$

and

$$h(d) w_d^{-1} = (2\pi)^{-1} |d|^{\frac{1}{2}} L(1, \chi_d) \qquad \text{if } d < 0, \tag{2.6}$$

with $\chi_d(n) = (d/n)$ the Kronecker-Jacobi-Legendre symbol, and

$$w_d = \begin{cases} 2 & \text{if } d < -4 \\ 4 & \text{if } d = -4 \\ 6 & \text{if } d = -3 \end{cases} \tag{2.7}$$

the number of elements of $SL(2,\mathbb{Z})$ that fix a form of discriminant $d < 0$.

In 1863 Lipschitz [Lip] an later Mertens [Mer] obtained

$$\sum_{n \leq N} h(-4n) = \frac{4\pi}{21\zeta(3)} N^{3/2} + O(N \log N) \tag{2.8}$$

by using (2.3) and counting lattice points in a trivial way, which partially proved Gauss statement. However Gauss conjecture for negative discriminants had to wait until 1917, when I. M. Vinogradov [Vin1] proved $E_2^-(N) \ll N^{5/6}(\log N)^{2/3}$ through a more precise estimation of the number of lattice points. A year later [Vin2] he improved that result to $E_2^-(N) \ll N^{3/4}(\log N)^2$ by introducing Fourier Analysis into the problem through the formula

$$\{x\} = \frac{1}{2} - \frac{1}{\pi}\sum_{n=1}^{\infty}\frac{\sin(2\pi n x)}{n}.$$

Gauss statement for positive discriminants (2.4) was also demonstrated by Vinogradov [Vin3] in 1919. He used Dirichlet formula (2.5) and to bound the error term he had to control incomplete sums of characters, proving for that aim the important inequality

$$\sum_{n\leq x}\chi_d(n) \ll d^{\frac{1}{2}}\log d, \tag{2.9}$$

that was obtained at the same time and independently by G. Pólya [Pól]. With this, Vinogradov deduced

$$\sum_{n\leq N} h(4n)\log\epsilon_{4n} = \frac{4\pi^2}{21\zeta(3)}N^{3/2} + O(N\log N). \tag{2.10}$$

He also checked that (2.6) can be used to obtain (2.8), what surpassed that obtained by him before. Years later Vinogradov [Vin4, Vin5, Vin6] and J.-R. Chen [Che1, Che2] proved, by bounding certain trigonometric sums through van der Corput's method, that the error term $o(N)$ in formula (2.2) is actually $O(N^{2/3+\epsilon})$.

In 1944 C. L. Siegel [Sie] rediscovered the use of characters for this problem, proving (2.8) and (2.10). It seems that he had no knowledge of Vinogradov's papers, and in fact in his work he used Pólya's paper in order to bound short character sums. Anyway the important point for us is that Siegel also proved (2.10) in another way. In the case of negative discriminant, any form $ax^2+bxy+cy^2$ can be identified with the unique point in the hyperbolic plane $\mathfrak{H}$ solution of the equation $az^2+bz+c=0$. Besides, the action of $SL(2,\mathbb{Z})$ on the space of forms translates into the usual $SL(2,\mathbb{Z})$-action on $\mathfrak{H}$. In this way, the condition that the form (a,b,c) is in the set (2.3) is equivalent to z being in the fundamental domain (or in the left part of its boundary)

$$\mathcal{F} = \{x+iy : x^2+y^2 > 1, |x| < \frac{1}{2}\}. \tag{2.11}$$

When the discriminant is positive, $az^2 + bz + c = 0$ has two real roots $\rho_- < \rho_+$ which made Siegel to consider $\mathfrak{H}$ endowed with the hyperbolic metric $ds^2 = y^{-2}(dx^2 + dy^2)$, and to attach to $ax^2 + bxy + cy^2$ the geodesic g_{abc} containing the two points ρ_- and ρ_+ with an orientation given by the inequality $a(\rho_- - \rho_+) > 0$. Besides he associated to that form the quantity

$$\mu(a, b, c) = \ell(g_{abc} \cap \mathcal{F}),$$

the hyperbolic length of the arc formed by the intersection of g_{abc} with the fundamental domain.

If A is an arc determined by the points z_1 and z_2 in the geodesic going from ρ_- to ρ_+, then it is easy to calculate the expression

$$\ell(A) = \int_{\lambda_1}^{\lambda_2} \frac{d\lambda}{\lambda} = \log \frac{\lambda_2}{\lambda_1}, \tag{2.12}$$

where λ_j is the tangent of the argument of $z_j - \rho_-$.

In such a way, choosing a representant g_{abc} of a class, we deduce that the elements of $SL(2, \mathbb{Z})$ fixing g_{abc} act on the points of the geodesics. Since this group is generated by the element

$$\begin{pmatrix} (t - bu)/2 & -cu \\ au & (t + bu)/2 \end{pmatrix} \qquad \text{with } \epsilon_n = (t + u\sqrt{n})/2$$

we can take as fundamental domain an arc J, which by (2.12) has hyperbolic length $\log \epsilon_n^2$.

On one hand, for each point $z_0 \in J$ there exists a unique $f \in PSL(2, \mathbb{Z})$ such that $f(z_0) \in \mathcal{F}$, and thus $A_{z_0} = f(J) \cap \mathcal{F}$ is a non-empty arc. On the other hand, for each geodesic intersecting $\mathcal{F}$ there exists a unique element in $PSL(2, \mathbb{Z})$ that sends it to an arc contained in J. In that way, there are finitely many disjoint arcs whose union is J that are the only images by some element of $SL(2, \mathbb{Z})$ of geodesic arcs contained in $\mathcal{F}$. Summing over every class of discriminant $n > 0$ we have

$$h(n) \log \epsilon_n^2 = \sum_{\substack{(a,b,c) \in \mathbb{Z}^3 \\ (a,b,c)=1 \\ b^2-4ac=n}} \mu(a, b, c). \tag{2.13}$$

Taking into account that $\mu(\lambda a, \lambda b, \lambda c) = \mu(a, b, c)$ for every $\lambda \in \mathbb{R}^\times$, this formula allowed Siegel to control $\sum_{n \le x} h(n) \log \epsilon_n$ through the integral

$$\int_{0 < b^2 - 4ac < 1} \mu(a, b, c)\, da\, db\, dc.$$

The formula (2.13) is an equivalent of expression (2.3) for positive discriminants.

Siegel generalized this procedure to quadratic forms in more variables. For $n \in \mathbb{N}$ with $n \geq 2$ we consider the action of $GL(n,\mathbb{R})$ on the set $V^{(n)}$ of symmetric real n-dimensional matrices (namely, of quadratic forms with n variables) given by $(g,x) \mapsto gxg^t$. Let $GL(n,\mathbb{R})_x$ the isotropy group of $x \in V_{\mathbb{Q}}^{(n)} = V^{(n)} \cap M_n(\mathbb{Q})$ with respect to this action. Then we can consider in the subgroups $G_x = GL(n,\mathbb{R})_x \cap SL(n,\mathbb{R})$ and $\Gamma_x = G_x \cap SL(n,\mathbb{Z})$ the usual Haar measures (in the first group the one induced by the described action, and in the second the counting measure) that induce in the homogeneous space $H_x = G_x/\Gamma_x$ an invariant measure (see [Wei]). Let m_x such measure, then define

$$\nu(x) = m_x(H_x)$$

whenever H_x is compact. H_x is always compact except when $n = 2$ and x is a form that factors in product of two linear forms (that is to say when the discriminant is a square). In this last case Γ_x is finite and $m(H_x) = \infty$; we define $\nu(x) = 0$.

It can be checked that $\nu(x)$ does not change whenever x moves inside a class with respect to $SL(n,\mathbb{Z})$. In the case $n = 2$ we have $\nu(x) = 2w_d^{-1}$ if the discriminant is negative and $\nu(x) = \log \epsilon_d^2$ if it is positive. For $n > 2$, in general $\nu(x)$ changes for distinct classes but with the same discriminant, however it can be obtained (as Siegel did) the average formula

$$\sum_{\substack{x \in SL(n,\mathbb{Z})\backslash L_i \\ |\det x| < N}} \nu(x) = \frac{1}{n+1}\Big(\prod_{k=2}^{n} \zeta(k)\Big) N^{\frac{n+1}{2}} + O(N^{\frac{n}{2}}), \tag{2.14}$$

where L_i is the lattice of forms with integer coefficients and of signature i, $0 \leq i \leq n$. The way to proceed in order to prove it is the same used to achieve (2.13), relating any form with positive-definite forms and choosing the ones that intersect the Minkowski fundamental domain (see [Sie]).

This new interpretation of class number for positive discriminants opened the door for the full use of Fourier Analysis. This was carried in a precise way by T. Shintani [Shi]. M. Sato and T. Shintani [SS] developed in the seventies the concept of prehomogeneous vector space, attaching to it zeta functions satisfying a functional equation. In the particular case of quadratic forms, for $n \geq 3$ Shintani associated to any lattice L in $V_{\mathbb{Q}}^{(n)}$ invariant by the group $SL(n,\mathbb{Z})$ the zeta function

$$\xi_i^{(n)}(s,L) = \sum_{x \in SL(n,\mathbb{Z})\backslash L_i} \nu(x) |\det x|^{-s}, \tag{2.15}$$

where $L_i = L \cap V_i^{(n)}$ and $V_i^{(n)}$ the set of symmetric matrices of dimension n and signature i, that converges on $\Re s > (n+1)/2$ by (2.14). By using Fourier Analysis in the homogeneous space $V_i^{(n)} = GL(n,\mathbb{R})/GL(n,\mathbb{R})_x$ he proved that $\xi_i^{(n)}$ is a meromorphic function with possible poles at $s = (n+1-j)/2$ $(0 \leq j \leq n-1)$, and satisfying the functional equation

$$\xi_i^{(n)}(\frac{n+1}{2} - s, L) = v(L)^{-1} \sum_{j=0}^{n} u_{j,i}(s)\xi_j^{(n)}(s, L^*) \tag{2.16}$$

where $u_{ij}(s)$ are products of Γ and exponential functions, $v(L)$ is the volume of the fundamental parallelogram of the lattice L, and L^* is the dual lattice

$$L^* = \{x \in V^{(n)} : \mathrm{tr}(xy) \in \mathbb{Z}\, \forall y \in L\}.$$

The case $n = 2$ is anomalous due to $m(H_x) = \infty$ for factorable forms. This makes necessary a change of definition for the function $\xi_1^{(2)}$. In the case that L is the lattice

$$L = \{\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} : a, b, c \in \mathbb{Z}\},$$

L^* is the set of symmetric matrices with coefficients in $\mathbb{Z}$. In this case Shintani defined

$$\xi_1^{(2)}(s, L) = \sum_{x \in SL(2,\mathbb{Z})\backslash L_1} \nu(x) |\det x|^{-s} + 4^{s-1}B(s) \tag{2.17}$$

with $B(s) = \zeta(2s-1)(\zeta'(2s)\zeta(2s)^{-1} - \zeta'(2s-1)\zeta(2s-1)^{-1})$ and

$$\xi_1^{(2)}(s, L^*) = \sum_{x \in SL(2,\mathbb{Z})\backslash L_1^*} \nu(x) |\det x|^{-s} + \frac{B(s)}{2} + \frac{\log 2}{4}\frac{\zeta(2s-1)}{1-2^{-2s}}. \tag{2.18}$$

He proved that it is a meromorphic function with poles at $s = 1$ and $s = 3/2$ and satisfies the following functional equation

$$\xi_i^{(2)}(s)(\frac{3}{2} - s) = \sum_{j=0}^{2} u_{j,i}(s)\xi_j^{(2)}(s, L^*) + \chi_i(s), \tag{2.19}$$

for a certain simple function $\chi_i(s)$ that we shall specify later. By using a modification of a lemma of Landau he obtained the main terms for the sum of its coefficients from the poles of the function and in that way proved

$$\sum_{n \leq N} h(4n) \log \epsilon_{4n} = \frac{4\pi^2}{21\zeta(3)} N^{\frac{3}{2}} - \frac{4}{\pi^2} N(\log N + C') + E_2^+(N) \tag{2.20}$$

with $C' = -1 + (8/3)\log 2 + \log(2\pi) - \zeta'(2)\zeta(2)^{-1}$ and $E_2^+(N) \ll N^{\frac{3}{4}}$, what on one hand showed the failure of Gauss intuition for the second term, and on the other hand that the bound for the error term obtained by Vinogradov and Siegel was sharp. In the same way Shintani got a similar formula for the average of $h(n)\log\epsilon_n$.

The bound given by Chen and Vinogradov for E_2^- was not improved until F. Chamizo and H. Iwaniec [CI1, CI2] had the great idea of combining the two methods used before, Fourier Analysis and character sums. First they expressed the sum in terms of sums

$$\sum_{n\leq M} N_-(n) \tag{2.21}$$

where

$$N_-(n) = 2\sum_{k^2|n} h(-n/k^2)w^{-1}_{-n/k^2}, \tag{2.22}$$

which are the coefficients of one of Shintani's zeta functions. From this they divided the sum (2.21) as

$$\sum_{n\leq M} N_-(n) = \sum_{n\leq M+\Delta} N_-(n)g(n) - \sum_{M\leq n\leq M+\Delta} N_-(n)g(n)$$

with $\Delta \ll M^{1/2}$ and $g \in C_0^\infty((0,\infty))$ with $g = 1$ in $[1, M]$ an support contained in $(0, M+\Delta)$. Since Voronoi's work it was known that from a certain type of functional equations for zeta functions, summation formulas can be obtained. Chamizo and Iwaniec found that this could be done in the case of Shintani's zeta functions (from (2.19)), and in that way they treated the first sum. On the other hand, they transformed the second sum into a double sum of characters via Dirichlet's formula (2.6). The advantage is that for very short sums characters adapt better than exponentials, because we can enlarge the range of summation by using the multiplicativity of characters and Cauchy's inequality. To obtain the best result they used a precise estimation for double sums of real characters [HB1, HB2] due to Heath-Brown getting

$$|E_1^-(N)| + |E_2^-(N)| \ll N^{\frac{21}{32}+\epsilon} \qquad \text{for any } \epsilon > 0, \tag{2.23}$$

where $E_1^-(N)$ is the error term that is the equivalent of $E_2^-(N)$ when averaging over all discriminants.

In this chapter we shall study the case of positive discriminants, exposing the results obtained in [CU1] and [Ubi]. In order to bound E_1^+ and E_2^+ we shall follow Chamizo and Iwaniec by using Siegel's interpretation (2.13) of the class number. We shall also study the behaviour of the error terms in quadratic average.

In the first section we use Shintani's functional equations in order to obtain summation formulas for the coefficients, through the use of Mellin transform.

In the second, we shall see how Siegel's interpretation of class number for positive discriminants in terms of lengths of geodesic arcs allows us to control the exponential sums that appear in the summation formulas.

In the third, by using the previous sections and the result for character sums in [HB2] we obtain:

Theorem 2.1. *For any $\alpha > 21/32$ we have $E_1^+(N) \ll N^\alpha$, where*

$$\sum_{n\leq N} h(n)\log\epsilon_n = \frac{\pi^2}{18\zeta(3)}N^{3/2} - \frac{3}{\pi^2}(C+\log N)N + E_1^+(N)$$

and $C = \log(2\pi) - \zeta'(2)/\zeta(2) - 1$.

In the same way we achieve this related result.

Theorem 2.2. *For any $\alpha > 21/32$ we have $E_2^+(N) \ll N^\alpha$, where*

$$\sum_{n\leq N} h(4n)\log\epsilon_{4n} = \frac{4\pi^2}{21\zeta(3)}N^{3/2} - \frac{4}{\pi^2}(C'+\log N)N + E_2^+(N)$$

and $C' = \log(2\pi) + 8(\log 2)/3 - \zeta'(2)/\zeta(2) - 1$.

In general, this procedure could be applied to the study of the average of $h(n)\log\epsilon_n$ and $h(-n)$ over any arithmetic progression. This could permit to prove in another way the formula obtained in [GH] for the average over fundamental discriminants, namely averaging over quadratic fields. This could also be extended to improve the bound for the error term in (2.14), namely in the case of general quadratic forms.

In the last section we shall study the behaviour of error terms. It is known [Cho, GS] that

$$L(1,\chi_d) \geq e^\gamma(\log\log|d| - 10) \tag{2.24}$$

for infinitely many discriminants. By (2.5) and (2.6) we deduce that $E_1^+(n) = \Omega(\sqrt{d}\log\log d)$ and the same for the rest of error terms. On the other hand, from the summation formulas obtained in [CI2] (and the ones obtained in the first section) we shall infer a representation for the error term in the average of $N_-(n)$ (and of $N_+(n)$) in terms of exponential sums. This has been used [Küh] (cf. [Tsa]) to study the L^2-norm of the error terms, deducing that they are $\Omega_\pm((n\log n)^{1/2})$. In order to apply that method to the study of $E_j^+(N)$ first Möbius inversion formula must be used to transform $N_+(n)$ into sums

of $h(n)\log\epsilon_n$. But if now we want to find the L^2-norm of this expression, it seems difficult to control the non-diagonal terms. What can be done (see [Pet]) is to introduce absolute values getting the bound

$$(\sum_{N\leq x}|E_j^+(N)|^2)^{\frac{1}{2}} \ll x^{\frac{1}{2}}(\log x)^{\frac{3}{2}}. \tag{2.25}$$

Instead of following that path, we shall use Dirichlet's formula (2.5) and work with character sums in order to achieve this result.

Theorem 2.3. *For any $K \ll x^{\frac{1}{4}-\epsilon}$ we have*

$$\sum_{N\leq x}|E_2^+(N+K)-E_2^+(N)|^2 = (\frac{3P}{4\pi})^2x^2\log K + O(x^2(\log K)^{\frac{2}{3}}),$$

with

$$P=\prod_{p\neq 2}(1-\frac{1}{p^2(p+1)}).$$

From this result we deduce that

$$E_2^+(N)=\Omega((N\log N)^{\frac{1}{2}}),$$

but moreover E_2^+ is an oscillating function, because we know that the average $\sum_{n<x}E_2^+(N)$ is small. We can prove the same things for $E_j^{\pm}(N)$.

It is natural to ask if we have an asymptotic formula for the average of class number in the case of positive discriminants. In this case the behaviour is much more irregular (as Gauss noticed), mainly influenced through (2.5) by the chaotic distribution of the fundamental solution of Pell's equation. It is not even known the existence of infinitely many quadratic fields with class number one, that corresponds to unique factorization domains, the so called Gauss-Hasse conjecture. In 1984 C. Hooley [Hoo] obtained

$$\sum_{\substack{n\leq x\\ \epsilon_n\leq n^{1/2+\alpha}}} 1 \sim \frac{4\alpha^2}{\pi^2}x^{\frac{1}{2}}(\log x)^2 \tag{2.26}$$

in the range $0\leq\alpha\leq 1/2$, whence we deduce

$$\sum_{\substack{n\leq x\\ \epsilon_n\leq n^{1/2+\alpha}}} h(n) \sim \frac{4}{\pi^2}(2\alpha-\log(1+2\alpha))x\log x.$$

Besides, by heuristical arguments regarding the distribution of ϵ_n he arrived at the conjecture

$$\sum_{n\leq x} h(n) \sim \frac{25}{12\pi^2} x(\log x)^2.$$

On the other hand, P. Sarnak [Sar] has obtained, as a consequence of Selberg's trace formula, a formula when averaging according to the size of the discriminant

$$\sum_{\epsilon_n\leq x} h(n) = \mathrm{Li}(x^2) + O(x^{\frac{3}{2}}(\log x)^2).$$

2.2 Summation formulas

Voronoi [Vor1, Vor2] used the functional equation of $\zeta(s)^2 = \sum_{n=1}^{\infty} d(n)n^{-s}$, where $\zeta(s)$ is Riemann zeta function, in order to obtain a formula for the average of the divisor function. From that moment, it has been understood [CR] that in certain contexts a functional equation for a Dirichlet series is equivalent to a summation formula for its coefficients. Shintani's zeta functions are going to have as coefficients the numbers $N_+(n)$ y $N_-(n)$, where $N_-(n)$ is defined by (2.22) and

$$N_+(n) = \sum_{k^2|n} h(n/k^2)\log\epsilon_{n/k^2}.$$

In this way, from the functional equation we shall get summation formulas for this quantities. With those formulas we can recover the average for $h(-n)$ and $h(n)\log\epsilon_n$ from the following Möbius inversion formula:

Lemma 2.4. *If $n \geq 1$ then*

$$h(n)\log\epsilon_n = \sum_{k^2|n} \mu(k) N_+(n/k^2)$$

and

$$h(4n)\log\epsilon_{4n} = \sum_{\substack{k^2|n \\ 2\nmid k}} \mu(k)\big(N_+(4n/k^2) - N_+(n/k^2)\big).$$

Proof: The first formula is obvious. For the second we notice that

$$\begin{aligned} h(4n)\log\epsilon_{4n} &= \sum_{k^2|4n} \mu(k)N_+(4n/k^2) = \sum_{2\nmid k} + \sum_{2|k} \\ &= \sum_{\substack{k^2|n \\ 2\nmid k}} \mu(k)N_+(4n/k^2) + \sum_{k^2|n} \mu(2k)N_+(n/k^2) \end{aligned}$$

and the result follows since $\mu(2k) = -\mu(k)$ for k odd and $\mu(2k) = 0$ for k even. □

