TECHNISCHE UNIVERSITÄT WIEN

VIENNA UNIVERSITY OF TECHNOLOGY

D I P L O M A R B E I T

Gelfond's Sum of Digits Problems

Ausgeführt am Institut für

Diskrete Mathematik und Geometrie

der Technischen Universität Wien

unter der Anleitung von Univ.Prof. Dipl.-Ing. Dr. techn. Michael Drmota

durch

Johannes Morgenbesser

Otterthal 82

2880 Kirchberg am Wechsel

Datum

Unterschrift

Contents

Preface

The main goal of my diploma thesis is the treatment of Gelfond's sum of digits problems as formulated in his paper *Sur les nombres qui ont des propriétés additives et multiplicatives données* in 1968. Gelfond showed that the sequence $(s_q(n))_{n\in\mathbb{N}}$, where $s_q(n)$ denotes the sum of digits of n in base q, is well distributed in arithmetic progressions. At the end of the paper, however, he raises the question as to whether this and related statements are still true for special subsequences of $(s_q(n))_{n\in\mathbb{N}}$.

Though Bésineau provided an asymptotic result of Gelfond's first problem concerning the joint distribution of the sum of digits function in 1972, it still took more than thirty years (1999) until Dong-Hyun Kim completely solved it. He proved that under certain conditions $\#\{1 \leqslant n \leqslant N : s_{q_i}(n) \equiv a_i \bmod m_i, 1 \leqslant i \leqslant l\} = N/(m_1 \cdots m_l) + O(N^{1-\lambda})$, where $\lambda > 0$. In particular, he derived an even stronger result by replacing the sum of digits functions with q-additive functions. In Chapter 4, I refine Kim's proof for the sum of digits function, which allows me to sharpen his result. Gelfond's second problem regards the sequence $(s_q(p))_{p\in\mathbb{P}}$. Until recently it was not even known whether there are infinitely many members of this sequence in special arithmetic progressions. Through the achievements of Mauduit and Rivat we now know that the sequence is actually well distributed in arithmetic progressions. This result and the developed proof method will surely have a major impact on the works of number theorists, although it is not published yet (to appear in Annals of Mathematics). I show the solution of Gelfond's second problem in Chapter 5, where I simplify Mauduit's and Rivat's proof by adapting some ideas Drmota, Mauduit, Rivat and Stoll used in other papers. The third and last problem is not entirely proved yet, but here again Mauduit and Rivat showed that the sequence $(s_q(n^2))_{n\in\mathbb{N}}$ is well distributed in arithmetic progressions (to appear in Acta Mathematica). This result is proved in Chapter 6.

Before Gelfond's problems will be dealt with in detail, a historical survey of the sum of digits function is provided in Chapter 1. This chapter also illuminates Gelfond's questions as already mentioned above and treats his results on the distribution of $s_q(n)$. Furthermore, some of his statements will be improved. Chapter 2 is dedicated to exponential sums, which are of particular significance in analytic number theory. Van der Corput's inequality, for instance, and an important result concerning quadratic Gauss sums are proved. Chapter 3 finally presents an extensive treatment of trigonometric products, which turns out to be the main technical point in solving Gelfond's problems. At the end of this diploma thesis, a short summary of fundamental definitions and results in analytic number theory is enclosed (see Appendix A).

Johannes Morgenbesser

Acknowledgments

First of all I would like to thank my supervisor Professor Dr. Michael Drmota, who, in several courses, has aroused my interest in number theory and drew my attention to Gelfond's sum of digits problems. He always took his time, provided helpful suggestions and offered advise and support whenever I had any questions. I also thank him and Professor Dr. Peter M. Gruber for enabling me to gather teaching experience as a tutor at the Institute of Discrete Mathematics and Geometry. In addition, I would like to thank Dr. Thomas Stoll. He carefully proof-read my diploma thesis and provided useful hints concerning mathematical documents. I appreciate his corrections and suggestions for improvement. Furthermore, I gratefully acknowledge Associate Professor Florin Boca's help during my semester abroad at the University of Illinois at Urbana-Champaign. He equally provided valuable tips as how to approach this specific problem in analytic number theory. This diploma thesis was written with support of the Austrian Science Foundation (FWF).
I also obtained great help from Philipp Harms, Martins Bruveris, Dipl.-Ing. Reinhard Kutzelnigg and Caroline Wappel. In particular, I owe a huge debt to Cornelia Spreitzer for her support and useful remarks. Finally, I would like to thank my parents who have always encouraged me and made it possible for me to even write these lines.