In order to make the exposition easier we are going to change notation with respect to Shintani. In the half-plane $\Re s > 2$ define

$$\xi_2^-(s) = \sum_{n=1}^{\infty} \frac{N_-(4n)}{\sqrt{4n}}(\sqrt{4n})^{-s} \qquad \xi_1^-(s) = \sum_{n=1}^{\infty} \frac{N_-(n)}{\sqrt{n}}(\sqrt{n})^{-s}$$

$$\xi_1^+(s) = \sum_{n=1}^{\infty} \frac{N_+(n)}{\sqrt{n}}(\sqrt{n})^{-s} + \zeta(s)\left(\frac{\zeta'(s+1)}{\zeta(s+1)} - \frac{\zeta'(s)}{\zeta(s)}\right)$$

$$\xi_2^+(s) = \sum_{n=1}^{\infty} \frac{N_+(4n)}{\sqrt{4n}}(\sqrt{4n})^{-s} + 2^{-s}\zeta(s)\left(\frac{\zeta'(s+1)}{\zeta(s+1)} - \frac{\zeta'(s)}{\zeta(s)}\right) + \frac{\zeta(s)\log 2}{2^{s+1}-1}.$$

The relation with Shintani's zeta functions is

$$\begin{aligned}
\xi_1^{(2)}(s, L^*) &= \zeta(2)^{-1}\xi_2^+(2s-1) + c_1 2^{1-2s}\zeta(2s-1) \\
\xi_1^{(2)}(s, L) &= \zeta(2)^{-1}\xi_1^+(2s-1) + c_1\zeta(2s-1) \\
\xi_2^{(2)}(s, L^*) &= \zeta(2)^{-1}\pi\xi_2^-(2s-1) \\
\xi_2^{(2)}(s, L) &= \zeta(2)^{-1}\pi\xi_1^-(2s-1),
\end{aligned}$$

where c_1 is the residue of $\zeta(s)^2/\zeta(2s)$ at $s = 1$. Then, writing

$$\vec{z}_2(s) = \begin{pmatrix} \xi_2^+(s) \\ \xi_2^-(s) \end{pmatrix} \qquad \text{y} \qquad \vec{z}_1(s) = \begin{pmatrix} \xi_1^+(s) \\ \xi_1^-(s) \end{pmatrix}$$

we can set Shintani's functional equations (Theorem 2 in [Shi]) in the shape

Theorem 2.5. *Each component in the vectors*

$$\vec{z}_2(s) - \frac{1}{s-2}\begin{pmatrix} \pi^2/12 \\ \pi/12 \end{pmatrix} + \frac{1}{(s-1)^2}\begin{pmatrix} 1/2 \\ 0 \end{pmatrix} + \frac{1}{s-1}\begin{pmatrix} \log(2\pi)/2 \\ 1/4 \end{pmatrix}$$

and

$$\vec{z}_1(s) - \frac{1}{s-2}\begin{pmatrix} \pi^2/6 \\ \pi/6 \end{pmatrix} + \frac{1}{(s-1)^2}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{s-1}\begin{pmatrix} \log(2\pi) \\ 1/2 \end{pmatrix}$$

has an order 1 entire continuation to the complex plane. Moreover we have

$$\vec{z}_1(1-s) = (2\pi)^{-s}\Gamma(s)(\mathcal{A}(s)\vec{z}_2(s) - \cos(\pi s/2)\zeta(s)\vec{B}(s)).$$

where

$$\mathcal{A}(s) = 2^{s+1}\begin{pmatrix} \cos(\pi s/2) & \pi \\ 0 & -\sin(\pi s/2) \end{pmatrix}, \quad \vec{B}(s) = \begin{pmatrix} \psi(s/2) - \psi((s+1)/2) \\ \sec(\pi s/2) \end{pmatrix}$$

with $\psi(s) = \Gamma'(s)/\Gamma(s)$.

Let us see in which summation formulas these functional equations can be transformed. Defining α_n and β_n as the coefficients of Dirichlet series

$$\zeta(s)\left(\frac{\zeta'(s+1)}{\zeta(s+1)}-\frac{\zeta'(s)}{\zeta(s)}\right)$$

and

$$2^{-s}\zeta(s)\left(\frac{\zeta'(s+1)}{\zeta(s+1)}-\frac{\zeta'(s)}{\zeta(s)}\right)+\frac{\zeta(s)\log 2}{2^{s+1}-1}$$

respectively, we can express our main result as

Proposition 2.6. *Let $g\in C_0^\infty\big((0,\infty)\big)$. Then*

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{N_+(n)}{\sqrt{n}}g(\sqrt{n}) &= \frac{\pi^2}{6}\int_0^\infty tg(t)\,dt-\int_0^\infty g(t)\log(2\pi t)\,dt-\sum_{n=1}^{\infty}g(n)\log n\\ &+\sum_{d=1}^{\infty}\frac{\Lambda(d)}{d}\sum_{n=1}^{\infty}g(dn)+2\sum_{n=1}^{\infty}\frac{N_+(4n)}{\sqrt{4n}}\widetilde{g}(\sqrt{4n})+2\sum_{n=1}^{\infty}\beta_n\widetilde{g}(n)\\ &+2\pi\sum_{n=1}^{\infty}\frac{N_-(4n)}{\sqrt{4n}}\int_0^\infty g(t)e^{-\pi\sqrt{4n}t}\,dt+2\int_0^1\frac{1}{t(1+t)}\sum_{n=1}^{\infty}\widetilde{g}(2n/t)\,dt\end{aligned}$$

where $\widetilde{g}$ is the Cosine Fourier transform $\int g(t)\cos(\pi xt)\,dt$.

Proof: The summation formula of the statement is equivalent to

$$\begin{aligned}\sum_{n=1}^{\infty}b_{1n}^+g(\sqrt{n}) &= \frac{\pi^2}{6}\int_0^\infty tg(t)\,dt-\int_0^\infty g(t)\log(2\pi t)\,dt+2\sum_{n=1}^{\infty}b_{2n}^+\widetilde{g}(\sqrt{n})\\ &+ 2\pi\sum_{n=1}^{\infty}b_{2n}^-\int_0^\infty g(t)e^{-\pi\sqrt{n}t}\,dt+2\int_0^1\frac{1}{t(1+t)}\sum_{n=1}^{\infty}\widetilde{g}(2n/t)\,dt\end{aligned}$$

where b_{in}^+ and b_{in}^- are defined by setting $\xi_i^+(s)=\sum b_{in}^+(\sqrt{n})^{-s}$ y $\xi_i^-(s)=\sum b_{in}^-(\sqrt{n})^{-s}$. By Mellin inversion formula we have

$$\sum_{n=1}^{\infty}b_{1n}^+g(\sqrt{n})=\frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty}\mathcal{M}_g(s)\xi_1^+(s)ds$$

with $2<\sigma<3$ and $\mathcal{M}_g(s)$ the Mellin transform of g. By Theorem 2.5 we have

$$\xi_1^+(1-s)=\pi^{-s}\Gamma(s)\big(2\pi\xi_2^-(s)+2\cos(\frac{\pi}{2}s)\xi_2^+(s)-2^{-s}\cos(\frac{\pi}{2}s)B_1(s)\zeta(s)\big) \tag{2.27}$$

where B_1 is the first component of $\vec{B}$. This equation assures (by convexity) that $\xi_1^+(s)$ grows as a polynomial on vertical lines, hence by the decay of $\mathcal{M}_g(s)$ we can move integration line to $-2 < \sigma' < -1$. In this way, by Residue Theorem and taking into account the poles of the functions involved (see Theorem 2.5) we deduce that

$$\begin{aligned}\sum_{n=1}^{\infty} b_{1n}^+ g(\sqrt{n}) &= \frac{1}{2\pi i}\int_{\sigma'-i\infty}^{\sigma'+i\infty} \mathcal{M}_g(s)\xi_1^+(s)\,ds + \frac{\pi^2}{6}\mathcal{M}_g(2) \\ &\quad -\mathcal{M}_g'(1) - \log(2\pi)\mathcal{M}_g(1).\end{aligned}$$

Besides, by (2.27)

$$\frac{1}{2\pi i}\int_{\sigma'-i\infty}^{\sigma'+i\infty} \mathcal{M}_g(s)\xi_1^+(s)ds = I_1 + I_2 + I_3$$

where

$$\begin{aligned}I_1 &= 2\pi\frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} \mathcal{M}_g(1-s)\pi^{-s}\Gamma(s)\xi_2^-(s)\,ds \\ I_2 &= 2\frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} \mathcal{M}_g(1-s)\pi^{-s}\Gamma(s)\cos(\frac{\pi}{2}s)\xi_2^+(s)\,ds \\ I_3 &= -\frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} \mathcal{M}_g(1-s)(2\pi)^{-s}\Gamma(s)\cos(\frac{\pi}{2}s)B_1(s)\zeta(s)ds\end{aligned}$$

By using the expansion as Dirichlet series of $\xi_2^+(s)$ and moving the integration line to $0 < \sigma'' < 1$ we obtain

$$I_2 = 2\sum_{n=1}^{\infty} b_{2n}^+ \frac{1}{2\pi i}\int_{\sigma''-i\infty}^{\sigma''+i\infty} \mathcal{M}_g(1-s)(\pi\sqrt{n})^{-s}\Gamma(s)\cos(\frac{\pi}{2}s)\,ds.$$

In this area we have the representation $\Gamma(s)\cos(\pi s/2) = \int_0^{\infty} t^{s-1}\cos t\ dt$, [GR] 17.43.3, hence

$$I_2 = 2\sum_{n=1}^{\infty} b_{2n}^+ \int_0^{\infty} \frac{1}{2\pi i}\int_{\sigma''-i\infty}^{\sigma''+i\infty} \mathcal{M}_g(1-s)t^{s-1}\,ds\cos(\pi\sqrt{n}t)\,dt$$

and by Mellin inversion formula follows

$$I_2 = 2\sum_{n=1}^{\infty} b_{2n}^+ \widetilde{g}(\sqrt{n}).$$

In the same way we obtain

$$I_1 = 2\pi \sum_{n=1}^{\infty} b_{2n}^{-} \int_0^{\infty} g(t) e^{-\pi t\sqrt{n}}\, dt.$$

On the other hand, by the formula

$$B_1(s) = -2 \int_0^1 \frac{x^s}{1+x} \frac{dx}{x}$$

in $\Re s > 0$ (see [GR] 8.371.1), we can write

$$I_3 = 2 \int_0^1 \frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} \mathcal{M}_g(1-s)(2\pi x^{-1})^{-s}\Gamma(s)\cos(\frac{\pi}{2}s)\zeta(s)\, ds\, \frac{1}{1+x}\frac{dx}{x},$$

and expanding ζ as Dirichlet series we arrive at

$$I_3 = 2 \int_0^1 \sum_{n=1}^{\infty} \widetilde{g}(2nx^{-1}) \frac{1}{1+x}\frac{dx}{x},$$

proceeding as in the case of I_2. □

The dual summation formula is the following:

Proposition 2.7. *Let $g \in C_0^{\infty}\big((0,\infty)\big)$. Then*

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{N_+(4n)}{\sqrt{4n}} g(\sqrt{4n}) &= \frac{\pi^2}{12}\int_0^{\infty} t g(t)\, dt - \frac{1}{2}\int_0^{\infty} g(t)\log(2\pi t)\, dt - \sum_{n=1}^{\infty} g(2n)\log n \\ &+ \sum_{d=1}^{\infty}\frac{\Lambda(d)}{d}\sum_{n=1}^{\infty} g(2dn) - \log 2 \sum_{k=1}^{\infty} 2^{-k}\sum_{n=1}^{\infty} g(2^k n) + \sum_{n=1}^{\infty}\frac{N_+(n)}{\sqrt{n}}\widetilde{g}(\sqrt{n}) \\ &+ \sum_{n=1}^{\infty}\alpha_n \widetilde{g}(n) + \pi\sum_{n=1}^{\infty}\frac{N_-(n)}{\sqrt{n}}\int_0^{\infty} g(t) e^{-\pi\sqrt{n}t}\, dt - \int_0^1 \frac{1}{t(1+t)}\sum_{n=1}^{\infty}\widetilde{g}(n/t)\, dt\end{aligned}$$

Proof: We proceed as in the proof of the previous proposition, but starting from the functional equation

$$\xi_2^+(1-s) = \pi^{-s}\Gamma(s)\big(\pi\xi_1^-(s) + \cos(\frac{\pi}{2}s)\xi_1^+(s) - \frac{1}{2}\cos(\frac{\pi}{2}s)B_1(s)\zeta(s)\big),$$

which can be deduced from Theorem 2.5 by equation

$$B_1(1-s) + B_1(s) = -2\pi\csc(\pi s).$$

□

2.3 Exponential sums

We have just seen that in summation formulas of Propositions 2.6 and 2.7 appear certain main terms and some oscillatory ones which depend on sums of the kind

$$\sum N_+(n)e(R\sqrt{n}) \qquad \text{y} \qquad \sum N_+(4n)e(R\sqrt{n})$$

with R a certain parameter. In order to treat this formula we shall write $N_+(n)$ as a sum over lattice points. To this end we use the quantity defined in the introduction

$$\mu(a,b,c) = \ell(g_{abc} \cap \mathcal{F})$$

where g_{abc} is the geodesic defined by equation $a(x^2+y^2)+bx+c=0$, $y>0$. Adding (2.13) for every $k^2 \mid n$ and taking into account that $\mu(\lambda a, \lambda b, \lambda c) = \mu(a,b,c)$ we obtain this basic lemma.

Lemma 2.8. *Let $n \in \mathbb{Z}^+$ not a square. Then*

$$N_+(n) = \sum_{\substack{b^2-4ac=n \\ a>0}} \mu(a,b,c).$$

It is easy to check in this sum there are only a finite number of non-vanishing terms. These can be described into a explicit way.

Lemma 2.9. *Let $ax^2+bxy+cy^2$, $a>0$, with discriminant n not a square. Then $\mu(a,b,c) \neq 0$ if and only if $a+c<|b|/2$. Besides, if $\mu(a,b,c)\neq 0$ then $a \leq \sqrt{n/3}$, $|b| \leq 2\sqrt{n/3}$ and $a|c| \leq n/4$.*

Proof: The first part of the lemma follows noticing that the geodesic g_{abc} has non-empty intersection with the fundamental domain $\mathcal{F}$ if and only if some of the points $(\pm 1 + i\sqrt{3})/2$ is below g_{abc}. The inequalities are obtained from the identity

$$\frac{1}{4}(4a-|b|)^2 + \frac{3}{4}b^2 = n + 4a(a+c-\frac{1}{2}|b|).$$

□

Our aim is to bound $\sum N_+(n)e(R\sqrt{n})$ as in [CI1]. It will be possible because, although in some ranges the derivative of $\mu(a,b,c)$ is going to be large, by splitting the domain of values (a,b,c) into three parts, according to the geometrical situation of the geodesic g_{abc}, the function $\mu(a,b,c)$ is the logarithm of an algebraic function in each part.

Proposition 2.10. *For $R > 1/2$ and $1 \le M < M' \le 2M$ we have*

$$\sum_{M\le n<M'} N_+(n)e(R\sqrt{n}) \ll M^{5/4+\epsilon} + (RM)^\epsilon L$$

with

$$L = \min\big(R^{3/8}M^{15/16} + R^{1/8}M^{17/16}, R^{7/24}M^{49/48} + R^{5/24}M^{53/48}\big),$$

and a similar result holds if $N_+(n)$ is substituted by $N_+(4n)$.

Proof: By Lemmas 2.8 and 2.9 we can write

$$\sum_{M\le n<M'} N_+(n)e(R\sqrt{n}) = \sum_{\substack{a+c<|b|/2\\ b^2-4ac\neq\square}} \mu(a,b,c)E(b^2-4ac) \tag{2.28}$$

where

$$E(n) = \begin{cases} e(R\sqrt{n}) & \text{if } M \le n < M' \\ 0 & \text{otherwise} \end{cases}$$

We consider the set

$$\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2 \cup \mathcal{M}_3$$

where the disjoint sets $\mathcal{M}_j$ are defined by

$$\begin{aligned} \mathcal{M}_1 &= \{(a,b,c)\in\mathbb{Z}^3 \,:\, |a+c| < -b/2,\ a>0,\ c\neq 0\} \\ \mathcal{M}_2 &= \{(a,b,c)\in\mathbb{Z}^3 \,:\, a+c \le b/2 \le -a-c,\ a>0,\ c\neq 0\} \\ \mathcal{M}_3 &= \{(a,b,c)\in\mathbb{Z}^3 \,:\, |a+c| < b/2,\ a>0,\ c\neq 0\}. \end{aligned}$$

Vertices $1/2 + i\sqrt{3}/2$ and $-1/2 + i\sqrt{3}/2$ of $\mathcal{F}$ are in the circle determined by g_{abc} if and only if $(a,b,c)\in\mathcal{M}_2$; in the same way, only the first vertex or the second are in the circle are in the circle if and only if $(a,b,c)\in\mathcal{M}_1$ or $(a,b,c)\in\mathcal{M}_3$, respectively. Thus in $\mathcal{M}$ are covered each geometrical possibility such that $\mu(a,b,c)\neq 0$.

By (2.12), in each $\mathcal{M}_i$ the function $\mu = \mu(a,b,c)$ is the logarithm of an algebraic function, and besides $\mu(a,b,c) = O(\log M)$ for $M \le b^2-4ac < 2M$.

Note that $\mu(a,b,c)$ is well defined as $\ell(g_{abc}\cap\mathcal{F})$ also when b^2-4ac is a square. On the other hand the number of elements in the set

$$\{(a,b,c) \,:\, b^2-4ac = h^2,\ M\le h^2 < 2M,\ a+c<|b|/2,\ a>0,\ c\neq 0\}$$

is $O(M^{1+\epsilon})$. Hence by (2.28) we infer

$$\begin{aligned} \sum_{M\le n<M'} N_+(n)e(R\sqrt{n}) &\ll M^{1+\epsilon} + \sum_{(a,b,c)\in\mathcal{M}} \mu(a,b,c)E(b^2-4ac) \\ &\ll M^{1+\epsilon} + \sum_{(a,b,c)\in\mathcal{M}_i} \mu(a,b,c)E(b^2-4ac) \end{aligned}$$

for some $i \in \{1,2,3\}$.

Let us fix a, c and consider $\mu(a,b,c)$ as a function on b. Since e^μ is an algebraic function in $\mathcal{M}_i$ has an uniformly bounded number of maximums and minimums. So given a, c we can write $\{b \ : \ (a,b,c) \in \mathcal{M}_i\}$ as a finite union of intervals I_j in which $\mu(a,\cdot,c)$ is monotone. The bound $\mu(a,b,c) \ll \log M$ and summation by parts give

$$\sum_{(a,b,c)\in\mathcal{M}_i} \mu(a,b,c)E(b^2-4ac) \ll M^\epsilon \sum_{a,c} \Big| \sum_{b\in I_j'} E(b^2-4ac)\Big|,$$

where the interval $I_j' \subset I_j$ depends on a, c and will be void if $(a,b,c) \notin \mathcal{M}_i$ for every b. Lemma 2.9 assures that $a|c| \leq M/2$ and $|b| \leq 2\sqrt{M}$, hence by Lemma 7.3 in [GK] applied to $[-2\sqrt{M}, 2\sqrt{M}]$ and making the change $n = 4a|c|$ we deduce that

$$\sum_{a,c} \Big| \sum_{b\in I_j'} E(b^2-4ac)\Big| \ll M^\epsilon \sum_{n\leq 2M} \Big| \sum_{|b|\leq 2\sqrt{M}} e(\theta b)E(b^2-n)\Big| \tag{2.29}$$

for some $\theta \in \mathbb{R}$.

Now we follow the arguments exposed in Lemma 4.1 in [CI2]. We divide the range of b in M^ϵ intervals of length $O(M^{1/2-\epsilon})$. If J is one of those intervals, by Cauchy's inequality we obtain

$$\Big(\sum_{n\leq 2M} \Big| \sum_{b\in J} e(\theta b)E(b^2-n)\Big|\Big)^2 \ll M\Big(M^{3/2} + \sum_{|b_1|<|b_2|} |\sum_n E(b_1^2-n)\overline{E(b_2^2-n)}|\Big).$$

Writing $u = b_1^2 - n$, the last double sum is

$$\sum_{|b_1|<|b_2|} \Big| \sum_{M\leq u\leq M'+b_1^2-b_2^2} e\big(R(\sqrt{u} - \sqrt{u+b_2^2-b_1^2})\big)\Big| \ll$$

$$\ll M^\epsilon \sum_{v\asymp D} \Big| \sum_{u\asymp M} e(R(\sqrt{u}-\sqrt{u+v}))\Big|$$

for some $D = o(M)$, where we have employed that the number of representations of v as $b_2^2 - b_1^2$ is $O(M^\epsilon)$ and $b_2^2 - b_1^2 = o(M)$ because $|J| = o(M^{1/2})$.

From all of this we finally obtain

$$\sum_{M\leq n<M'} N_+(n)e(R\sqrt{n}) \ll M^{5/4+\epsilon} + M^{1/2+\epsilon}\Big(\sum_{v\asymp D} \Big| \sum_{u\asymp M} e(R(\sqrt{u}-\sqrt{u+v}))\Big|\Big)^{\frac{1}{2}}$$

This sum was bounded in Lemma 3.1 of [CI1], giving the expected result.

The proof in the case of $N_+(4n)$ is similar, taking into account that $4|b^2 - 4ac$ is equivalent to $2|b$ and $2\sum_{2|b} f(b) = \sum_b f(b) + \sum_b e(b/2)f(b)$, hence the phase $b/2$ can be accumulated to θb in (2.29). $\square$

2.4 Bound for the error term

Now we shall proceed as in [CI2] and [CI1]. We write the sum as

$$\sum_{n\leq N} N_+(n) = \sum_{\sqrt{n}\leq N^{1/2}+\Delta} \frac{N_+(n)}{\sqrt{n}} g(\sqrt{n}) - \sum_{N^{1/2}\leq\sqrt{n}\leq N^{1/2}+\Delta} \frac{N_+(n)}{\sqrt{n}} g(\sqrt{n}), \tag{2.30}$$

with $\Delta > 0$, and $g : [0,\infty] \longrightarrow \mathbb{R}$ the function defined by

$$g(x) = \begin{cases} \int_0^x \eta(u)\, du & \text{if } x \leq 1 \\ x & \text{if } 1 \leq x \leq N^{1/2} \\ N^{1/2}\Delta^{-1}(N^{1/2}+\Delta-x) & \text{if } N^{1/2} \leq x \leq N^{1/2}+\Delta \\ 0 & \text{if } x \geq N^{1/2}+\Delta, \end{cases}$$

$\eta \in C_0^\infty\big((1/2,1)\big)$ with $\int_0^1 \eta = 1$. Note that $g \in C_0\big((0,\infty)\big)$ and is differentiable except at finitely many points.

Proposition 2.11. *If $N^{-1/2} < \Delta \leq N^{-1/4} < 1$ then*

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{N_+(n)}{\sqrt{n}} g(\sqrt{n}) &= \frac{\pi^2}{18} N^{\frac{3}{2}} + \frac{\pi^2 N\Delta}{12} - \frac{N}{2}\log N + \big(1 - \frac{\zeta'(2)}{\zeta(2)} - \log(2\pi)\big)\frac{N}{2} \\ &+ O(N^{\frac{21}{32}+\epsilon} + N^{\frac{1}{2}+\epsilon}\Delta^{-\frac{1}{2}} + N^{\frac{11}{16}+\epsilon}\Delta^{\frac{1}{8}}) \end{aligned}$$

and

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{N_+(4n)}{\sqrt{4n}} g(\sqrt{4n}) &= \frac{\pi^2}{36} N^{\frac{3}{2}} + \frac{\pi^2 N\Delta}{24} + \big(1 - \frac{\zeta'(2)}{\zeta(2)} + \frac{\log 2}{3} - \log(2\pi)\big)\frac{N}{4} \\ &- \frac{N}{4}\log N + O(N^{\frac{21}{32}+\epsilon} + N^{\frac{1}{2}+\epsilon}\Delta^{-\frac{1}{2}} + N^{\frac{11}{16}+\epsilon}\Delta^{\frac{1}{8}}) \end{aligned}$$

Remark 2.12. With the only use of this proposition we can improve Shintani's result: choosing $\Delta = N^{-1/3}$ we realize that error term in the smoothed sum is $O(N^{2/3+\epsilon})$, and subtracting the same result changing $N^{1/2}$ by $N^{1/2}-\Delta$ we see that the contribution of the terms with $N^{1/2} \leq \sqrt{n} \leq N^{1/2}+\Delta$ is absorb by this bound.

Proof: We shall restrict firs to the proof of the first formula and after we shall point out the necessary change for the second.

For any $x > 0$ we have

$$\widetilde{g}(x) = \frac{\cos(\pi N^{\frac{1}{2}} x) - \cos(\pi x) - \phi(x)}{\pi^2 x^2} + \frac{2N^{\frac{1}{2}}}{\pi^2 x^2 \Delta} \sin(\frac{\pi}{2}\Delta x) \sin\big(\frac{\pi}{2}(2N^{\frac{1}{2}} + \Delta)x\big) \tag{2.31}$$

where $\phi(x) = \pi x \int \eta(t) \sin(\pi x t)\, dt$. We have $\phi(x) = O(x^{-\alpha})$ for any $\alpha > 0$.

Let $\tau \in C_0^\infty((-1/2, 1/2))$ even, with $\int \tau = 1$, and $\tau_m(x) = m\tau(mx)$ for every $m \in \mathbb{N}$. Defining $g_m = g * \tau_m$ we have $g_m \in C_0^\infty((0,\infty))$ and $\widetilde{g_m}(x) = \widetilde{g}(x)\widehat{\tau}(x/2m)$ converge uniformly to g and $\widetilde{g}$. Moreover by Proposition 2.10 we find that the sum $\sum N_+(n)\widetilde{g}(\sqrt{n})/\sqrt{n}$ converges, and by Abel's Lemma $\sum_n N_+(n)\widetilde{g_m}(\sqrt{n})/\sqrt{n}$ converges uniformly in m. All of this justifies the application of Proposition 2.6 to the function g.

In the considered range for Δ we have

$$\frac{\pi^2}{6} \int_0^\infty t g(t)\, dt = \frac{\pi^2}{18} N^{3/2} + \frac{\pi^2 N\Delta}{12} + O(1).$$

On the other hand

$$\int_0^\infty g(t) \log(2\pi t)\, dt = \frac{N}{4}\log N + \big(2\log(2\pi) - 1\big)\frac{N}{4} + O(N^{1/2+\epsilon})$$

and by partial summation

$$\sum_{n=1}^\infty g(n)\log n - \sum_{d=1}^\infty \frac{\Lambda(d)}{d} \sum_{n=1}^\infty g(dn) = \frac{N}{4}\log N - \frac{N}{4} + \frac{\zeta'(2)}{2\zeta(2)} N + O(N^{1/2+\epsilon}).$$

Sums with terms β_n, $N_-(4n)$ y $\widetilde{g}(2n/t)$ are negligible. Their contributions are $O(N^{1/2+\epsilon})$ which is proved by noticing $\widetilde{g}(x) \ll x^{-2} + N^{1/2}\min(x^{-1}, \Delta^{-1}x^{-2})$, $\beta_n \ll \log n$ and $N_-(4n) = O(n^{1/2+\epsilon})$.

By (2.31), the sum $\sum N_+(4n)\widetilde{g}(\sqrt{4n})/\sqrt{n}$ can be written up to a constant as

$$\sum_{n=1}^\infty \frac{N_+(4n)}{n^{3/2}} \big(\cos(2\pi\sqrt{Nn}) - \cos(2\pi\sqrt{n}) - \phi(\sqrt{4n})\big) +$$

$$2\frac{N^{\frac{1}{2}}}{\Delta} \left(\sum_{n<N^{1/2}} + \sum_{N^{\frac{1}{2}} \le n < \Delta^{-2}} + \sum_{n \ge \Delta^{-2}} \right) \frac{N_+(4n)}{n^{3/2}} \sin(\pi\Delta\sqrt{n}) \sin\big(\pi(2N^{\frac{1}{2}} + \Delta)\sqrt{n}\big)$$

$$= S_0 + S_1 + S_2 + S_3.$$

The decay of ϕ and Proposition 2.10 prove $S_0 \ll \log N$. For S_1 note that $\sqrt{n}\Delta \ll 1$ and that we can extract the factor $n^{-3/2}\sin(\pi\sqrt{n}\Delta)$ summing by parts. By Proposition 2.10 taking the second value of the minimum gives

$$S_1 \ll (N^{5/8} + N^{7/48}N^{49/96} + N^{5/48}N^{53/96})N^{\epsilon} \ll N^{21/32+\epsilon}.$$

In order to bound S_2 we do the same but using the first value of the minimum, concluding

$$\begin{aligned} S_2 &\ll N^{21/32+\epsilon} + N^{1/2+\epsilon}\Delta^2\big(\Delta^{-5/2} + N^{3/16}\Delta^{-15/8} + N^{1/16}\Delta^{-17/8}\big) \\ &\ll N^{21/32+\epsilon} + N^{1/2+\epsilon}\Delta^{-1/2} + N^{11/16+\epsilon}\Delta^{1/8}. \end{aligned}$$

Finally, for S_3 we shall directly use Proposition 2.10 as in S_2 getting the same bound.

From all these bounds we obtain

$$\sum_{n=1}^{\infty} \frac{N_+(4n)}{n^{3/2}}\widetilde{g}(\sqrt{4n}) \ll N^{21/32+\epsilon} + N^{1/2+\epsilon}\Delta^{-1/2} + N^{11/16+\epsilon}\Delta^{1/8}$$

which proves the first formula.

For the second we take into account that

$$\sum_{n=1}^{\infty} g(2n)\log n = \frac{N}{8}\log N - \frac{N}{8} - \frac{N}{4}\log 2 + O(N^{1/2+\epsilon})$$

and that the next two terms in Proposition 2.7 contribute

$$\frac{N}{4}\sum_{d=1}^{\infty}\frac{\Lambda(d)}{d^2} - \log 2\sum_{k=1}^{\infty} 2^{-2k-1}N + O(N^{1/2+\epsilon}).$$

By introducing these calculations, the proof is the same. □

Now we shall estimate the short sum through character sums.

Proposition 2.13. *Let g, N and Δ as in the previous proposition. Then*

$$\sum_{N^{1/2}<\sqrt{n}<N^{1/2}+\Delta} \frac{N_+(n)}{\sqrt{n}}g(\sqrt{n}) = \frac{\pi^2 N\Delta}{12} + O(E)$$

and

$$\sum_{N^{1/2}<\sqrt{4n}<N^{1/2}+\Delta} \frac{N_+(4n)}{\sqrt{4n}}g(\sqrt{4n}) = \frac{\pi^2 N\Delta}{24} + O(E)$$

where $E = N^{11/12+\epsilon}\Delta^{5/6} + N^{7/12+\epsilon}\Delta^{-1/6} + N^{19/30+\epsilon}$.

Proof: We have that $h(n)\log\epsilon_n \neq 0$ if and only if $n \in \mathcal{R}$, where $\mathcal{R} = \{n \in \mathbb{Z}^+ : n \equiv 0, 1 \pmod 4, n \neq \square\}$. Moreover in this case holds Dirichlet formula (2.5), hence we can write the left hand side of the first identity in the statement as

$$\sum_{\sqrt{N}<d\sqrt{a}<\sqrt{N}+\Delta} h(a)\log\epsilon_a \frac{g(d\sqrt{a})}{d\sqrt{a}} = \sum_{d<\sqrt{N}+\Delta} \sum_{\substack{N<ad^2<(\sqrt{N}+\Delta)^2 \\ a\in\mathcal{R}}} \frac{g(d\sqrt{a})}{d} L(1,\chi_a)$$

and by Abel's summation formula

$$\frac{N^{1/2}}{2\Delta} \sum_{d<N^{1/2}+\Delta} \frac{1}{d} \int_0^{2\Delta N^{1/2}+\Delta^2} \frac{C(Nd^{-2}, xd^{-2})}{(N+x)^{1/2}} dx, \tag{2.32}$$

where

$$C(x,K) = \sum_{\substack{x<n<x+K \\ n\in\mathcal{R}}} L(1,\chi_n).$$

But in [HB2] we have the estimate

$$C(x,K) = \frac{\zeta(2)}{\zeta(3)}\frac{K}{2} + x^{\epsilon}O(K^{5/6} + x^{2/15} + x^{1/6}\min(1, K^{-1/4}))$$

for every $0 < K \ll x^{1/2}$. Substituting this into (2.32) the first identity follows. For the second we proceed in a similar way $\square$

Choosing $\Delta = N^{-5/16}$, as a consequence of the two previous propositions and of decomposition (2.30) we obtain:

Corollary 2.14. *For any $N > 1$ we have*

$$\sum_{n\leq N} N_+(n) = \frac{\pi^2}{18}N^{\frac{3}{2}} - \frac{N}{2}\log N + (1 - \frac{\zeta'(2)}{\zeta(2)} - \log(2\pi))\frac{N}{2} + O(N^{\frac{21}{32}+\epsilon})$$

and

$$\sum_{n\leq N} N_+(4n) = \frac{2\pi^2}{9}N^{\frac{3}{2}} - N\log N + \big(1 - \frac{\zeta'(2)}{\zeta(2)} - \frac{5\log 2}{3} - \log(2\pi)\big)N + O(N^{\frac{21}{32}+\epsilon}).$$

Now, by Möbius inversion formula we conclude the proofs of the average results for class number.

Proof of Theorem 2.1: By Lemma 2.4 we obtain the expression

$$\sum_{n\leq N} h(n)\log\epsilon_n = \sum_{k\leq\sqrt{N}} \mu(k) \sum_{n\leq N/k^2} N_+(n),$$

and therefore the result follows from Corollary 2.14. Note that $\sum k^{-2}\log k = -\zeta'(2)$. □

Proof of Theorem 2.2: In the same way, by the second part of Lemma 2.4,

$$\sum_{n\le N} h(4n)\log\epsilon_{4n} = \sum_{\substack{k\le\sqrt{N}\\ 2\nmid k}} \mu(k)\Big(\sum_{n\le N/k^2} N_+(4n) - \sum_{n\le N/k^2} N_+(n)\Big),$$

and as before the result is an outcome of Corollary 2.14, noticing in this case that

$$\sum_{2\nmid k}\frac{\mu(k)}{k^3} = \frac{8}{7\zeta(3)},\quad \sum_{2\nmid k}\frac{\mu(k)}{k^2} = \frac{8}{\pi^2}\quad \text{y}\quad \sum_{2\nmid k}\mu(k)\frac{\log k}{k^2} = \big(\frac{\log 2}{3} + \frac{\zeta'(2)}{\zeta(2)}\big)\frac{8}{\pi^2},$$

(for the last identity, calculate the derivative of $\big((2^{-s}-1)\zeta(s)\big)^{-1}$ at $s=2$). □

2.5 Study of the oscillatory term

In the previous section we have demonstrated that

$$E_2^+(x) \ll x^{\frac{21}{32}}.$$

but it is believed that actually $E_2^+(x) \ll x^{1/2+\epsilon}$ for any $\epsilon > 0$. In this section we are going to study the term E_2^+ on average.

We shall calculate the L^2-norm of the function $E_2^+(N+K) - E_2^+(N)$ in the interval $R \le N \le 2R$. To this end we are going to take advantage of the fact that this function can be written by means of short character sums, which will be suitable in order to control the norm, but besides these sums can be expressed in terms of exponentials what in turn is going to permit to carry the integration. In this process will be relevant the Gauss sums

$$\tau_b(m) = \sum_{a(\mathrm{mod}\ m)} \big(\frac{a}{m}\big)e\big(\frac{ba}{m}\big).$$

The influence of K will be codified into the function

$$f(y) = \frac{e(-Ky)-1}{e(-y)-1}.$$

In the following lemma we are going to show how that expression can be created.

Lemma 2.15. *Let $R > 1$, $R < N < 2R$ and $K < R^{1/2}(\log R)^{-1}$. For every $K < M < R$ holds the expression*

$$\frac{E_2^+(N+K) - E_2^+(N)}{(4N)^{\frac{1}{2}}} = B_M(N) + \sum_{\substack{N \le n \le N+K \\ M \le m \le R}} \frac{\chi_{4n}(m)}{m} - C(N)\log R + O(1),$$

with

$$B_M(N) = \sum_{m<M, m\neq\square}{}^{*} \frac{1}{m^2} \sum_{b(mod\ m)} \tau_b(m) f\big(\frac{b}{m}\big) e\big(\frac{-b}{m}N\big)$$

(where the asterisk restricts the summation to odd numbers) and $C(N)$ the function taking the value 1 whenever there is some integer inside the interval $[N^{1/2}, (N+K)^{1/2}]$ and zero otherwise.

Proof: We begin by using Theorem 2.2 in order to infer the formula

$$\frac{E_2^+(N+K) - E_2^+(N)}{(4N)^{\frac{1}{2}}} = \sum_{\substack{N < n \le N+K \\ 4n \neq \square}} L(1, \chi_{4n}) - \frac{\pi^2}{7\zeta(3)}K + O(1) \qquad (2.33)$$

for any $1 < K < N^{1/2}(\log N)^{-1}$. By Pólya-Vinogradov inequality, for $4n \neq \square$ we can write

$$L(1, \chi_{4n}) = \sum_{m<R} \frac{\chi_{4n}(m)}{m} + O(R^{-\frac{1}{2}}\log R). \qquad (2.34)$$

By a calculation we can see that

$$\sum_{N<n\le N+K} \sum_{m<R, m=\square} \chi_{4n}(m) m^{-1} = \frac{\pi^2}{7\zeta(3)}K + O(1)$$

hence

$$(4N)^{-\frac{1}{2}}(E_2^+(N+K) - E_2^+(N)) = \sum_{\substack{N<n\le N+K \\ 4n\neq\square}} \sum_{\substack{m<R \\ m\neq\square}} \frac{\chi_{4n}(m)}{m} + O(1).$$

We can write

$$\sum_{\substack{N<n\le N+K \\ 4n\neq\square}} \sum_{\substack{m<R \\ m\neq\square}} \frac{\chi_{4n}(m)}{m} = \sum_{\substack{m<R \\ m\neq\square}} \frac{1}{m} \sum_{N<n\le N+K} \chi_{4n}(m) - C(N)\log R + O(1).$$

For m even we have $(4n/m) = 0$, and for $m \neq \square$ odd $(4\cdot/m) = (\cdot/m)$ is a non-principal character with modulus m. In this last case we have

$$\sum_{x<n\le x+K} \big(\frac{4n}{m}\big) = \frac{1}{m} \sum_{a(\mathrm{mod}\ m)} \big(\frac{a}{m}\big) \sum_{x<n\le x+K} \sum_{b(\mathrm{mod}\ m)} e\big(\frac{b(a-n)}{m}\big) =$$

$$\frac{1}{m}\sum_{b(\mathrm{mod}\ m)}\tau_b(m)\sum_{x<n\leq x+K}e\big(\frac{-bn}{m}\big)=\frac{1}{m}\sum_{b(\mathrm{mod}\ m)}\tau_b(m)f\big(\frac{b}{m}\big)e\big(\frac{-b}{m}x\big)$$

that proves the lemma. □

When doing the average mean of $E_2^+(N+K)-E_2^+(N)$, the main term will come from the diagonal terms that appear when expanding $B_M(N)$, namely from the sum

$$S=\sum_{\substack{m_1,m_2<M\\ m_1,m_2\neq\square}}^{*}\frac{1}{m_1^2m_2^2}\sum_{b_1m_2=b_2m_1}\tau_{b_1}(m_1)\overline{\tau_{b_2}(m_2)}f(\frac{b_1}{m_1})\overline{f(\frac{b_2}{m_2})}. \tag{2.35}$$

Let us see it is possible to control the behaviour of S with precision.

Proposition 2.16. *Let $2\leq K\leq M\leq R$. Then*

$$S=3(P/4\pi)^2\log K+O((\log K)^{2/3})$$

with $P=\prod_{p\neq 2}(1-1/(p^3+p^2))$.

Proof: The start point is the formula for Gauss sums

$$\tau_{\lambda s}(cs^2)=\varepsilon_c c^{1/2}s\sum_{d|(\lambda,s)}d\big(\frac{\lambda sd^{-2}}{c}\big)\mu\big(\frac{s}{d}\big) \tag{2.36}$$

for any c odd square-free number [IK], with $\varepsilon_c=1$ if $c\equiv 1\ (\mathrm{mod}\,4)$ and $\varepsilon_c=i$ if $c\equiv -1\ (\mathrm{mod}\,4)$. We notice that $\tau_b(cs^2)=0$ if $s\nmid b$ and we can rewrite S as

$$\sum_{\substack{c_1s_1^2d_1^2<M\\ c_2s_2^2d_2^2<M\\ c_1\neq 1,c_2\neq 1}}^{*}\frac{\mu^2(c_1)\varepsilon_{c_1}\mu^2(c_2)\overline{\varepsilon_{c_2}}}{(d_1d_2)^2(c_1s_1^2c_2s_2^2)^{\frac{3}{2}}}\sum_{\substack{\lambda_1<c_1s_1\\ \lambda_2<c_2s_2\\ \lambda_1c_2s_2=\lambda_2c_1s_1}}\big|f\big(\frac{\lambda_1}{c_1s_1}\big)\big|^2\big(\frac{\lambda_1s_1}{c_1}\big)\big(\frac{\lambda_2s_2}{c_2}\big)\mu(s_1)\mu(s_2).$$

With these restrictions we can consider the sum only over the terms satisfying

$$c_1(c_2,s_1)=c_2(c_1,s_2),\quad s_1/(s_1,c_2)\mid\lambda_1,\ s_2/(s_2,c_1)\mid\lambda_2.$$

Thus writing

$$c_1=cj_1,s_2=q_2j_1,c_2=cj_2,s_1=q_1j_2,(c,q_1q_2)=1,$$

$$\lambda_1=\lambda q_1,\lambda_2=\lambda q_2,$$

follows that S equals

$$\sum_{\substack{cj_1q_1^2j_2^2d_1^2<M\\ cj_2q_2^2j_1^2d_2^2<M\\ (q_1q_2,j_1j_2)=1\\ (c,q_1q_2)=1}}{}^{*}\frac{\mu(q_1)\mu(q_2)\mu(j_1j_2)\mu^2(c)}{(d_1d_2)^2(j_1j_2)^{\frac{9}{2}}(q_1q_2)^3}\big(\frac{j_1j_2}{c}\big)\frac{\varepsilon_{cj_1}\overline{\varepsilon_{cj_2}}}{c^3}\sum_{\substack{\lambda<cj_1j_2\\ c\neq 1}}|f\big(\frac{\lambda}{cj_1j_2}\big)|^2\big(\frac{\lambda j_1}{j_2}\big)\big(\frac{\lambda j_2}{j_1}\big).$$

Bounding trivially, we have that the quantity given by the terms holding $\lambda(cj_1j_2)^{-1}<1/K$ is $O(1)$, noting that

$$|f(u)|^2=\frac{1-\cos(2\pi Ku)}{2\pi^2u^2}+O(1).$$

Moreover the sums can be completed obtaining

$$S=\frac{1}{2\pi^2}\sum_{\substack{(q_1q_2,j_1j_2)=1\\ j_1j_2\equiv 1(4)}}{}^{*}\frac{\mu(q_1)\mu(q_2)\mu(j_1j_2)}{(d_1d_2)^2(j_1j_2)^{\frac{5}{2}}(q_1q_2)^3}\sum_{\lambda=1}^{\infty}\big(\frac{\lambda j_1}{j_2}\big)\big(\frac{\lambda j_2}{j_1}\big)\frac{\Delta(\lambda,j_1j_2,q_1q_2)}{\lambda^2}+O(1) \tag{2.37}$$

with

$$\Delta(\lambda,j,q)=\sum_{\substack{c<K/j\\ (c,q)=1}}{}^{*}\frac{1-\cos(2\pi K\lambda/(cj))}{c}\big(\frac{j}{c}\big)\mu^2(c).$$

For $j>1$, we have (applying $\mu^2(c)=\sum_{d^2|c}\mu(d)$ and Pólya-Vinogradov)

$$\sum_{\substack{c<K/j\\ (c,q)=1}}{}^{*}\frac{1}{c}\big(\frac{j}{c}\big)\mu^2(c)\ll(qj)^{1/2}\log(qj).$$

On the other hand, for any j one can write

$$\sum_{\substack{c<K/j\\ (c,q)=1}}{}^{*}e\big(\frac{K\lambda j^{-1}}{c}\big)\big(\frac{j}{c}\big)\frac{\mu^2(c)}{c}=\sum_{\substack{d^2<K/j\\ (d,2q)=1}}\frac{\mu(d)}{d^2}\big(\frac{j}{d^2}\big)\sum_{\substack{c<Kj^{-1}d^{-2}\\ (c,2q)=1}}\big(\frac{j}{c}\big)e\big(\frac{K\lambda j^{-1}d^{-2}}{c}\big)\frac{1}{c}$$

which is smaller than

$$2jq\sum_{d=1}^{\infty}\frac{1}{d^2}\max_{1\leq a\leq 2jq}\Big|\sum_{0\leq n<(Kj^{-1}d^{-2}-a)/(2jq)}e\big(\frac{K\lambda j^{-2}q^{-1}d^{-2}}{n+a/(2jq)}\big)\frac{1}{2jqn+a}\Big|.$$

Hence we see that it is necessary to bound exponential sums with the shape

$$S(N,N_1)=\sum_{N<n<N_1}e(g(n))$$

for $N_1 < 2N < 2\tilde{K}$ and $g(n) = \tilde{K}/(n+\alpha)$, $0 < \alpha \leq 1$. In the range $\tilde{K}/N \geq N^4$ we can apply Vinogradov's method [IK] obtaining

$$S(N, N_1) \ll N \exp(-2^{-18}(\log N)^3(\log(\tilde{K}/N))^{-2}).$$

Moreover in the range $\tilde{K}^{1/5} \leq N \leq \tilde{K}^{1/2}$ we use van der Corput method (see [IK]) in order to get

$$S(N, N_1) \ll (\tilde{K}N^{-6})^{1/62}N,$$

y en $\tilde{K}^{1/2} \leq N \leq \tilde{K}$

$$S(N, N_1) \ll (N\tilde{K}^{-1})^{1/2}N.$$

Hence

$$\sum_{\substack{c<Kj^{-1} \\ (c,q)=1}}{}^{*} e(\frac{K\lambda j^{-1}}{c})(\frac{j}{c})\frac{\mu^2(c)}{c} \ll jq + (\log \lambda K)^{2/3},$$

and thus for $j \neq 1$ we have

$$\Delta(\lambda, j, q) \ll jq + (\log \lambda K)^{2/3} \tag{2.38}$$

and

$$\Delta(\lambda, 1, q) = \sum_{\substack{c<K \\ (c,2q)=1}} \mu^2(c)c^{-1} + O(q + (\log \lambda K)^{2/3}). \tag{2.39}$$

It is possible to estimate the sum

$$\begin{aligned}
\sum_{\substack{c<K \\ (c,2q)=1}} \mu^2(c)c^{-1} &= \sum_{\substack{d^2<K \\ (d,2q)=1}} \frac{\mu(d)}{d^2} \sum_{\substack{c<Kd^{-2} \\ (c,2q)=1}} \frac{1}{c} \\
&= \sum_{\substack{d^2<K \\ (d,2q)=1}} \frac{\mu(d)}{d^2}(\frac{\varphi(2q)}{2q}\log\frac{K}{d^2} + O((\log q)^2)) \\
&= \frac{\varphi(2q)}{2q}\log K \sum_{\substack{d=1 \\ (d,2q)=1}}^{\infty} \mu(d)d^{-2} + O((\log q)^2) \\
&= \frac{1}{\zeta(2)}\frac{\varphi(2q)}{2q\prod_{p|2q}(1-p^{-2})}\log K + O((\log q)^2) \\
&= \frac{1}{\zeta(2)}\frac{2}{3}\eta(q)\log K + O((\log q)^2)
\end{aligned} \tag{2.40}$$

with $\eta(q) = \prod_{p|q}(1+p^{-1})^{-1}$. By (2.37), (2.38), (2.39) and (2.40) we have

$$S = \frac{1}{18\zeta(2)^2}T\log K + O((\log K)^{2/3}), \tag{2.41}$$

with

$$T=\sum\nolimits^{*}\frac{\mu(q_1)\mu(q_2)}{(d_1d_2)^2(q_1q_2)^3}\eta(q_1q_2)\sum_{\lambda=1}^{\infty}\frac{1}{\lambda^2}=(1-2^{-2})^2\zeta(2)^2(\sum_{q}^{*}\frac{\mu(q)\eta(q)}{q^3})^2\zeta(2)$$

By using Euler's product for this sum the result is proved. □

We are going to use the previous proposition to get:

Proposition 2.17. *Let $R>1$. Uniformly in $1<L<R$ and $K<R^{\frac{1}{4}-\epsilon}$ we have*

$$\sum_{R\leq N\leq R+L}\frac{(E_2^{+}(N+K)-E_2^{+}(N))^2}{4N}=3(P/4\pi)^2L\log K+O(R(\log K)^{2/3})$$

with

$$P=\prod_{p\neq 2}\big(1-\frac{1}{p^3+p^2}\big).$$

Proof: We have

$$\sum_{R\leq N\leq 2R}C(N)^2\ll KR^{1/2}\ll R. \tag{2.42}$$

Also, by Cauchy's inequality we have

$$\sum_{R\leq N\leq 2R}|\sum_{\substack{N\leq n\leq N+K\\ M\leq m\leq R}}\frac{\chi_{4n}(m)}{m}|^2\ll K^2\sum_{n\leq 3R}|\sum_{M\leq m\leq R}\frac{\chi_{4n}(m)}{m}|^2.$$

Writing $n=cs^2$ with $\mu(c)\neq 0$ we have

$$\sum_{n\leq 3R}|\sum_{M\leq m\leq R}\frac{\chi_{4n}(m)}{m}|^2=\sum_{s^2\leq 3R}\sum_{\substack{c<3Rs^{-2}\\ \mu(c)\neq 0}}|\sum_{\substack{M<m<R\\ (m,2s)=1}}\frac{\chi_{c}(m)}{m}|^2.$$

Appealing to Corollary 3 in [HB1] in dyadic intervals we can see that this sum is

$$\ll R^{\epsilon}\sum_{s^2\leq 3R}(RM^{-1}s^{-2}+1)\ll R^{\frac{1}{2}+\epsilon}(1+R^{\frac{1}{2}}M^{-1}).$$

Thus, taking $M=R^{\frac{1}{2}-\epsilon}$ we deduce that

$$\sum_{R\leq N\leq 2R}|\sum_{\substack{N\leq n\leq N+K\\ M\leq m\leq R}}\frac{\chi_{4n}(m)}{m}|^2\ll K^2R^{\frac{1}{2}+2\epsilon}\ll R. \tag{2.43}$$

Hence by (2.42), (2.43), Lemma 2.15 and Cauchy's inequality we see that to prove the proposition is equivalent to obtain

$$\sum_{R<N<R+L} |B_M(N)|^2 = 3(P/4\pi)^2 L \log K + O(R(\log K)^{2/3}). \tag{2.44}$$

Expanding the square we see that

$$B_M(N)^2 = \sideset{}{^*}\sum_{\substack{m_1,m_2<M \\ m_1,m_2\neq\square}} \sum_{\substack{b_1 (\mathrm{mod}\ m_1) \\ b_2 (\mathrm{mod}\ m_2)}} \frac{\tau_{b_1}(m_1)}{m_1^2}\overline{\frac{\tau_{b_2}(m_2)}{m_2^2}} f(\frac{b_1}{m_1})\overline{f(\frac{b_2}{m_2})} e\big((\frac{b_2}{m_2}-\frac{b_1}{m_1})N\big).$$

By the formula

$$\sum_{R<N\leq R+L} e(N\theta) = \frac{e((R+L)\theta)}{2\pi\theta} - \frac{e(R\theta)}{2\pi\theta} + O(1) \qquad |\theta|<1/2$$

we obtain

$$\sum_{R<N<R+L} |B_M(N)|^2 = LS + O(D(\log R)^2) + O(M^2)$$

where

$$D = \max_{M_1,M_2\leq M} \Big| \sideset{}{^*}\sum_{\substack{M_1<m_1<2M_1 \\ M_2<m_2<2M_2}} \sum_{\substack{b_1 \ (\mathrm{mod}\ m_1) \\ b_2 \ (\mathrm{mod}\ m_2) \\ b_1m_2\neq b_2m_1}} \frac{a_{b_2,m_2}\overline{a_{b_1,m_1}}}{b_2/m_2 - b_1/m_1}\Big|,$$

with $a_{b,m} = m^{-2}f(b/m)\tau_b(m)e(Zb/m)$ for some $Z\in\mathbb{R}$. For $M_j \leq m_j \leq 2M_j$ we have

$$|\frac{b_2}{m_2} - \frac{b_1}{m_1}| \geq \frac{1}{M_1M_2},$$

hence by generalized Hilbert inequality (see [IK]) we get

$$D \ll \max_{M_1\leq M} M_1^2 \sideset{}{^*}\sum_{\substack{M_1<m<2M_1 \\ b\ (\mathrm{mod}\ m)}} |a_{b,m}|^2 \ll \max_{M_1\leq M} M_1^{-2} \sum_{\substack{M_1<m<2M_1 \\ 1\leq|b|\leq m/2}} |\tau_b(m)|^2 |f(\frac{b}{m})|^2.$$

From (2.36) we deduce that $|\tau_{\lambda s}(cs^2)| \ll c^{\frac{1}{2}} s(\lambda,s)\log\log(s)$, hence for any $U\leq M_1$ holds

$$\sideset{}{^*}\sum_{M_1<m<2M_1} \sum_{U<b<2U} |\tau_m(b)|^2 \ll (UM_1^2 + M_1^2\log M_1)\log\log M_1,$$

and since $|f(t)| \ll \min(K, |t|^{-1})$ for any $|t| \leq 1/2$ we have

$$\sum_{\substack{M_1<m<2M_1 \\ 1\leq|b|\leq m/2}}{}^{*}|\tau_b(m)|^2|f(\frac{b}{m})|^2 \ll (KM_1^3 + K^2M_1^2\log M_1)\log\log M_1$$

hence $D \ll KM\log\log M \ll R$ and therefore

$$\sum_{R<N<R+L}|B_M(N)|^2 = LS + O(R), \tag{2.45}$$

and an appeal to Proposition 2.16 proves (2.44). □

Finally we arrived at the searched result.

Theorem 2.18. *Let $x > 1$, $K \leq x^{1/4-\epsilon}$. Then*

$$\sum_{N\leq x}(E_2^+(N+K) - E_2^+(N))^2 = (\frac{3Px}{4\pi})^2\log K + O(x^2(\log K)^{\frac{2}{3}}).$$

Proof: By Abel's Lemma

$$\sum_{R\leq N\leq 2R}(E_2^+(N+K) - E_2^+(N))^2 = 8RT(R) - 4\int_R^{2R}T(u)du$$

with $T(u) = \sum_{R\leq N\leq u}(4N)^{-1}(E_2^+(N+K) - E_2^+(N))^2$. For $R > x(\log x)^{-3}$, by Proposition 2.17 we have

$$\sum_{R\leq N\leq 2R}(E_2^+(N+K) - E_2^+(N))^2 = 2(\frac{3P}{4\pi})^2R^2 + O(R^2(\log K)^{3/2}).$$

Adding the results for $R = x/2^j$, $j \in \mathbb{N}$, with $R > x(\log x)^{-3}$ and using (2.25) for $R < x(\log x)^{-3}$ we deduce the theorem. □

Chapter 3

The number of sumsets

3.1 Introduction.

For any A, B subsets of a group G we define its sumset as the set of all possible sums of elements of A and B

$$A + B = \{a + b \in G : a \in A, b \in B\}.$$

Several properties of these sets has been studied, beginning with Cauchy's work [Cau], that proved the inequality

$$|A + B| \geq \min(|A| + |B| - 1, |G|), \tag{3.1}$$

when $G = \mathbb{Z}/p\mathbb{Z}$, p prime integer. This result was rediscovered a century after by H. Davenport [Dav1]. Later Vosper [Vos] proved that the cases for which equality happens are very special: if $|A|, |B| \geq 2$, then A and B are arithmetic progressions with the same difference or alternatively B is a translation of the complementary of A in $\mathbb{Z}/p\mathbb{Z}$.

In the case $G = \mathbb{Z}$ happens something similar. We have $|A + B| \geq |A| + |B| - 1$ and, if A and B are sets of more than one element equality holds only in the case A and B are arithmetic progressions with the same difference. Finally Kemperman [Kem], using methods developed by Kneser and van der Corput, generalized this kind of result to any abelian group.

Instead of being so restrictive we can ask what happens if we require only that

$$|A + A| \leq C|A| \tag{3.2}$$

with C a positive constant. If $|A + A| \leq 3|A| - 4$ in the case $G = \mathbb{Z}$ and $|A + A| \leq (12/5)|A| - 3$ with $|A| \leq p/35$ in the case $G = \mathbb{Z}/p\mathbb{Z}$, Freiman (see [Nat]) had proved that A is contained in an arithmetic progression of length

smaller than $2|A|-2$ and $(7/5)|A|-1$ respectively. Nevertheless, when the constant C is bigger we can easily construct sets A not well covered by any arithmetic progression. Freiman understood the situation and in order to solve the problems considered the sets

$$P = \{y_0 + \sum_{j=1}^{d} y_j a_j : 0 \leq a_j \leq m_j - 1\}$$

that we shall call arithmetic progressions of dimension d. If the sums defining the set are all distinct we say P is proper, and in this case we have $|P+P| \leq 2^d|P|$. In this way he proved [Fre] that basically these are the unique subsets of $\mathbb{Z}$ with small sumset, that is to say if $A \subset \mathbb{Z}$ satisfies (3.2) then A is contained in an arithmetic progression of dimension d and size $K|A|$, where d and K are constants only depending on C. This result has been used by T. Gowers [Gow1, Gow2] to prove that for any $k \geq 3$, any subset of $\{1, 2, \ldots, N\}$ of size larger than $N(\log\log N)^{-2^{-2^{k+9}}}$ contains some non-trivial arithmetic progression of length k, improving substantially Szemerédi's result [Sze].

I. Ruzsa [Ruz1] generalized Freiman's theorem to the case $|A+B| < C|A|$ with $|A| = |B|$ for abelian torsion-free groups, and later [Ruz2] he has proved a result of the same kind for G abelian group of finite bounded torsion: let $A \subset G$, such that there exist $B \subset G$ of the same size that A with

$$|A + B| \leq C|A|,$$

then A is contained in a subgroup H with $|H| \leq K|A|$, where K only depends on C and on the maximum order of the elements of G.

It is also known that if A and B are large sets of $\mathbb{Z}/p\mathbb{Z}$, their sumset has a lot of structure. In particular it has been proven that contains long arithmetic progressions. The best result is that of B. Green [Gre1]: if $|A| = \alpha p$ and $|B| = \beta p$ with $\alpha, \beta > 0$, then $A + B$ contains an arithmetic progression of size larger than

$$e^{K\sqrt{\log p}},$$

where $K > 0$ only depends on α and β.

In another direction, recently Green and Ruzsa [GrRu] have studied the cardinal of $\mathrm{SS}(G)$, the set of sumsets of the form $A + A$ in an abelian finite group G. They have obtained

$$|\mathrm{SS}(\mathbb{Z}/p\mathbb{Z})| = (2^{\frac{1}{3}})^{p+o(p)},$$

extending later this result to another groups.

In this chapter we are going to treat a related problem, exposing the results obtained in [GU]. We shall be interested in controlling the number of

sets that are sum of big sets, namely we would like to know the size of the set

$$T(k,G)=\{A+B:|A|,|B|\geq k\}.$$

In the first section we shall show that in the case $G=\mathbb{Z}/p\mathbb{Z}$ with p a prime integer we have

Theorem 3.1. *Let $p(\log p)^{-1/10}<k<p/8$. Then*

$$|T(k,\mathbb{Z}/p\mathbb{Z})|=(\sqrt{2})^{p+o(p)}.$$

In order to prove it we shall use Green-Ruzsa method of granular sets. Basically, what happens is that as A and B are large the characteristic function of $A+B$ can be well approximated by the convolution of the characteristic functions of A and B in most cases. In another words, the set $A+B$ is going to be "smooth". This allows to treat the problem through harmonic analysis in $\mathbb{Z}/p\mathbb{Z}$.

When A is small, the structure of the sets $B+A$ changes strongly by any small variation of the set A. This motivates the following definition: let G be a group and A a subset of G. We call A-set to any subset of G that can be represented as

$$B+A$$

for some $B\subset G$. If G is finite, we are interested in controlling the size of the set

$$S(A,G)=\{B+A:B\subset G\}.$$

In the case that G is abelian and finitely generated, $G=H\times\mathbb{Z}^d$ with H finite, we shall want to know the size of

$$S_N(A,G)=\{B+A:B\subset H\times I_N^d\}$$

for N growing to infinity, with

$$I_N=\{n\in\mathbb{Z}:1\leq n\leq N\}.$$

This size is controlled by the constant (see Lemma 3.12)

$$c(A,G)=\lim_{N\to\infty}|S_N(A,G)|^{\frac{1}{N^d|H|}}.$$

In the second section we shall see that in the case $G=\mathbb{Z}$, if A is finite an $\ell(A)=\max_{a,a'\in A}|a-a'|$, we have

$$c(A,\mathbb{Z})=\rho_A, \tag{3.3}$$

where ρ_A is the spectral radius of an square matrix M_A of dimension $2^{2\ell(A)+1}$ that can be expressed in explicit form in terms of A. This characterization, together with the property

$$c(\lambda A, \mathbb{Z}) = c(A, \mathbb{Z}) \qquad \text{for any } \lambda \in \mathbb{Z}^\times,$$

where $\lambda A = \{\lambda a : a \in A\}$, is going to allow us to demonstrate that

Theorem 3.2. *For any $a, b \in \mathbb{Z}$ distinct we have*

$$c(\{a, b\}, \mathbb{Z}) = \rho$$

where $\rho = 1.75488\ldots$ is the positive root of equation

$$x^3 - 2x^2 + x - 1 = 0.$$

We shall be able also to calculate the constant $c(A, \mathbb{Z})$ for sets A with $\ell(A)$ small and for special sets as $A_k = \{0, 1 \ldots, k-1\}$.

The case $|A| = 3$ can be treated geometrically, establishing the following relation with the two-dimensional case.

Theorem 3.3. *Let $a, b \in \mathbb{Z}$ with $|a| < |b|$ and $(a, b) = 1$. Then*

$$c(U_2, \mathbb{Z}^2)^{1-1/b} \le c(\{0, a, b\}, \mathbb{Z}) \le c(U_2, \mathbb{Z}^2)^{1+1/b}.$$

with $U_2 = \{(0,0), (1,0), (0,1)\}$. In particular for any $a \in \mathbb{Z}$ we have

$$\lim_{n\to\infty} c(\{0, a, n\}, \mathbb{Z}) = c(U_2, \mathbb{Z}^2).$$

We shall also show that

$$c(U_2, \mathbb{Z}^2) < c(U_1, \mathbb{Z})$$

where $U_1 = \{0, 1\}$. By Theorem 3.3 we immediately deduce:

Theorem 3.4. *There exists $b^* \in \mathbb{N}$ such that for any $b > b^*$ and $a \in \mathbb{N}$, $(a, b) = 1$ we have*

$$c(\{0, a, b\}, \mathbb{Z}) < c(\{0, 1\}, \mathbb{Z}).$$

Defining

$$c(k, G) = \sup\{c(A, G) : A \in G, |A| = k\},$$

by Theorem 3.4 we see that in order to prove $c(3, \mathbb{Z}) < c(2, \mathbb{Z}) = c(\{0, 1\}, \mathbb{Z})$ only remains to control $c(\{0, a, b\}, \mathbb{Z})$ for finitely many sets $\{0, a, b\}$. But it

seems that the remaining cases are to large to be treated computationally through (3.3). A new idea is needed.

It seems reasonable to think that the sequence $(c(k,\mathbb{Z}))_{k\in\mathbb{N}}$ is always decreasing, but we do not know how to prove it for any value k larger than one. Considering the set $A=\{1,2,4,6,\dots,2k\}$, we can see that

$$c(k,\mathbb{Z})\geq\sqrt{2}\qquad\text{for any } k\in\mathbb{N}.$$

We shall prove that this inequality is actually strict. The natural question, in part motivated by Theorem 3.1, is that if this sequence decreases to $\sqrt{2}$. Theorem 3.1 permits to demonstrate the following partial result.

Theorem 3.5. *Let $\lambda>0$ and*

$$c_\lambda(k,\mathbb{Z})=\sup\{c(A,\mathbb{Z}):|A|=k,\ell(A)\leq\lambda|A|\}.$$

Then

$$\lim_{k\to\infty}c_{\lambda(k)}(k,\mathbb{Z})=\sqrt{2}.$$

for any sequence $(\lambda(k))_{k\in\mathbb{N}}$, with $2\leq\lambda(k)\leq(\log k)^{\frac{1}{10}}$.

In the third chapter we shall study $|S(A,\mathbb{Z}/p\mathbb{Z})|$. For each $A\in\mathbb{Z}/p\mathbb{Z}$, with $|A|\geq 2$, we have

$$B+x\subset B+\{x,y\}\subset B+A,$$

(where $B+x$ denotes $B+\{x\}$) for any $x,y\in A$. From them, by combinatorial arguments we shall prove:

Theorem 3.6. *For any $A\subset\mathbb{Z}/p\mathbb{Z}$ of cardinal larger or equal than two we have*

$$|S(A,\mathbb{Z}/p\mathbb{Z})|\ll 1.9814^p.$$

Of course we think that this bound is not a accurate one; we should have

$$|S(A,\mathbb{Z}/p\mathbb{Z})|\ll\eta^p\qquad\text{with }\eta<c(\{0,1\},\mathbb{Z})$$

for any A with $|A|\geq 3$. In any case, this allows us to prove that

$$c(k,\mathbb{Z})\leq 1.9814\qquad\text{for any } k\geq 3,$$

and by Theorem 3.1 it can be demonstrated that

$$c(2,\mathbb{Z})^{p+o(p)}\ll|T(2,\mathbb{Z}/p\mathbb{Z})|\ll 1.9814^{p+o(p)},$$

where $c(2,\mathbb{Z})=\rho$ with $\rho=1.7548\dots$ defined in Theorem 3.2.

3.2 Sums of large sets

In this section we want to count the number of sets of the for $A+B$, A and B being subsets of $\mathbb{Z}/p\mathbb{Z}$ of size almost comparable to p. This question is related to count the number of sets of the shape $A + A$ with $A \subset \mathbb{Z}/p\mathbb{Z}$, problem successfully solved by Green and Ruzsa in [GrRu]. After that B. Green used the same method and another tools in order to prove [Gre2] Cameron-Erdős conjecture on the number of sum-free sets in $\{1, 2, \dots, N\}$. We shall use their method to prove Theorem 3.1.

We begin giving some notation. Let $f, g : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ y $n \in \mathbb{Z}/p\mathbb{Z}$, we define convolution in $\mathbb{Z}/p\mathbb{Z}$ as

$$f * g(n) = \sum_{m \in \mathbb{Z}/p\mathbb{Z}} f(m)g(n-m).$$

We also define Fourier coefficients

$$\widehat{f}(n) = \sum_{m \in \mathbb{Z}/p\mathbb{Z}} f(m)e(-nm/p).$$

Let $C \subset \mathbb{Z}/p\mathbb{Z}$, we write $C(n)$ for the characteristic function of the set C. With these definitions, and being $D \subset \mathbb{Z}/p\mathbb{Z}$, we have

$$C * D(n) = |\{(x, y) \in C \times D : x + y = n\}|.$$

In the proof we shall use basically Plancherel identity

$$\sum_n |f(n)|^2 = p^{-1} \sum_x |\widehat{f}(x)|^2 \tag{3.4}$$

as well as the relation between convolution and Fourier transform

$$\widehat{f * g}(x) = \widehat{f}(x)\widehat{g}(x). \tag{3.5}$$

Now, let m a fixed natural number. For each $d \in (\mathbb{Z}/p\mathbb{Z})^\times$ we are going to divide $\mathbb{Z}/p\mathbb{Z}$ into m arithmetic progressions with common difference d defined as

$$J_i(d) = \{\lambda d : \frac{ip}{m} \leq \lambda < \frac{(i+1)p}{m}\},$$

with $0 \leq i \leq m-1$. The length of $J_i(d)$ is L or $L-1$, where $L = \lceil p/m \rceil$. We say that $B \subset \mathbb{Z}/p\mathbb{Z}$ is an m-granular set if there exist $d \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $I \subset \{0, 1, \dots, m-1\}$ such that

$$B = \bigcup_{i \in I} J_i(d).$$

Finally, let C a subset of $\mathbb{Z}/p\mathbb{Z}$ and $\epsilon_1 > 0$, and let

$$T(d) = \{i \in \{0, 1, \ldots, m-1\} : |C \cap J_i(d)| \geq \epsilon_1 |J_i(d)|\}.$$

Then, define the $(m, d)-$granularization C' of C (with respect to the parameter ϵ_1) as

$$C' = C'(d) = \bigcup_{i \in T(d)} J_i(d).$$

We have

$$|C \setminus C'| = \sum_{i \notin T(d)} |C \cap J_i(d)| < \epsilon_1 \sum_{i \notin T(d)} |J_i(d)| \leq \epsilon_1 p, \tag{3.6}$$

taking into account that the sets $J_i(d)$ are disjoint.

The fundamental result that can be obtained by using Green-Ruzsa method is the following:

Lemma 3.7. *Let C any subset of $\mathbb{Z}/p\mathbb{Z}$. Then there exists $d \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that*

$$\max_{x \in \mathbb{Z}/p\mathbb{Z}} h_d(x)|\widehat{C}(x)| \leq \frac{(\log((2/3)^{1/2}\pi L))^{1/2}}{(\log p)^{1/2}} |C|^{1/2} p^{1/2}$$

where

$$h_d(x) = \frac{2}{2L-1} \sum_{j=1}^{L-1} \big(1 - \cos\big(\frac{2\pi j d x}{p}\big)\big).$$

We shall call "good length for C" to any d satisfying this conditions.

Proof: Let $\epsilon > 0$. Suppose we want to prove that

$$h_d(x)|\widehat{C}(x)| \leq \epsilon |C| \tag{3.7}$$

holds for every $x \in \mathbb{Z}/p\mathbb{Z}$. Of course it does for $x = 0$ or $|\widehat{C}(x)| \leq \epsilon|C|$ (because $0 \leq h_d(x) \leq 1$). Let R the set of remaining x, namely

$$R = \{x \in \mathbb{Z}/p\mathbb{Z} : x \neq 0, |\widehat{C}(x)| > \epsilon|C|\}.$$

It remains to demonstrate that (3.7) holds for each $x \in R$. Writing $\|t\|$ for the distance from t to the nearest integer, we have the inequality $1 - \cos 2\pi t \leq 2\pi^2 \|t\|^2$. Therefore

$$h_d(x) \leq \frac{4\pi^2}{2L-1} \sum_{j=1}^{L-1} \|\frac{jdx}{p}\|^2 \leq \frac{4\pi^2}{2L-1} \|\frac{dx}{p}\|^2 \sum_{j=1}^{L-1} j^2 \leq \frac{2\pi^2 L^2}{3} \|\frac{dx}{p}\|^2.$$

Hence, for (3.7) to hold is enough that

$$\|\frac{dx_i}{p}\| \leq b_i \tag{3.8}$$

for any $1 \leq i \leq k$, where $R = \{x_1, x_2, \ldots, x_k\}$ and

$$b_i = \frac{\sqrt{3}}{\sqrt{2}\pi L}(\frac{\epsilon|C|}{|\widehat{C}(x_i)|})^{1/2}.$$

But this is equivalent to the following condition: let $M = \prod_{i=1}^{k}[-b_i p, b_i p] \subset \mathbb{R}^k$ and $\Lambda \subset \mathbb{R}^k$ the lattice generated by the vectors $\vec{x}, p\vec{e_1}, p\vec{e_2}, \ldots, p\vec{e_k}$, with $\vec{e_i}$ the vectors of the usual basis for $\mathbb{R}^k$ and $\vec{x} = (x_1, x_2, \ldots, x_k)$. There exists an element $y \in \Lambda, y \neq \vec{0}$ such that y is also in M.

By Minkowski's First Theorem this last condition follows from the inequality $|M| \geq 2^k|\Lambda|$. Since $|M| = 2^k p^k \prod b_i$ and as we can check that $|\Lambda| \leq p^{k-1}$, we get (3.8) follows from

$$\prod_{i=1}^{k} b_i \geq \frac{1}{p},$$

or written into another way

$$w(k) \leq p \tag{3.9}$$

with

$$w(k) = (\frac{2^{1/2}\pi L}{3^{1/2}\epsilon^{1/2}|C|^{1/2}})^k(\prod_{x\in R}|\widehat{C}(x)|)^{1/2}.$$

Now we can use the arithmetic-geometric inequality to say that we have

$$(\prod_{x\in R}|\widehat{C}(x)|)^{1/k} \leq (\frac{1}{k}\sum_{x\in R}|\widehat{C}(x)|^2)^{1/2}.$$

Besides, by (3.4)

$$\sum_{x\in R}|\widehat{C}(x)|^2 \leq p|C|, \tag{3.10}$$

and thus $w(k) \leq w_1(k)$, with

$$w_1(k) = ((2/3)^2\pi^4 L^4 \frac{p}{k\epsilon^2|C|})^{k/4}.$$

From (3.10) we also obtain $k < p\epsilon^{-2}|C|^{-1}$ and since $w_1(k)$ is an increasing function in this range, we have

$$w_1(p\epsilon^{-2}|C|^{-1}) \leq p \tag{3.11}$$

implies (3.7). But (3.11) holds with

$$\epsilon \geq (\frac{\log((2/3)^{1/2}\pi L)p}{\log p|C|})^{1/2},$$

hence we deduce the statement of the lemma. □

The following result is equivalent to Proposition 3 in [GrRu], and will be fundamental in the proof of the theorem.

Proposition 3.8. *Let A, B two subset of $\mathbb{Z}/p\mathbb{Z}$, and let $\epsilon_1, \epsilon_2 > 0$, $m \in \mathbb{N}$. If d is good length for A then the (m,d)-granularizations A' and B' (with respect to ϵ_1) holds that $A+B$ contains every x for which $A' * B'(x) \geq \epsilon_2 p$, with at most*

$$\frac{324\log((2/3)^{1/2}\pi L)}{\epsilon_1^4\epsilon_2^2\log p}\frac{|A||B|}{p}$$

exceptions.

Proof: Let C a subset of $\mathbb{Z}/p\mathbb{Z}$. We define the function $f_{C,d} : \mathbb{Z}/p\mathbb{Z} \to \mathbb{R}$ as

$$f_{C,d}(n) = \frac{1}{|dP|}(C * dP)(n) = \frac{1}{|dP|}|C \cap (dP + n)|,$$

where $P = \{-(L-1), \ldots, -2, -1, 0, 1, 2, \ldots, (L-1)\}$. Note that $\widehat{f_{C,d}}(x) = \widehat{C}(x)g_d(x)$, with $g_d(x) = (|dP|)^{-1}\widehat{dP}(x)$. Applying Plancherel identity (3.4) twice we have

$$\begin{aligned}
\sum_n |(A*B)(n) - (f_{A,d} * f_{B,d})(n)|^2 &= p^{-1}\sum_x |\widehat{A}(x)\widehat{B}(x) - \widehat{f_{A,d}}(x)\widehat{f_{B,d}}(x)|^2 \\
&= p^{-1}\sum_x |\widehat{B}(x)|^2|\widehat{A}(x)|^2(1-g_d(x)^2)^2 \\
&\leq (\max_x |\widehat{A}(x)||1-g_d(x)^2|)^2 \sum_x \frac{|\widehat{B}(x)|^2}{p} \\
&\leq |B|(\max_x |\widehat{A}(x)||1-g(x)^2|)^2.
\end{aligned}$$

Since $|1-g_d(x)^2| = |(1+g_d(x))(1-g_d(x))| \leq 2|1-g_d(x)|$, by applying Lemma 3.7 to the set A (because $1-g_d(x) = h_d(x)$) we get

$$\sum_n |(A*B)(n) - (f_A * f_B)(n)|^2 \leq 4\frac{\log((2/3)^{1/2}\pi L)}{\log p}|A||B|p. \qquad (3.12)$$

Moreover if $n \in A'$ there exists an arithmetic progression of difference d and length L containing to n and at least $\epsilon_1(L-1)$ point of A. On the

other hand, this progression is contained in $dP+n$. Hence $f_{A,d}(n)$ is at least $\epsilon_1(L-1)/(2L-1) \geq \epsilon_1/3$, and then $f_{A,d}(n) \geq \epsilon_1 A'(n)/3$ for any $n \in \mathbb{Z}/p\mathbb{Z}$. For similar reasons follows that $f_{B,d}(n) \geq \epsilon_1 B'(n)/3$. So we obtain for every n the inequality $(f_{A,d} * f_{B,d})(n) \geq \epsilon_1^2 (A' * B')(n)/9$.

Now let us consider the set $M = \{x \in \mathbb{Z}/p\mathbb{Z}; (A' * B')(x) \geq \epsilon_2 p, x \notin A+B\}$. We have

$$|(A*B)(n) - (f_{A,d} * f_{B,d})(n)|^2 \geq \frac{\epsilon_1^4 \epsilon_2^2 p^2}{3^4} \qquad \text{for any } n \in M.$$

Substituting in (3.12) we get

$$|M| \leq \frac{4\log((2/3)^{1/2}\pi L)(\log p)^{-1}|A||B|p}{\epsilon_1^4\epsilon_2^2 p^2/3^4} = \frac{324\log((2/3)^{1/2}\pi L)}{\epsilon_1^4\epsilon_2^2 \log p}\frac{|A||B|}{p}.$$

□

Roughly speaking this proposition says that, under certain conditions, we can split the set of pairs (A,B) into some few parts in such a way that in each of them the sumsets $A+B$ are very similar. This is the way in which we can see the overlapping that happens when adding sets.

Now we need a generalization of Cauchy-Davenport Theorem (inequality (3.1) due to Pollard [Pol].

Proposition 3.9. *Let $C, D \subset \mathbb{Z}/p\mathbb{Z}$, and for each $i \in \mathbb{Z}$ let $R_i = R_i(C,D) = \{n \in \mathbb{Z}/p\mathbb{Z} : (C*D)(n) \geq i\}$. Then for any $r \leq \min(|C|,|D|)$ we have*

$$|R_1| + |R_2| + \ldots + |R_r| \geq r(\min(p, |C|+|D|) - r).$$

We are going to use this result in order to handle the size of the set of elements that are representable in at least k distinct ways as sum of elements of C and D:

Proposition 3.10. *Let C, D subsets of $\mathbb{Z}/p\mathbb{Z}$. Let k a positive integer. Then, whenever the sizes of C and D are larger than $\sqrt{kp}$ we have*

$$|R_k| \geq \min(|C|+|D|, p) - 2\sqrt{kp}.$$

Proof: We have $|R_j| \leq |R_k|$ for any $j \geq k$. Thus, if $r \geq k$ then

$$r(\min(|C|+|D|,p) - r) \leq |R_1| + \ldots + |R_r| \leq (k-1)p + |R_k|r.$$

whence

$$|R_k| \geq \min(|C|+|D|,p) - r - (k-1)p/r.$$

Now, taking $r = [\sqrt{kp}\,]$ in Proposition 3.9 (which is possible because $[\sqrt{kp}\,] \leq \min(|C|,|D|)$) we obtain the result. □

We are already prepared to prove our main result.

Theorem 3.11. *Let p a prime integer. For every $\gamma(p) < k < p/8$ we have*

$$|T(k, \mathbb{Z}/p\mathbb{Z})| = 2^{\frac{p}{2}+O(\gamma(p))}$$

where $p(\log\log p)^{2/3}(\log p)^{-1/9} \ll \gamma(p) \ll p(\log\log p)^{2/3}(\log p)^{-1/9}$.

Proof: Let N, M be two m-granular sets. We define

$$\mathcal{F}(N,M) = \{A+B : A, B \subset \mathbb{Z}/p\mathbb{Z}, |A|, |B| \geq \gamma(p) \text{ and there exists}$$

d good length for A such that $N = A'(d), M = B'(d)$(with respect to ϵ_1)$\}$.

Then

$$|\{B+A; B, A \subset \mathbb{Z}/p\mathbb{Z}, |A|, |B| > \gamma(p)\}| \leq \sum_{\substack{N,M \\ m-\text{granular}}} |\mathcal{F}(N,M)|.$$

But

$$|\{(N,M) : N, M \ m\text{-granular subsets of } \mathbb{Z}/p\mathbb{Z}\}| \leq (p2^m)^2. \tag{3.13}$$

Now we shall bound $|\mathcal{F}(N,M)|$ for any pair of m-granular sets N, M. By (3.6) we deduce that if $A+B$ is in $\mathcal{F}(N,M)$ then A is a subset of N union with a set of at most $\epsilon_1 p$ points, and B is a subset of M union a set of at most $\epsilon_1 p$ points. Thus

$$|\mathcal{F}(N,M)| \leq \text{number of choices for } (A,B) \leq 2^{|M|+|N|}\exp(C_1\log(1/\epsilon_1)\epsilon_1 p) \tag{3.14}$$

for some constant $C_1 > 0$. Moreover Proposition 3.8 says that if $A+B$ is in $\mathcal{F}(N,M)$ then $A+B$ contains to the set $R_{\epsilon_2 p}(N,M)$ menus a set of at most $\epsilon_3 p$ points (with $\epsilon_3 = 324\log((2/3)^{1/2}\pi L)\ (\log p)^{-1}\epsilon_1^{-4}\epsilon_2^{-2}$), or equivalently that $A+B$ is contained into the union of the complementary of $R_{\epsilon_2 p}(N,M)$ with a set of less than $\epsilon_3 p$ points.

Let ϵ_1, ϵ_2 with $\epsilon_1 + \epsilon_2^{1/2} \leq \gamma(p)$. As the sizes of A and B are larger than $\gamma(p)$ and $|N| \geq |A| - \epsilon_1 p$, $|M| \geq |B| - \epsilon_1 p$, we have $\min(|N|, |M|) \geq \gamma(p) - \epsilon_1 p \geq \epsilon_2^{1/2} p$. Hence we can apply Proposition 3.10 to the sets N y M, obtaining

$$|R_{\epsilon_2 p}(N,M)| \geq \min(|N|+|M|, p) - 2\epsilon_2^{1/2} p.$$

Therefore

$$|\mathcal{F}(N,M)| = |\{(A+B)^c; A+B \in \mathcal{F}(N,M)\}| \leq 2^{p-(|N|+|M|-2\epsilon_2^{\frac{1}{2}}p)} e^{C_2\log(\frac{1}{\epsilon_3})\epsilon_3 p} \tag{3.15}$$

From the bounds (3.14) y (3.15) we get

$$|\mathcal{F}(N,M)| \leq 2^{p/2}\exp(C_3 p(\epsilon_2^{\frac{1}{2}} + \log(1/\epsilon_1)\epsilon_1 + \log(1/\epsilon_3)\epsilon_3)),$$

hence by (3.13) taking $1/L = \epsilon_2^{1/2} = \epsilon_1 \log(1/\epsilon_1)$, $\epsilon_1 = (\log p)^{-\frac{1}{9}}(\log\log p)^{-\frac{1}{3}}$ we deduce the upper bound of the theorem.

The lower bound is trivial. Let A, B be any pair of subset of $\mathbb{Z}/p\mathbb{Z}$, with $|A|, |B| > p/8$, and let $y = 0, x = \frac{p-1}{2}$. If $A \subset [1, [\frac{p-1}{4}]]$ and $B \subset [[\frac{p-1}{4}] + 1, \frac{p-1}{2}]$, then

$$(A \cup x) + (B \cup y) = ((A+B) \cup \{x+y\}) \cup (A+y) \cup (B+x),$$

where unions are disjoint, and thus

$$|\{B + A; B, A \subset \mathbb{Z}/p\mathbb{Z}, |A|, |B| > p/8\}| \gg \binom{[p/4]}{[p/8]}^2 = 2^{\frac{p}{2}+O(\gamma(p))}.$$

□

3.3 A-sets

In this section we are going to study the A-sets of G a finitely generated abelian group, focusing on the case $G = \mathbb{Z}$ and in particular in $|A| \leq 3$. First we are going to prove the existence of the constant $c(A, G)$ associated to the A-sets.

Lemma 3.12. *Let $G = H \times \mathbb{Z}^d$, H finite and A subset of G. There exists the limit*

$$c(A,G) = \lim_{N\to\infty} |S_N(A,G)|^{\frac{1}{N^d|H|}},$$

and we have $1 \leq c(A,G) \leq 2$.

Proof: For any $j, N \in \mathbb{N}$ we can write

$$\begin{aligned} S_{jN}(A,G) &= \{\bigcup_{h\in H}(B_h \times \{h\}) + A : B_h \subset I_{jN}^d \, \forall h \in H\} \\ &= \{\bigcup_{u\in I_j^d}(\bigcup_{h\in H}(B_{h,u} \times \{h\}) + A) : B_{h,u} \subset I_N^d + (u-w)N\} \end{aligned}$$

with $w = (1, 1, \ldots, 1) \in \mathbb{Z}^d$, whence we deduce that

$$|S_{jN}(A,G)| \leq |S_N(A,G)|^{j^d}. \tag{3.16}$$

Let $M \geq N$, with $M = aN + b$ and $0 \leq b \leq N - 1$. By (3.16) we have

$$|S_M(A,G)|^{M^{-d}} \leq |S_{(a+1)N}(A,G)|^{M^{-d}} \leq |S_N(A,G)|^{N^{-d}(1+N/M)^d}$$

and thus for any $N \in \mathbb{N}$ we have

$$\limsup_{M\to\infty} S_M(A,G)^{M^{-d}} \leq S_N(A,G)^{N^{-d}}.$$

Finally we arrive at the inequality

$$\limsup_{M\to\infty} S_M(A,G)^{M^{-d}} \leq \liminf_{M\to\infty} S_M(A,G)^{M^{-d}},$$

which implies the existence of the limit defining $c(A,G)$. Bound $c(A,G) \leq 2$ is trivial taking into account that $|S_N(A,G)| \leq |\mathcal{P}(H \times I_N^d)|$. □

The constant $c(A,G)$ has several properties:

Lemma 3.13. *For any $A' \subset G$ finite we have*

$$c(A + A', G) \leq c(A,G)$$

and for any $x \in G$, we have

$$c(A + x, G) = c(A,G).$$

Proof: Let $G = \mathbb{Z}^d \times H$, with H finite. There exists $r \in \mathbb{N}$ such that $A' \subset I_r^d$. In this way, we have $S_N(A + A', G) \subset S_{N+r}(A,G)$ for any $N \in \mathbb{N}$, which proves $c(A + A', G) = c(A,G)$. To prove $c(A + x, G) = c(A,G)$ we notice that the application $C \mapsto C + x$ defines a bijection from $S_N(A,G)$ into $S_N(A + x, G)$. □

Besides, we have the following fundamental result.

Lemma 3.14. *Let λ and automorphism of $G = \mathbb{Z}^d \times H$. We have*

$$c(\lambda A, G) = c(A,G).$$

Proof:

$$S_N(A,G) = \{B + \lambda A : B \subset I_N^d \times H\},$$

hence

$$|S_N(A,G)| = |\{B + A : B \subset \lambda^{-1} I_N^d \times H\}|.$$

For any $N \in \mathbb{N}$, there exist $R_N \in \mathbb{N}$ and $(v_k)_{1\leq k\leq R_N}$, $v_k \in \mathbb{Z}^d$ such that

$$\lambda^{-1} I_{N^2}^d \subset \bigcup_{k=1}^{R_N} (I_N^d + N v_k),$$

and with $R_N|I_N^d| \sim |\lambda^{-1} I_{N^2}^d| = |I_{N^2}^d|$. Thus

$$|S_{N^2}(\lambda A, G)| \leq |S_N(A, G)|^{R_N}$$

and for $N \to \infty$ we have

$$c(\lambda A, G) \leq c(A, G).$$

Considering this inequality for the automorphism λ^{-1} we obtain the identity of the statement. □

Remark 3.15. This result allows to extend the definition of the constant associated to the A-sets to any finitely generated abelian group: if λ is an isomorphism from G to $\mathbb{Z}^d \times H$ and $A \subset G$ we define $c(A, G) = c(\lambda A, \mathbb{Z}^d \times H)$ (the previous lemma assures that the definition does not depend on λ). Moreover the constant does not change under group isomorphisms.

Lemma 3.16. *Let λ a injective endomorphism of G. We have*

$$c(\lambda A, G) = c(A, G).$$

Proof: Let $G = \mathbb{Z}^d \times H$, H finite group. By the previous lemma, is enough to demonstrate $c(fA, G) = c(A, G)$ where

$$f((a_1, \ldots, a_d, h)) = (\lambda a_1, \ldots, a_d, h), \qquad \lambda \in \mathbb{N}.$$

The image $f(G)$ equals $(\lambda\mathbb{Z}) \times \mathbb{Z}^{d-1} \times H$, which permits to write G as the disjoint union

$$G = \bigcup_{j=1}^{\lambda} g_j + \lambda\mathbb{Z} \times \mathbb{Z}^{d-1} \times H.$$

where g_j are representatives of the classes of the group G/fG. Therefore

$$S_{\lambda N}(fA, G) = \{\bigcup_{j=1}^{\lambda} (g_j + f(B_j + A)) : B_j \subset I_N \times I_{\lambda N}^{d-1} \times H \, \forall j \in I_\lambda\}$$

and

$$|S_{\lambda N}(fA, G)| = |\{B + A : B \subset I_N \times I_{\lambda N}^{d-1} \times H\}|^{\lambda}. \tag{3.17}$$

Hence $|S_{\lambda N}(fA, G)| \leq |S_N(A, G)|^{\lambda^d}$ which proves $c(fA, G) \leq c(A, G)$. On the other hand, writing $w = (1, 0, \ldots, 0) \in G$, we have

$$S_{\lambda N}(A, G) = \{\bigcup_{j=1}^{\lambda} B_j + A + jNw : B_j \subset I_N \times I_{\lambda N}^{d-1} \times H\}$$

and using (3.17) we see that $|S_{\lambda N}(A,G)| \leq |S_{\lambda N}(fA,G)|$, which proves the lemma. □

Let C an A-set of a group G. We can always construct the set

$$B_0 = \bigcup_{B\subset G,\, B+A=C} B.$$

Moreover we have $C = B_0 + A$, and B_0 can be explicitly expressed as the set $i_A(C) = \cap_{a\in A}(C-a)$. Thus, we see that to be A-set amounts to satisfy the condition

$$C = i_A(C) + A.$$

In this way, for an abelian group $G = \mathbb{Z}^d \times H$, H finite, and for any finite subset A we define

$$U_A(N,G) = \{C \subset I_N^d \times H : C = i_A(C) + A\}.$$

If $0 \in A$, then there exists $r \in \mathbb{N}$ such that for any $N > r$ we have that if $B \subset I_N^d \times H$ then $B + A \subset I_{N+r}^d \times H$, and besides $i_A(C) \subset C$ for every C. Therefore we have

$$S_{N-r}(A,G) \subset U_A(N,G) \subset S_N(A,G).$$

From these reasonings we deduce:

Lemma 3.17. *Let $A \subset G$ be a finite set. Then*

$$c(A,G) = \lim_{N\to\infty} |U_A(N,G)|^{1/N^d|H|}.$$

Remark 3.18. Identity $C = i_A(C) + A$ is equivalent to satisfy

$$C \subset \bigcup_{x\in A} \bigcap_{y\in A, y\neq x} C + x - y,$$

or also

$$c \in C \Rightarrow \exists x_c \in A \text{ such that } c + A \subset x_c + C.$$

In the case $G = \mathbb{Z}$ this reformulation will permit to calculate $c(A,\mathbb{Z})$ through a recurrence. Let d the smallest natural number such that $A \subset \{0,1,\ldots,d\}$ (by a translation we can suppose that 0 is the smallest element of A). We define $\Gamma_d = \{-d,\ldots,d\}$ and

$$\mathcal{E}_A = \{D \subset \Gamma_d : 0 \in D \Rightarrow \exists x \in A \text{ such that } A \subset D + x\}.$$

For any $D \subset \Gamma_d$ we define

$$v(D) = (D-1) \cap \Gamma_d$$

and

$$u(D) = v(D) \cup \{d\}.$$

We consider the bijection between the sets Γ_d and $I_{2^{2d+1}} - 1$ defined by $C \mapsto \sum_{j \in \Gamma_d} 2^{j+d} u_j$ where $u_j = 1$ if $j \in C$ and $u_j = 0$ if $j \notin C$. This bijection induces a order in the set Γ_d.

In this way we define $M_A = (m_{D,C})$ as the square matrix indexed in $\mathcal{P}(\Gamma_d) \times \mathcal{P}(\Gamma_d)$, with the order we have just described, and

$$m_{D,u(D)} = m_{D,v(D)} = 1 \qquad \text{if } D \in \mathcal{E}_A$$

and $m_{D,C} = 0$ otherwise. Since the matrix is non-negative, by the theory of Perron-Frobenius (see [MeyC]) we can say that the spectral radius ρ_A is a real eigenvalue of M_A and we have

$$\lim_{N \in \mathbb{N}} (\left\| M_A^N \right\|_1)^{1/N} = \rho_A.$$

But we have the following result.

Lemma 3.19. *Let $U_A(N) = U_A(N, \mathbb{Z})$. For every $N \in \mathbb{N}$, $N > 4d$ we have*

$$2^{-8d} \left\| M_A^N \right\|_1 \leq |U_A(N)| \leq \left\| M_A^N \right\|_1.$$

Proof: We can write

$$\begin{aligned} U_A(N) &= \{C \subset I_N : j \in C \Rightarrow \exists x_j \in A \text{ such that } j + A \subset x_j + C\} \\ &= \{C \subset I_N : (C-j) \cap \Gamma_d \in \mathcal{E}_A \, \forall j \in I_N \}. \end{aligned}$$

In this way, we consider the set

$$\Delta_N = \{(D_j)_{j \in I_N} \in \mathcal{P}(\Gamma_d)^N : m_{D_j, D_{j+1}} = 1 \, \forall j \in I_{N-1}\}.$$

On the one hand, the application

$$f : U_A(N) \longrightarrow \Delta_N$$

defined by $C \mapsto ((C-j) \cap \Gamma_d)_{j \in I_N}$ is an injection, hence $|U_A(N)| \leq |\Delta_N|$.

On the other hand, the application

$$g : \Delta_N \longrightarrow U_A(N)$$

defined by

$$(D_j)_{j\in I_N} \mapsto I_d \cup (I_d + N - d) \bigcup_{j=2d+1}^{N-2d} (D_j + j)$$

satisfies $|g^{-1}(C)| \leq 2^{8d}$ for any $C \in U_A(N)$ (because $g((D_j)_j) = g((D'_j)_j)$ implies that $D_j = D'_j$ for every $2d+1 \leq j \leq N-2d$). Thus $2^{8d}|U_A(N)| \geq |\Delta_N|$.

We conclude the proof noting that

$$|\Delta_N| = \sum_{\substack{(D_1,\dots,D_N)\\ D_j\in\mathcal{P}(\Gamma_d)}} m_{D_1,D_2}\dots m_{D_{N-1},D_N} = \left\|M_A^N\right\|_1.$$

□

As an outcome of this lemma we deduce that for any $A \subset \mathbb{Z}$ finite

$$c(A,\mathbb{Z}) = \rho_A.$$

When $A = \{0,1\}$, we have

$$\mathcal{E}_A = \{D \subset \{-1,0,1\} : 0 \in D \Rightarrow 0 \in (D-1)\cup(D+1)\} = \mathcal{P}(\Gamma_1)\setminus\{\{0\}\}$$

and

$$M_A = \begin{pmatrix} 1&1&0&0&0&0&0&0\\ 0&0&1&1&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&1\\ 1&1&0&0&0&0&0&0\\ 0&0&1&1&0&0&0&0\\ 0&0&0&0&1&1&0&0\\ 0&0&0&0&0&0&1&1 \end{pmatrix}.$$

Calculating the characteristic polynomial of this matrix we can see that ρ_A is the positive root of the equation

$$x^3 - 2x^2 + x - 1 = 0.$$

Therefore

Proposition 3.20. *We have*

$$c(2,\mathbb{Z}) = c(\{0,1\},\mathbb{Z}) = \rho$$

with $\rho = 1.75488\dots$ *the positive root of the equation*

$$x^3 - 2x^2 + x - 1 = 0.$$

In the same way we can calculate (by using the computer when the matrix is too large) the minimal polynomial $p_A(t)$ of ρ_A over $\mathbb{Z}$ for different sets A of small length:

$$A = \{0, 1, 2\} \quad \rho_A = 1.6180\ldots \quad p_A(t) = -1 - t + t^2$$

$$A = \{0, 1, 2, 3\} \quad \rho_A = 1.5000\ldots \quad p_A(t) = -1 + t^3 - 2t^4 + t^5$$

$$A = \{0, 1, 3\} \quad \rho_A = 1.6822\ldots \quad p_A(t) = 1 - 2t^4 + t^5 - t^6 + t^7 - t^8 + t^9 - 2t^{10} + t^{11}$$

$$A = \{0, 1, 2, 3, 4\} \quad \rho_A = 1.4655\ldots \quad p_A(t) = -1 - t^2 + t^3$$

$$A = \{0, 1, 2, 4\} \quad \rho_A = 1.5750\ldots$$
$$p_A(t) = 1 - 2t^5 + t^6 - t^7 + t^8 - t^9 + t^{11} - 2t^{12} + t^{13}$$

$$A = \{0, 1, 4\} \quad \rho_A = 1.6863\ldots$$
$$p_A(t) = 1 + 3t^5 + 2t^8 - t^9 - t^{10} + 2t^{11} - 6t^{12} + t^{13} + t^{16} - t^{18} + t^{19} - 2t^{20} + t^{21}$$

$$A = \{0, 1, 5\} \quad \rho_A = 1.6825\ldots$$
$$p_A(t) = -1 - 2t^3 - t^4 - t^6 - 3t^7 + t^8 + 2t^9 - 4t^{10} - 2t^{11} + t^{12} - 6t^{13} + 8t^{14} + t^{15} - 9t^{16}$$
$$+ 13t^{17} - 4t^{18} - 2t^{19} - 3t^{20} + 13t^{21} + 11t^{22} - 3t^{23} + 20t^{24} + 12t^{25} - 5t^{26} - 2t^{27} + 10t^{28}$$
$$- t^{29} - 10t^{30} - t^{31} + t^{32} - 11t^{33} + t^{34} - t^{35} + 4t^{36} - 2t^{37} + t^{38} + t^{39} - 2t^{40} + t^{42} - 2t^{43} + t^{44}$$

$$A = \{0, 2, 5\} \quad \rho_A = 1.6827\ldots \quad p_A(t) = 1 + t + 3t^2 + 3t^3 + 3t^4 + 4t^5 + t^6 + 2t^7 +$$
$$2t^8 - t^9 + 2t^{10} - 2t^{11} + 9t^{12} - t^{13} + 7t^{14} + 12t^{15} - 11t^{16} + 17t^{17} - 12t^{18} + 6t^{19} - 12t^{20} +$$
$$12t^{21} - 20t^{22} + 12t^{23} - 6t^{24} + 2t^{25} - 2t^{26} + 3t^{27} - 2t^{28} + t^{29} - t^{30} + t^{31} - 2t^{32} + t^{33}$$

For sets A with simple structure we are able to calculate $c(A, \mathbb{Z}) = \rho_A$. For example, we have

Proposition 3.21. *Let $k \in \mathbb{N}$, $k \geq 2$ y $A_k = \{0, 1, \ldots, k-1\}$. We have*

$$p_{A_k}(t) \mid t^{k+1} - 2t^k + t^{k-1} - 1$$

and thus

$$\rho_{A_k} = 1 + \frac{2\log(k-1)}{k-1}(1 + o(1)).$$

Proof: We could prove it by calculating the characteristic polynomial the matrix M_{A_k}, but

$$U_{A_k}(N) = \{C \subset I_N : x \in C \Rightarrow \exists j \in A_k, x - j + A_k \subset C\}$$

in a direct way we see that $U_{A_k}(N)$ can be expressed for $N \geq k+2$ as the disjoint union

$$U_{A_k}(N) = \Delta_1 \cup \Delta_2 \cup \Delta_3,$$

where

$$\Delta_1 = \{C_1 \cup \{N\} : C_1 \in U_{A_k}(N-1)\},$$

$$\Delta_2 = \{C_2 \cup (N - k + 1 + A_k) : C_2 \in U_{A_k}(N-k-1)\},$$

$$\Delta_3 = \{C_3 \cup \{N\} : C_3 \in U_{A_k}(N-1), N-1 \in C_3\},$$

whence we have the recurrence

$$|U_{A_k}(N)| = |U_{A_k}(N-1)| + |U_{A_k}(N-k-1)| + (|U_{A_k}(N-1)| - |U_{A_k}(N-2)|),$$

and we deduce the result for $p_{A_k}(t)$. From this follows the claim for ρ_{A_k}, taking into account $\rho_{A_k}^{k-1}(\rho_{A_k} - 1)^2 = 1$. □

However we do not know the way to control ρ_A in the general case. Considering

$$A_k = \{1, 2, 4, 6, \ldots, 2k\}$$

we notice (taking $B \subset 2\mathbb{Z}$) that for every $k \in \mathbb{N}$ we have

$$c(k, \mathbb{Z}) \geq \sqrt{2}.$$

We can prove a somewhat stronger result.

Proposition 3.22. *For any $k \in \mathbb{N}$ we have*

$$c(k, \mathbb{Z}) \geq 2^{\frac{1}{2} + 3^{-k}}.$$

Proof: Let A a finite subset of $\mathbb{Z}$ and $A' = \{1\} \cup 3A$. Writing

$$B = 3B_0 \cup (3B_1 + 1) \cup (3B_2 + 2)$$

we can see that

$$B + A' = [3(B_0 + A \cup B_2 + 1)] \cup [3(B_1 + A \cup B_0) + 1] \cup [3(B_2 + A \cup B_1) + 2]$$

and taking $B_2 = \emptyset$ we prove that

$$c(A', \mathbb{Z}) \geq 2^{\frac{1}{3}} c(A, \mathbb{Z})^{\frac{1}{3}}.$$

Beginning with $A_0 = \{0\}$ and defining $A_{j+1} = \{1\} \cup 3A_j$, by the inequality we have just demonstrated we have

$$c(A_k, \mathbb{Z}) \geq 2^{\frac{1}{2} + 3^{-k}}.$$

□

Taking into account Theorem 3.11 it seems reasonable to think that

$$\lim_{k \to \infty} c(k, \mathbb{Z}) = \sqrt{2}.$$

As a consequence of that theorem we can prove a partial result. Defining $\ell(A) = \sup_{a,a' \in A} |a - a'|$ we have

Proposition 3.23. *Let A, with $|A| = k$ and $\ell(A) = d \leq (1/2)k(\log k)^{1/10}$. Then*

$$c(A, \mathbb{Z}) \leq 2^{\frac{1}{2} + 2dk^{-1}(\log k)^{-1/10} + o(1)}.$$

Proof: Let p a prime in the interval $[k(\log k)^{10}, 2k(\log k)^{10}]$. We have $|A| = k \asymp p(\log p)^{-1/10}$, hence applying Theorem 3.11 we get

$$|S_{p-d}(A, \mathbb{Z})| \leq |S(A, \mathbb{Z}/p\mathbb{Z})| \leq 2^{\frac{p}{2} + o(p)}.$$

Besides, from (3.16) it can be deduced that $c(A, \mathbb{Z})^{p-d} \leq |S_{p-d}(A, \mathbb{Z})|$ and thus

$$c(A, \mathbb{Z}) \leq 2^{\frac{1}{2} + \frac{d}{k(\log k)^{1/10} - d} + o(1)} \leq 2^{\frac{1}{2} + 2dk^{-1}(\log k)^{-1/10} + o(1)}.$$

□

Corollary 3.24. *Let $\lambda > 0$ and*

$$c_\lambda(k, \mathbb{Z}) = \sup\{c(A, \mathbb{Z}) : |A| = k, \ell(A) \leq \lambda |A|\}.$$

Then

$$\lim_{k \to \infty} c_\lambda(k, \mathbb{Z}) = \sqrt{2}.$$

In the rest of the section we are going to treat $k = 3$. To this end we start generalizing the concept of sumset.

Let H be a finite abelian group, $l \in \mathbb{N}$ and $G = \mathbb{Z}^d \times H$. Let $f : G \to \mathcal{P}(G)$ be a real function such that $f(\cdot, h)$ is constant for every $h \in H$. From f we build the following function $\tilde{f} : \mathcal{P}(G) \to \mathcal{P}(G)$ defined by $\tilde{f}(B) = \bigcup_{b\in B}(b + f(b))$. For any $s \in \mathbb{Z}$, $0 \leq s \leq d$ and $D \subset G$, $D = \mathbb{Z}^s \times J$ and $J \subset \mathbb{Z}^{d-s} \times H$ a finite set we define (the existence of the limit is proved as in Lemma 3.12)

$$c(f, D, G) = \lim_{x\to\infty} |\{\tilde{f}(B) : B \subset I_N^s \times J\}|^{1/|I_N^s \times J|}.$$

When f is constantly equal to A we have $\tilde{f}(B) = B + A$ and we write $c(f, D, G) = c(A, D, G)$; moreover we abbreviate $c(f, G, G)$ as $c(f, G)$. With these notations we have the following result:

Theorem 3.25. *Let $a, b \in \mathbb{Z}$, $0 < a < b$ with $(a, b) = 1$. We have*

$$c(U_2, \mathbb{Z} \times I_{b-1}, \mathbb{Z}^2)^{1-1/b} \leq c(\{0, a, b\}, \mathbb{Z}) \leq c(U_2, \mathbb{Z} \times I_b, \mathbb{Z}^2),$$

with $U_2 = \{(0, 0), (1, 0), (0, 1)\}$.

Proof: Considering bijection

$$w : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

defined as $w(m) = ([m/b], m + b\mathbb{Z})$ (the quotient and the remainder when dividing by b), we deduce that

$$c(\{0, a, b\}, \mathbb{Z}) = c(f, \mathbb{Z} \times \mathbb{Z}/b\mathbb{Z})$$

with

$$f(m, \lambda) = \begin{cases} \{(0, 0), (1, 0), (0, a)\} & \text{if } 0 \leq \lambda \leq b - a - 1 \\ \{(0, 0), (1, 0), (1, a)\} & \text{if } b - a \leq \lambda \leq b - 1. \end{cases}$$

Besides, by the automorphism $a^{-1} : \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ follows that

$$c(f, \mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}) = c(g, \mathbb{Z} \times \mathbb{Z}/b\mathbb{Z})$$

with

$$g(m, \lambda) = \begin{cases} \{(0, 0), (1, 0), (0, 1)\} & \text{if } 0 \leq a\lambda \leq b - a - 1 \\ \{(0, 0), (1, 0), (1, 1)\} & \text{if } b - a \leq a\lambda \leq b - 1. \end{cases}$$

On the other hand we realize that

$$c(g', \mathbb{Z} \times I_{b-1}, \mathbb{Z}^2)^{1-1/b} \leq c(g, \mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}) \leq c(g', \mathbb{Z} \times I_b, \mathbb{Z}^2),$$

where g' is the function induced by g in the group $\mathbb{Z}^2$. Finally, bijections $d_j : \mathbb{Z}^2 \to \mathbb{Z}^2$ defined by $d_j(n,m) = (n,m)$ for $m \leq j$ and $d_j(n,m) = (n+1,m)$ for $m > j$ can be used to prove

$$c(g', \mathbb{Z} \times I_b, \mathbb{Z}^2) = c(U_2, \mathbb{Z} \times I_b, \mathbb{Z}^2).$$

□

Corollary 3.26. *With the hypothesis of Theorem 3.25 we have*

$$c(U_2, \mathbb{Z}^2)^{1-1/b} \leq c(\{0,a,b\}, \mathbb{Z}) \leq c(U_2, \mathbb{Z}^2)^{1+1/b}$$

and in particular

$$\lim_{b\to\infty} c(\{0,a,b\}, \mathbb{Z}) = c(U_2, \mathbb{Z}^2).$$

Proof: This is a consequence of Theorem 3.25 and of inequalities

$$c(U_2, \mathbb{Z}^2) \leq c(U_2, \mathbb{Z} \times I_b, \mathbb{Z}^2) \leq c(U_2, \mathbb{Z}^2)^{1+1/b}.$$

□

Remark 3.27. If we would know that $c(U_2, \mathbb{Z} \times I_b, \mathbb{Z}^2)$ decreases when b increases, we could prove by using Theorem 3.25 that

$$c(3, \mathbb{Z}) < c(\{0,1\}, \mathbb{Z}),$$

but using a computer in order to obtain several characteristic polynomials associated to the constants $c(U_2, \mathbb{Z} \times I_b, \mathbb{Z}^2)$.

Remark 3.28. Until now we have not been capable of finding the value of $c(U_2, \mathbb{Z}^2)$. We even do not know how to solve a simpler problem: to calculate the number of subsets of I_n^2 (for large n) not containing a pair of points at distance 1. The only related question we know is that of calculating the number of ways in which on can fill I_n^2 with dominoes, which is solved in section 4 of [Lov].

Theorem 3.29. *We have*

$$c(\{(0,0),(1,0),(0,1)\}, \mathbb{Z}^2) < c(\{0,1\}, \mathbb{Z}).$$

Proof: We check that $c(\{0,1\}, \mathbb{Z}) = c(\{(0,0),(1,0)\}, \mathbb{Z}^2)$. For any set $D = B + \{(0,0),(1,0),(0,1)\}$ with $B \subset \mathbb{N}^2$ finite, we are going to build a set $D' = B' + \{(0,0),(1,0)\}$ with $B' \subset \mathbb{Z}^2$ finite. To this end we proceed as follows:

Let $M \in \mathbb{N}$ such that $D \subset I_M^2$, then we begin from point (M, M). From there we go to the point $(M-1, M)$, and then to $(M-2, M)$ and we continue in the same way until we arrive at $(1, M)$. Then we go to point $(M, M-1)$ and after that to $(M-1, M-1)$. In general we go from the point (a_0, b_0) to $(a_0 - 1, b_0)$ except when $a_0 = 1$, that we go to $(M, b_0 - 1)$. In this way we continue until arriving at $(1, 1)$. Following this path, we do not change the set D on which we are moving except when we are at a point $x_0 \in D$ such that $x_0 + (1, 0)$ and $x_0 + (-1, 0)$ are not in D. In this case, we change D locally. We begin by defining some abbreviations: $\mathtt{o} \equiv x_0 + (-4, 0) \notin D$, $\mathtt{r} \equiv x_0 + (-3, 0) \notin D$, $\mathtt{s} \equiv x_0 + (-3, -1) \notin D$, $\mathtt{u} \equiv x_0 + (-2, 0) \notin D$, $\mathtt{v} \equiv x_0 + (-2, -1) \notin D$, $\mathtt{w} \equiv x_0 + (-2, -2) \notin D$, $\mathtt{x} \equiv x_0 + (-1, 0) \notin D$, $\mathtt{y} \equiv x_0 + (-1, -1) \notin D$, $\mathtt{z} \equiv x_0 + (-1, -2) \notin D$, $\mathtt{a} \equiv x_0 \notin D$, $\mathtt{b} \equiv x_0 + (0, -1) \notin D$, $\mathtt{c} \equiv x_0 + (0, -2) \notin D$, $\mathtt{d} \equiv x_0 + (1, 0) \notin D$, $\mathtt{e} \equiv x_0 + (1, -1) \notin D$, $\mathtt{f} \equiv x_0 + (1, -2) \notin D$, $\mathtt{g} \equiv x_0 + (2, 0) \notin D$, $\mathtt{h} \equiv x_0 + (2, -1) \notin D$, $\mathtt{i} \equiv x_0 + (2, -2) \notin D$, $\mathtt{j} \equiv x_0 + (3, 0) \notin D$, $\mathtt{l} \equiv x_0 + (3, -2) \notin D$, $\mathtt{n} \equiv x_0 + (4, -1) \notin D$, $\mathtt{ñ} \equiv x_0 + (4, -2) \notin D$, $\mathtt{q} \equiv x_0 + (5, -2) \notin D$. In the same way we define the equivalents with capital letters meaning the same but with the relation of ownership; for example $\mathtt{H} \equiv x_0 + (2, -1) \in D$. For convenience we also abbreviate $\Delta \equiv \mathtt{xABCdEFI}$, $\vartheta \equiv \mathtt{rUVxYABcdE}$, $\gamma \equiv \vartheta\mathtt{WZ}$, $\lambda \equiv \mathtt{XAbdEH}$, $\tau \equiv \mathtt{xaBDEGh}$, $\sigma \equiv \mathtt{vxYABDE}$. In this way, we modify the set D locally according to the following rules (whenever there is a coincidence between different rules, the one with largest number will be chosen):

1) $\mathtt{xABdE} \mapsto \mathtt{xaBdE}$.
2) $\Delta\mathtt{H} \mapsto \lambda\mathtt{cfi}$.
3) $\Delta\mathtt{GHJKLÑq} \mapsto \mathtt{xabcdEfGHiJKlñq}$.
4) $\Delta\mathtt{GHJKLÑQ} \mapsto \mathtt{xabcdEfGHiJKlÑQ}$.
5) $\Delta\mathtt{HLñ} \mapsto \lambda\mathtt{cfILñ}$.
6) $\Delta\mathtt{wZHL} \mapsto \lambda\mathtt{wZCfIL}$.
7) $\Delta\mathtt{wZHl} \mapsto \lambda\mathtt{wZCfil}$.
8) $\Delta\mathtt{gh} \mapsto \tau\mathtt{cfi}$.
9) $\Delta\mathtt{ghLñ} \mapsto \lambda\mathtt{cfgILÑ}$.
10) $\Delta\mathtt{GhJ} \mapsto \tau\mathtt{CFiJ}$.
11) $\Delta\mathtt{GhJLñ} \mapsto \mathtt{xabcdEfGHIJLñ}$.
12) $\Delta\mathtt{wZhL} \mapsto \lambda\mathtt{WZCfIL}$.
13) $\Delta\mathtt{wZhl} \mapsto \lambda\mathtt{WZCfil}$.
14) $\Delta\mathtt{vY} \mapsto \sigma\mathtt{cFI}$.
15) $\Delta\mathtt{vwYZ} \mapsto \sigma\mathtt{wzCFI}$.
16) $\vartheta\mathtt{Sw} \mapsto \mathtt{rSUVwXyaBcdE}$.
17) $\gamma \mapsto \mathtt{ruVWXYZAbcde}$.
18) $\gamma\mathtt{oHk} \mapsto \mathtt{ORuVWxYZAbcDehk}$.
19) $\gamma\mathtt{OHk} \mapsto \mathtt{ORuVWXYZAbcdehk}$.

In this way, when we arrive at the point $(1, 1)$ the set D have already been transformed into the set D' that we named at the beginning of the proof. In fact, for any $N \in \mathbb{N}$ this transformation defines and injection from $S_N(\{(0,0),(1,0),(0,1)\}, \mathbb{Z}^2)$ into $S_{N+10}(\{(0,0),(1,0)\}, \mathbb{Z}^2)$, which proves that $c(\{(0,0),(1,0),(0,1)\}, \mathbb{Z}^2) \leq c(\{0,1\}, \mathbb{Z})$.

Besides, defining $A = \{(x, y) \in \mathbb{Z}^2 : \max(|x|, |y|) \leq 10\}$ one can check that for any set D' in the image of the application and for any $x_0 \in \mathbb{Z}^2$ we

have $D' \cap (x_0 + A) \neq \{x_0 - (1,0), x_0, x_0 + (1,0)\}$. Let us see that this already demonstrates the strict inequality between the constants:

For what we have just proved we deduce that

$$c(U_2, \mathbb{Z}^2)^{N^2+o(N^2)} \leq |\{C \subset I_N^2 : C \text{ is } V\text{-set}, (C - x_0) \cap A \neq A^* \forall x_0 \in \mathbb{Z}^2\}|$$

with $A^* = \{(-1,0), (0,0), (1,0)\}$ and $V = \{(0,0), (1,0)\}$. Hence

$$c(U_2, \mathbb{Z}^2)^{(21N)^2+o(N^2)} \leq |\Omega_{21N}|^N$$

with

$$\Omega_N = \{D \subset I_N \times I_{21} : D \text{ is } V\text{-set}, \ (D - (a, 11)) \cap A \neq A^* \ \forall a \in \mathbb{Z}\}.$$

On the other hand

$$c(V, \mathbb{Z}^2)^{(21N)^2+o(N^2)} = |\{D \subset I_{21N} \times I_{21} : D \text{ is } V\text{-set } \}|^N.$$

We have $|\Omega_{jN}| \leq |\Omega_{N+1}|^j$ for any $j \in \mathbb{N}$, which proves the existence of

$$c_0 = \lim_{N \to \infty} |\Omega_N|^{1/N}$$

and the inequality $|\Omega_N| \geq c_0^{N-1}$. We conclude that

$$|\{D \subset I_{21N} \times I_{21} : D \text{ is } V\text{-set } \}| \geq \sum_{k=0}^{N} \binom{N}{k} c_0^{21N-21k-1} = c_0^{-1}(c_0^{21} + 1)^N$$

whence

$$c(V, \mathbb{Z}^2)^{21^2} \geq c(U_2, \mathbb{Z}^2)^{21^2} + 1.$$

□

Corollary 3.30. *There exists $b_0 \in \mathbb{N}$ such that for any $b \geq b_0$ and $(a, b) = 1$ we have*

$$c(\{0, a, b\}, \mathbb{Z}) < c(\{0, 1\}, \mathbb{Z}).$$

Remark 3.31. The injection of Theorem 3.29 seems to indicate that something similar can be done for the remaining sets $\{0, a, b\}$.

3.4 A-sets modulo p

In this section we shall study the number of A-sets of $\mathbb{Z}/p\mathbb{Z}$, with p prime, where A is any set with more than one element, proving Theorem 3.6.

Let $a, b, c \in \mathbb{Z}$, holding $0 \le b/2 \le c \le b \le a \le p$. We define the following sets:

$$G(b,c) = \{B \subset \mathbb{Z}/p\mathbb{Z} : |B| = c, |B + \{0,1\}| = b\}.$$

$$F(b,a) = \{E : B + \{0,1\} \subset E, B \subset \mathbb{Z}/p\mathbb{Z}, |E| = a, |B + \{0,1\}| = b\}.$$

In order to study the behaviour of these sets when a, b and c varies.

Lemma 3.32. *Let $0 < \alpha/2 < \lambda < \alpha < 1$, with $\alpha p, \lambda p$ integers. Then*

i) we have

$$|G(\alpha p, \lambda p)| \ll p g(\alpha,\lambda)^p,$$

where

$$g(\alpha,\lambda) = \frac{\lambda^\lambda}{(\alpha-\lambda)^{(\alpha-\lambda)}(2\lambda-\alpha)^{(2\lambda-\alpha)}} \frac{(1-\lambda)^{1-\lambda}}{(\alpha-\lambda)^{(\alpha-\lambda)}(1-\alpha)^{(1-\alpha)}}.$$

ii) Let $g_1(\alpha) = \max_{\alpha/2 \le \lambda \le \alpha} g(\alpha,\lambda)$. Then g_1 is increasing $\forall \alpha$, $0 \le \alpha < 3/4$.

Proof: We notice that

$$G(\alpha p, \lambda p) = \{B \subset \mathbb{Z}/p\mathbb{Z} : |B| = \lambda p, B \text{ is the union of } (\alpha-\lambda)p \text{ intervals}\},$$

where interval means a sequence $\{a, a+1, a+2, \ldots, a+k-1\} \subset B$ (with $k \ge 1$) such that $a-1 \notin B$ y $a+k \notin B$. Then we can write $B = \cup_{r=1}^{(\alpha-\lambda)p} I^{(r)}$ with $I^{(r)}$ an interval. Hence we can identify up to translation any set B with an element $(i_1, j_1, i_2, j_2, \ldots, i_{(\alpha-\lambda)p}, j_{(\alpha-\lambda)p})$ of $\mathbb{N}^{2(\alpha-\lambda)p}$ satisfying the conditions $i_r, j_r \ge 1$,

$$i_1 + i_2 + \ldots + i_{(\alpha-\lambda)p} = \alpha p$$

and

$$j_1 + j_2 + \ldots + j_{(\alpha-\lambda)p} = (1-\alpha)p.$$

(i_r is the size of $I^{(r)}$ and j_r is the number of elements of $\mathbb{Z}/p\mathbb{Z}$ between $I^{(r)}$ and $I^{(r+1)}$). Thus, the number of elements in $G(\alpha p, \lambda p)$ is bounded by

$$p\binom{\lambda p - 1}{(\alpha-\lambda)p-1}\binom{(1-\lambda)p-1}{(\alpha-\lambda)p-1},$$

(factor p comes from possible translations). By using Stirling's formula we obtain i).

For ii), differentiating g with respect to λ, we deduce that g is increasing in λ if and only if $r(\lambda) > 0$, where

$$r(\lambda) = \lambda(\alpha - \lambda)^2 - (2\lambda - \alpha)^2(1 - \lambda).$$

But $r(\alpha/2) > 0$, $r(\alpha) < 0$ and there is only one root (that we shall call $\lambda_{max}(\alpha)$) of equation $r(\lambda) = 0$ in the interval $\alpha/2 < \lambda < \alpha$. It is obvious that $g(\alpha, \lambda_{max}(\alpha)) = g_1(\alpha)$. Hence if g is increasing in α for $\lambda = \lambda_{max}(\alpha)$ then g_1 is also increasing due to the inequalities

$$g_1(\alpha) = g(\alpha, \lambda_{max}(\alpha)) \leq g(\alpha + \Delta, \lambda_{max}(\alpha)) \leq g_1(\alpha + \Delta)$$

(for $\Delta > 0$ sufficiently small). Calculating $\partial g/\partial\alpha$ we realize that g is increasing in α for any α holding

$$\alpha - \lambda < \lambda(1 - \lambda), \tag{3.18}$$

that under our conditions is equivalent to

$$\lambda > \lambda_0(\alpha) \tag{3.19}$$

with $\lambda_0(\alpha) = 1 - \sqrt{1 - \alpha}$. In this way, if $\lambda_{max}(\alpha) > \lambda_0(\alpha)$ then g_1 is increasing for this α. But it happens if and only if $r(\lambda_0(\alpha)) > 0$. Since $\lambda_0(\alpha)$ satisfies (3.18), we have

$$r(\lambda_0(\alpha)) = \lambda_0(\alpha)^3(1 - \lambda_0(\alpha))(1 - 2\lambda_0(\alpha)),$$

and then

$$r(\lambda_0(\alpha)) > 0 \Leftrightarrow \lambda_0(\alpha) = 1 - \sqrt{1 - \alpha} < 1/2 \Leftrightarrow \alpha < 3/4.$$

□

Lemma 3.33. *Let $0 < \alpha < \delta < 1$, p prime and $\alpha p, \delta p \in \mathbb{N}$. We have*

$$|F(\alpha p, \delta p)| \ll p^3(\max_{\substack{0 \leq \alpha_0 \leq 1 \\ 0 \leq \alpha_1 \leq \delta - \alpha}} f(\delta, \alpha_0, \alpha_1))^p$$

where $f(\delta, \alpha_0, \alpha_1)$ is the function

$$\frac{(1 - \delta)^{(1-\delta)}(2\delta - 1 + \alpha_0)^{2\delta - 1 + \alpha_0}}{\alpha_0^{\alpha_0}\alpha_1^{\alpha_1}(1 - \delta - \alpha_0 - \alpha_1)^{2(1-\delta-\alpha_0-\alpha_1)}(3\delta - 2 + \alpha_1 + 2\alpha_0)^{3\delta - 2 + \alpha_1 + 2\alpha_0}}.$$

Proof: Let n_i the number of intervals of length i in E $\forall i \geq 1$, and n_0 the number of elements $s \in \mathbb{Z}/p\mathbb{Z}$ such that $s \notin E$ and $s-1 \notin E$. Then we have $\sum_i in_i = \delta p$ y $\sum_i (i+1)n_i = p$. Besides, since $B + \{0,1\} \subset E$ and $B + \{0,1\}$ does not have isolated elements, we have $2n_2 + 3n_3 + \ldots \geq \alpha p$. Therefore $\sum n_i = (1-\delta)p$ and $n_1 \leq (\delta - \alpha)p$. In this way, the number of sets E satisfying lemma conditions will be up to translation smaller than or equal to

$$((1-\delta)p)! \times \text{ coefficient of } x^{(1-\delta)p} y^{\delta p} \text{ in } \sum_{n_0=0}^{\infty} \frac{x^{n_0}}{n_0!} \sum_{n_1=0}^{(\delta-\alpha)p} \frac{(xy)^{n_1}}{n_1!} \sum_{n_2=0}^{\infty} \frac{(xy^2)^{n_2}}{n_2!} \ldots$$

$$= \sum_{n_1=0}^{(\delta-\alpha)p} \sum_{n_0=0}^{\infty} \frac{((1-\delta)p)!}{n_0! n_1!} \times \text{ coefficient of } x^{(1-\delta)p-n_0-n_1} y^{\delta p - n_1}$$

$$\text{in } \exp(xy^2 + xy^3 + \ldots),$$

and expanding $\exp(\frac{xy^2}{1-y})$ this is equal to

$$\sum_{n_1=0}^{(\delta-\alpha)p} \sum_{n_0=0} \frac{((1-\delta)p)!}{n_0! n_1! ((1-\delta)p - n_1 - n_0)!} \times \text{ coefficient of } y^{(3\delta-2)p+n_1+2n_0}$$

$$\text{in } (1-y)^{-((1-\delta)p-n_0-n_1)} =$$

$$= \sum_{n_1=0}^{(\delta-\alpha)p} \sum_{n_0=0} \binom{(1-\delta)p}{n_0, n_1, (1-\delta)p - n_1 - n_0} \binom{(2\delta-1)p + n_0}{(1-\delta)p - n_1 - n_0}.$$

Using Stirling's formula for $n_0 = \alpha_0 p$ y $n_1 = \alpha_1 p$ and adding the factor p due to the translations we obtain the result. □

Theorem 3.34. *Let A a subset of $\mathbb{Z}/p\mathbb{Z}$, $|A| \geq 2$. Then*

$$|S(A, \mathbb{Z}/p\mathbb{Z})| \ll 1.9184^p$$

Proof: Let us take two different elements in $A \subset \mathbb{Z}/p\mathbb{Z}$, x and y. We have

$$S(A, \mathbb{Z}/p\mathbb{Z}) \subset \bigcup_{0 \leq b/2 \leq c \leq b \leq a \leq p} D_A(a,b,c)$$

where

$$D_A(a,b,c) = \{B + A : B \subset \mathbb{Z}/p\mathbb{Z}, |B+A| = a, |B + \{x,y\}| = b, |B| = c\}.$$

Then

$$|S(A,\mathbb{Z}/p\mathbb{Z})| \le (p+1)^3 \max_{0\le c\le b\le a\le p} |D_A(a,b,c)|. \tag{3.20}$$

Since for any $d \in (\mathbb{Z}/p\mathbb{Z})^\times$ the applications $M \mapsto dM$ and $M \mapsto M+d$ are bijections of $\mathcal{P}(\mathbb{Z}/p\mathbb{Z})$, we have $|D_A(a,b,c)| = |\overline{D}_{A'}(a,b,c)|$, where $A' = (y-x)^{-1}A$ and $\overline{D}_{A'}(a,b,c) = \{B+A' : B \subset \mathbb{Z}/p\mathbb{Z}, |B+A'| = a, |B+\{0,1\}| = b, |B| = c\}$. Moreover we have $\overline{D}_{A'}(a,b,c) \subset F(b,a)$ and $|\overline{D}_{A'}(a,b,c)| \le |G(b,c)|$. Thus

$$|D_A(a,b,c)| \le \min(|F(b,a)|, |G(b,c)|),$$

and finally by Lemmata 3.32*i*) and 3.33 and by (3.20), taking $a = \delta p, b = \alpha p, c = \lambda p$, we obtain

$$\begin{aligned} |S(A,\mathbb{Z}/p\mathbb{Z})| &\ll p^6(\max_{0<\lambda<\alpha<\delta<1}(\min(\max_{0\le\alpha_0\le 1, 0\le\alpha_1\le\delta-\alpha} f(\delta,\alpha_0,\alpha_1), g(\alpha,\lambda))))^p \\ &\ll p^6(\max_{0<\alpha<1} \min(f_1(\alpha), g_1(\alpha)))^p \end{aligned}$$

with

$$f_1(\alpha) = \max_{\substack{(\delta,\alpha_0,\alpha_1)\\ \delta-\alpha_1\ge\alpha}} f(\delta,\alpha_0,\alpha_1)$$

and $g_1(\alpha)$ defined as in Lemma 3.32. Note that $f_1(\alpha)$ is decreasing and by Lemma 3.32ii) $g_1(\alpha)$ is increasing if $0 \le \alpha < 3/4$.

Let $\widetilde{\alpha}$ be a real number with $0 \le \widetilde{\alpha} < 3/4$. If $\alpha < \widetilde{\alpha}$, then $g_1(\alpha) < g_1(\widetilde{\alpha})$. If $\alpha > \widetilde{\alpha}$ then $f_1(\alpha) < f_1(\widetilde{\alpha})$. Thus

$$\min(f_1(\alpha), g_1(\alpha)) \le \max(f_1(\widetilde{\alpha}), g_1(\widetilde{\alpha}))$$

for any α, and then

$$|S(A,\mathbb{Z}/p\mathbb{Z})| \ll p^6(\max(f_1(\widetilde{\alpha}), g_1(\widetilde{\alpha})))^p$$

for any $\widetilde{\alpha}$, $0 \le \widetilde{\alpha} \le 3/4$. We choose $\widetilde{\alpha} = 0.57402$. Using Lagrange multipliers we see that the maximum of the function $f(\delta,\alpha_0,\alpha_1)$ in the domain $\delta-\alpha_1 \ge \widetilde{\alpha}$ occurs at δ root of the equation

$$-1-15\widetilde{\alpha}-49\widetilde{\alpha}^2-51\widetilde{\alpha}^3-9\widetilde{\alpha}^4+23\delta+201\widetilde{\alpha}\delta+415\widetilde{\alpha}^2\delta+233\widetilde{\alpha}^3\delta+24\widetilde{\alpha}^4\delta-178\delta^2$$

$$-955\widetilde{\alpha}\delta^2-1158\widetilde{\alpha}^2\delta^2-347\widetilde{\alpha}^3\delta^2-16\widetilde{\alpha}^4\delta^2+635\delta^3+2023\widetilde{\alpha}\delta^3+1333\widetilde{\alpha}^2\delta^3+169\widetilde{\alpha}^3\delta^3$$

$$-1130\delta^4 - 1965\widetilde{\alpha}\delta^4 - 547\widetilde{\alpha}^2\delta^4 + 975\delta^5 + 715\widetilde{\alpha}\delta^5 - 325\delta^6 = 0$$

and at $\alpha_0 = \sqrt{(1-\delta)(\delta-\widetilde{\alpha})}$, $\alpha_1 = \delta - \widetilde{\alpha}$. As we know from the proof of Lemma 3.32*ii*), the maximum of $g(\widetilde{\alpha},\lambda)$ in the domain $0 \le \lambda \le \widetilde{\alpha}$ occurs at

λ root of the equation $r(\lambda) = 0$. Finally we obtain $\delta \approx 0.634563, \lambda \approx 0.36603$ and

$$|S(A, \mathbb{Z}/p\mathbb{Z})| \ll 1.9184^p.$$

□

Corollary 3.35. *We have*

$$c(2, \mathbb{Z})^{p+o(p)} \leq |T(2, \mathbb{Z}/p\mathbb{Z})| \ll 1.9184^{p+o(p)}$$

with $c(2, \mathbb{Z}) = 1.75488\ldots$ *the positive root of equation* $x^3 - 2x^2 + x - 1 = 0$.

Proof: Lower bound is trivial, taking into account Proposition 3.20. For the upper one, by Theorem 3.11 we know that

$$|T(\gamma(p), \mathbb{Z}/p\mathbb{Z})| = 2^{p/2+o(p)}.$$

Hence it only remains to study when $3 \leq |A| \leq \gamma(p)$. In this case we have

$$|\{B + A : A, B \subset \mathbb{Z}/p\mathbb{Z}, 3 \leq |A| \leq \gamma(p)\}| \leq p\binom{p}{\gamma(p)} \max_{3 \leq |A| \leq \gamma(p)} |S(A, \mathbb{Z}/p\mathbb{Z})|.$$

Since

$$p\binom{p}{\gamma(p)} = \exp(o(p)),$$

by Theorem 3.34 we obtain the result. □

Remark 3.36. We think that $|T(2, \mathbb{Z}/p\mathbb{Z})| = |\cup_{|A|=2} S(A, \mathbb{Z}/p\mathbb{Z})| + O(\alpha^p)$ for some $\alpha < c(2, \mathbb{Z})$, namely that the lower bound in the previous Theorem is the correct one. We have not been able to prove it, in part because when $|A| \geq 3$, actually in the proof we only use that $|A| \geq 2$. We should find the suitable way of using that $|A| \geq 3$.

Notation

$f \ll g \quad := \quad f = O(|g|).$

$f \sim g \quad := \quad \lim \dfrac{f}{g} = 1.$

$f \asymp g \quad := \quad g \ll f \ll g.$

$f = O(g) \quad := \quad \limsup \dfrac{|f|}{g} < \infty.$

$f = o(g) \quad := \quad \limsup \dfrac{f}{g} = 0.$

$f = \Omega(g) \quad := \quad \limsup \dfrac{|f|}{g} > 0.$

$\mathbb{I}_A \quad :=$ Characteristic function of the set A.

$|A| \quad :=$ Cardinal of the set A if it is finite, and Lebesgue measure of A if it is infinite.

$(a_1, a_2, \ldots, a_k) \quad :=$ Great common divisor of $a_1, a_2, \ldots, a_k$.

$d(n) \quad :=$ Number of divisors of n.

$\omega(n) \quad :=$ Number of prime factors of n.

$\chi \quad :=$ Dirichlet character.

$\left(\dfrac{d}{n}\right) \quad :=$ Legendre-Jacobi-Kronecker symbol.

$\widehat{f} \quad :=$ Fourier transform, $\widehat{f}(\xi) = \int_{-\infty}^{\infty} f(x)\, e^{-2\pi i \xi x}\, dx$.

$\mathcal{M}_f$:= Mellin transform, $\mathcal{M}_f(s) = \int_0^\infty f(x)\, x^{s-1}\, dx$.

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

$C_0^\infty(M)$:= Differentiable functions of any order with compact support M.

$p^k||n$:= $p^k|n$ and $p^{k+1} \not| n$.

$\dim_{\mathrm{H}} A$:= Hausdorff dimension of A.

$\dim_{\mathrm{M}} A$:= Minkowski dimension of A.

$\mathcal{H}^s(A)$:= Exterior s-dimensional Hausdorff measure of A.

$\mathrm{GL}(n, A)$:= Group of non-singular matrices $n \times n$ with coefficients in A.

$\mathrm{SL}(n, A)$:= Group of matrices $n \times n$ with determinant 1 and coefficients in A.

$L(s, \chi)$:= Dirichlet L-function attached to the character χ.

$\{x\}$:= Fractionary part of x.

$\|x\|$:= Distance to the nearest integer if $x \in \mathbb{R}$, and euclidean norm if it is a vector of more than one dimension.

$\mathrm{Li}(x)$:= Integral logarithm, $\mathrm{Li}(x) = \int_2^x \dfrac{dt}{\log t}$.

$\mu(n)$:= Möbius μ function, $\mu(1) = 1$, $\mu(n) = 0$ if n is not square-free and $\mu(n) = (-1)^k$ if n is a product of k different primes.

$\Lambda(n)$:= Von Mangoldt symbol, $\Lambda(n) = \log p$ if $n = p^k$ with p prime, and $\Lambda(n) = 0$ if $n \neq p^k$.

$\zeta(s)$:= Riemann ζ function.

$A^\times$:= Units of the ring A.

Bibliography

[Cal] A.-P. Calderón. Intermediate spaces and interpolation, the complex method. *Studia Math.*, 24 113–190, 1964.

[Cau] A. Cauchy. Recherches sur les nombres. *J. École Polytech*, 9 99–116, 1813.

[Cha] F. Chamizo. Automorphic forms and differentiability properties. *Trans. Amer. Math. Soc.*, 356 1909–1935, 2004.

[CC1] F. Chamizo, A. Córdoba. The fractal dimension of a family of Riemann's graphs. *C. R. Acad. Sci. Paris Sér. I Math.*, 317 455–460, 1993. (Erratum: *C. R. Acad. Sci. Paris Sér. I Math.* 320 649–650, 1995).

[CC2] F. Chamizo, A. Córdoba. Differentiability and dimension of some fractal Fourier series. *Adv. Math.*, 142 335–354, 1999.

[CCU] F. Chamizo, E. Cristóbal, A. Ubis. Visible points in the sphere. *Preprint.*

[CI1] F. Chamizo, H. Iwaniec. On the sphere problem. *Rev. Mat. Iberoamericana*, 11 417–429, 1995.

[CI2] F. Chamizo, H. Iwaniec. On the Gauss mean-value formula for class number. *Nagoya Math. J.*, 151 199–208, 1998.

[CU1] F. Chamizo, A. Ubis. An average formula for the class number. *Acta Arith.*, 122 75–90, 2006.

[CU2] F. Chamizo, A. Ubis. Some fourier series with gaps. To appear in *J. Anal. Math.*

[CR] K. Chandrasekharan, R. Narasimhan. Functional equations with multiple gamma factors and the average order of arithmetical functions. *Ann. of Math. (2)*, 76 93–136 1962.

[Che1] J.-R. Chen. Improvement of asymptotic formulas for the number of lattice points in a region of three dimensions. *Sci. Sinica*, 12 151–161, 1963.

[Che2] J.-R. Chen. Improvement on the asymptotic formulas for the number of lattice points in a region of the three dimensions. II. *Sci. Sinica*, 12 751–764, 1963.

[Cho] S. Chowla. On the k-analogue of a result in the theory of the Riemann zeta function. *Math. Z.*, 38 483–487, 1934.

[CiCo] J. Cilleruelo y A. Córdoba. *La teoría de los números*, Mondadori, Madrid, 1992.

[Dav1] H. Davenport. On the addition of residue classes. *J. London Math. Soc. 10, 30-32*, 1935.

[Dav2] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000.

[Dui] J. J. Duistermaat. Self-similarity of "Riemann's nondifferentiable function". *Nieuw Arch. Wisk. (4)*, 9 303–337, 1991.

[Fal1] K. J. Falconer. *The geometry of fractal sets*, volume 85 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1986.

[Fal2] K. J. Falconer. *Fractal geometry*. John Wiley & Sons Inc., Hoboken, NJ, second edition, 2003. Mathematical foundations and applications.

[Fre] G. A. Freĭman. *Foundations of a structural theory of set addition*. American Mathematical Society, Providence, R. I., 1973. Translations of Mathematical Monographs, Vol 37.

[Gau] C. F. Gauss. *Disquisitiones arithmeticae*. Springer-Verlag, New York, 1986.

[Ger1] J. Gerver. The differentiability of the Riemann function at certain rational multiples of π. *Amer. J. Math.*, 92 33–55, 1970.

[Ger2] J. Gerver. More on the differentiability of the Riemann function. *Amer. J. Math.*, 93 33–41, 1971.

[Ger3] J. Gerver. On cubic lacunary fourier series. *Trans. Amer. Math. Soc.*, 355 4297–4347, 2003.

[GH] D. Goldfeld, J. Hoffstein. Eisenstein series of 1/2-integral weight and the mean value of real Dirichlet L-series. *Invent. Math.*, 80 185–208, 1985.

[Gow1] W. T. Gowers. A new proof of Szemerédi's theorem for arithmetic progressions of length four. *Geom. Funct. Anal.*, 8 529–551, 1998.

[Gow2] W. T. Gowers. A new proof of Szemerédi's theorem. *Geom. Funct. Anal.*, 11 465–588, 2001. (Erratum: *Geom. Funct. Anal.*, 11 869, 2001).

[GR] I. S. Gradshteyn, I. M. Ryzhik. *Table of integrals, series, and products*. Academic Press Inc., Boston, MA, 1994.

[GK] S. W. Graham, G. Kolesnik. *van der Corput's method of exponential sums*, volume 126 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1991.

[GS] A. Granville, K. Soundararajan. The distribution of values of $L(1, \chi_d)$. *Geom. Funct. Anal.*, 13 992–1028, 2003. (Errata: *Geom. Funct. Anal.*, 14 245–246, 2004).

[GU] A. Granville, A. Ubis. Counting sumsets. *Preprint.*

[Gre1] B. Green. Arithmetic progressions in sumsets. *Geom. Funct. Anal.*, 12(3) 584–597, 2002.

[Gre2] B. Green. The Cameron-Erdős conjecture. *Bull. London Math. Soc.*, 36 769–778, 2004.

[GrRu] B. Green, I. Z. Ruzsa. Counting sumsets and sum-free sets modulo a prime. *Studia Sci. Math. Hungar.*, 41 285–293, 2004.

[GM] A. Grossmann, J. Morlet. Decomposition of Hardy functions into square integrable wavelets of constant shape. *SIAM J. Math. Anal.*, 15 723–736, 1984.

[Har] G. H. Hardy. Weierstrass's non-differentiable function. *Trans. Amer. Math. Soc.*, 17 301–325, 1916.

[HL] G. H. Hardy, J. E. Littlewood. Some problems of diophantine approximation. I. The fractional part of $n^k\Theta$. II. The trigonometrical series associated with the elliptic ϑ-functions. 1914.

[HB1] D. R. Heath-Brown. A mean value estimate for real character sums. *Acta Arith.*, 72 235–275, 1995.

[HB2] D. R. Heath-Brown. Lattice points in the sphere. In *Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997)*, pages 883–892. de Gruyter, Berlin, 1999.

[HW] E. Hernández, G. Weiss. *A first course on wavelets. Studies in Advanced Mathematics*. CRC Press, Boca Raton, FL, 1996.

[HT] M. Holschneider, Ph. Tchamitchian. Pointwise analysis of Riemann's "nondifferentiable" function. *Invent. Math.*, 105 157–175, 1991.

[Hoo] C. Hooley. On the Pellian equation and the class number of indefinite binary quadratic forms. *J. Reine Angew. Math.*, 353 98–131, 1984.

[Hör] L. Hörmander. *The analysis of linear partial differential operators. I*, volume 256 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1983. Distribution theory and Fourier analysis.

[IK] H. Iwaniec, Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[Jaf1] S. Jaffard. The spectrum of singularities of riemann's function. *Rev. Mat. Iberoamericana*, 12 441–460, 1996.

[Jaf2] S. Jaffard. Exposants de Hölder en des points donnés et coefficients d'ondelettes. *C. R. Acad. Sci. Paris Sér. I Math.*, 308 79–81, 1989.

[JM] S. Jaffard, Y. Meyer. Wavelet methods for pointwise regularity and local oscillations of functions. *Mem. Am. Math. Soc.*, 587 110 p., 1996.

[Kem] J. H. B. Kemperman. On small sumsets in an abelian group. *Acta Math.*, 103 63–88, 1960.

[Küh] M. Kühleitner. On the class number of binary quadratic forms: an omega estimate for the error term. *Math. Pannon.*, 13 63–78, 2002.

[Lan] E. Landau. *Elementary number theory*. Chelsea Publishing Co., New York, N.Y., 1958.

[LM] P. G. Lemarié, Y. Meyer. Ondelettes et bases hilbertiennes. *Rev. Mat. Iberoamericana*, 2 1–18, 1986.

[Lip] R. Lipschitz. Über die asymptotischen gesetze von gewissen gattungen zahlentheoretischer functionen. *Monatsber. Königl. Akad. Wiss. Berlin*, pages 174–185, 1865.

[Lov] L. Lovász. *Combinatorial problems and exercises*. North-Holland Publishing Co., Amsterdam, second edition, 1993.

[Mer] F. Mertens. Ueber einige asymptotische Gesetze der Zahlentheorie. 1873.

[MeyC] C. Meyer. *Matrix analysis and applied linear algebra*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2000.

[Mey] Y. Meyer. *Wavelets and operators*, volume 37 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1992.

[MS] S. D. Miller, W. Schmid. The highly oscillatory behavior of automorphic distributions for S$L(2)$. *Lett. Math. Phys.*, 69 265–286, 2004.

[Nat] M. B. Nathanson. *Additive number theory*, volume 165 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996. Inverse problems and the geometry of sumsets.

[Neu] E. Neuenschwander. Riemann's example of a continuous, 'nondifferentiable' function. *Math. Intelligencer*, 1 40–44, 1978/79.

[Pet] M. Peter. Mean values of Dirichlet L-series. *Math. Ann.*, 318 67–84, 2000.

[Pol] J. M. Pollard. A generalisation of the theorem of Cauchy and Davenport. *J. London Math. Soc. (2)*, 8 460–462, 1974.

[Pól] G. Pólya. Über die Verteilung der quadratischen Reste und Nichtreste. *Gött. Nach.* , 21–29, 1918.

[Que] H. Queffelec. Dérivabilité de certaines sommes de séries de Fourier lacunaires. *C. R. Acad. Sci. Paris Sér. A-B*, 273 A291–A293, 1971.

[Ruz1] I. Z. Ruzsa. Generalized arithmetical progressions and sumsets. *Acta Math. Hungar.*, 65 379–388, 1994.

[Ruz2] I. Z. Ruzsa. An analog of Freiman's theorem in groups. *Astérisque*, (258):xv, 323–326, 1999. Structure theory of set addition.

[Sar] P. Sarnak. Class numbers of indefinite binary quadratic forms. *J. Number Theory*, 15 229–247, 1982.

[SS] M. Sato, T. Shintani. On zeta functions associated with prehomogeneous vector spaces. *Ann. of Math. (2)*, 100 131–170, 1974.

[Shi] T. Shintani. On zeta-functions associated with the vector space of quadratic forms. *J. Fac. Sci. Univ. Tokyo Sect. I A Math.*, 22 25–65, 1975.

[Sie] C. L. Siegel. The average measure of quadratic forms with given determinant and signature. *Ann. of Math. (2)*, 45 667–685, 1944.

[Smi] A. Smith. The differentiability of Riemann's functions. *Proc. Amer. Math. Soc.*, 34 463–468, 1972.

[Ste] E. M. Stein. *Singular integrals and differentiability properties of functions*. Princeton Mathematical Series, No. 30. Princeton University Press, Princeton, N.J., 1970.

[Sze] E. Szemerédi. On sets of integers containing no four elements in arithmetic progression. *Acta Math. Acad. Sci. Hungar.*, 20 89–104, 1969.

[Tsa] K.-M. Tsang. Counting lattice points in the sphere. *Bull. London Math. Soc.*, 32 679–688, 2000.

[Ubi] A. Ubis. The error term in the average of class number. *Preprint.*

[Vau] R.C. Vaughan. *The Hardy-Littlewood method. 2nd ed.* Cambridge Tracts in Mathematics. 125. Cambridge: Cambridge University Press. vii, 232 p. , 1997.

[Vin1] I. M. Vinogradov. Eine neue Methode, die asymptotischen Ausdrücke der arithmetischen Funktionen zu finden. *Petrograd, Bull. Ac. Sc. (6) 11, 1347-1378* , 1917.

[Vin2] I. M. Vinogradov. Über den mittleren Wert der Klassenanzahl der binären quadratischen Formen von negativer Determinante. *Charikov, Comm. Soc. Math. (2) 16, 10-38* , 1918.

[Vin3] I. M. Vinogradov. 1. Über eine asymptotische Formel aus der Theorie der binären quadratischen Formen. 2. Sur la distribution des résidus et des nonrésidus des puissances. 3. Über die Verteilung der quadratischen Reste und Nichtreste. *1. Permi, Journ. Soc. Phys. et Math. de l'Univ. des Permi 1, 18-28 (1918 (1919)). 2. Ibid. 94-98 (1919). 3. Ibid. 2, 1-14* , 1919.

[Vin4] I. M. Vinogradov. Improvement of the remainder term of some asymptotic formulas. *Izvestiya Akad. Nauk SSSR. Ser. Mat.*, 13 97–110, 1949.

[Vin5] I. M. Vinogradov. Improvement of asymptotic formulas for the number of lattice points in a region of three dimensions. *Izv. Akad. Nauk SSSR. Ser. Mat.*, 19 3–10, 1955.

[Vin6] I. M. Vinogradov. On the number of integer points in a three-dimensional domain. *Izv. Akad. Nauk SSSR Ser. Mat.*, 27 3–8, 1963.

[Vor1] G. Voronoi. Sur un problème du calcul des fonctions asymptotiques. *J. für Math.*, 126 241-282, 1903.

[Vor2] G. Voronoi. Sur une fonction transcendante et ses applications à la sommation de quelques séries. *Ann. de l'Éc. Norm.*, 21 207–267, 459–533, 1904.

[Vos] A. G. Vosper. The critical pairs of subsets of a group of prime order. *J. London Math. Soc.*, 31 200–205, 1956.

[Wei] A. Weil. *L'intègration dans les groupes topologiques et ses applications*. Hermann, Paris, deuxième édition, 1965.

[Zyg] A. Zygmund. *Trigonometric series. Vol. I and II.* Cambridge University Press. XIV, 1977.