Chapter 1

Gelfond's Problems

Throughout this work, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote the sets of natural numbers, integers, rational numbers, real numbers and complex numbers. If x is a positive real number, we mark by $\log x$ the natural logarithm of x. If m and n are integers, then (m, n) denotes the greatest common divisor and $\operatorname{lcm}(m, n)$ the lowest common multiple of m and n. q is, unless otherwise stated, an integer $\geqslant 2$ and p a prime number. For the set of all primes, we use the common abbreviation $\mathbb{P}$. Furthermore, $\sum_{p\leqslant N}$ always means, that we only sum over primes less than or equal to N. We write for a (real or complex valued) function f

$$f(x) = O(g(x)) \quad \text{or} \quad f(x) \ll g(x),$$

if there exists a constant $C > 0$, such that $|f(x)| \leqslant C|g(x)|$. If the constant depends on a set of variables, say for example m and q, we write $f(x) = O_{m,q}(g(x))$ or $f(x) \ll_{m,q} g(x)$, respectively. The expression $f(x) = o(g(x)), x \to \infty$ means, that $\lim_{x\to\infty} f(x)/g(x) = 0$. If x is a real number, we have $\lfloor x \rfloor = \max\{n \in \mathbb{Z} : n \leqslant x\}$, $\lceil x \rceil = \min\{n \in \mathbb{Z} : n \geqslant x\}$ and $\|x\| = \min_{n\in\mathbb{Z}} |x - n|$ (distance from x to the nearest integer). Furthermore, we use the well-established abbreviation $\mathrm{e}(x) = \exp(2\pi i x)$ for a real number x.

1.1 The Sum of Digits Function

It is a well-known fact, that every non-negative integer can be written uniquely in base q as $n = \sum_{k\geqslant 0} n_k q^k$, where the integers n_k satisfy $0 \leqslant n_k \leqslant q-1$ and $n_k \neq 0$ for only finitely many. The sum of digits function in base q is defined by

$$s_q(n) = \sum_{k\geqslant 0} n_k.$$

In this section we want to shed light on the historical background of the sum of digits function. For further information see [1, Chapter 3] and [31].

It seems that the first mathematician who studied the sum of digits function was Prouhet (1851). He gives in [44] a solution to the so called Prouhet-Tarry-Escott problem (see [31]), which is the problem of finding two distinct sets of integers $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ such that the sum of all the k-th powers of the elements of each set is the same, where k is bounded by some integer k_0. Prouhet's solution for $n = q^r$ and $k < r$ consists in dividing the integers depending on the value modulo q of the sum of their digits in base q. If $q = 2$, the following result gives an answer to the Prouhet-Tarry-Escott problem. For any positive integers k and r with $k < r$, we have

$$\sum_{\substack{0\leqslant n<2^r \\ s_2(n)\equiv 0 \bmod 2}} n^k = \sum_{\substack{0\leqslant n<2^r \\ s_2(n)\equiv 1 \bmod 2}} n^k.$$

The next encounter with the sum of digits function was at the beginning of the twentieth century. In 1906 and 1912, the Norwegian mathematician Axel Thue (see [52, 51]) asked among other questions whether it is possible to find an infinite binary sequence that contains no cube, i.e. a sequence with no three consecutive identical blocks. Indeed, he could show that the sequence $\mathbf{t} = (s_2(n) \bmod 2)_{n\in\mathbb{N}}$ solves the problem. This sequence is now known as the Thue-Morse sequence (or Prouhet-Thue-Morse sequence), and it starts with following members

$$0\,1\,1\,0\,1\,0\,0\,1\,1\,0\,0\,1\,0\,1\,1\,0\,1\,0\,0\,1\,0\,1\,1\,0\ldots.$$

The Thue-Morse sequence arises in many different fields of mathematics and physics. For instance, Morse rediscovered this sequence in 1921 to show a result in differential geometry (which is the reason why it is also named after him). In particular, he proved (see [38] and [31]) that on a surface of negative curvature, having at least two different normal segments, there exists a set of geodesics that are recurrent without being periodic (which has the power of the continuum). Coding the geodesics by infinite words on the alphabet $\{a, b\}$ according to which boundary of the surface they meet, he arrived to the problem of constructing a non-periodic infinite word such that any sub word of it occurs infinitely often and with bounded gaps. By doing so, he introduced the same sequence as Thue and showed that it solves the problem.

Several other mathematicians rediscovered the Thue-Morse sequence after its first appearance. For a short summary and further references see [1, Notes on Chapter 1]. We only want to mention one other occurrence. In 1929, the Dutch chess grandmaster and world champion (1935-1937) Max (Machgielis) Euwe independently discovered the Thue-Morse sequence and applied it to a problem in chess [16]. The so-called German rule (which is slightly different to a current rule) states that a draw occurs if the same sequence of moves occurs three times in succession. Euwe proved, using the cube-free property of the sequence $(s_2(n) \bmod 2)_{n\in\mathbb{N}}$, that under such a rule infinite games of chess are possible.

Mahler is the first mathematician who used the sum of digits function in the context of harmonic analysis, which is deeply connected to the topics in this work (see [31, 32]). By a theorem of Fréchet, any monotone function f can be decomposed as $f = f_1 + f_2 + f_3$, where f_1 is a monotone step-function, f_2 a monotone function which is the integral of its derivative and f_3 a monotone continuous function which has almost everywhere a derivative zero. In [55] Wiener extended the spectrum theory to the harmonic analysis of functions defined for a denumerable set of arguments (that he called arrays). As an application of some theorems proved in [55], Mahler gives in [30] a construction based on the array $(-1)^{s(n)}$ for which $f_3 \neq 0$ in the Fréchet decomposition. The crucial point is the following property.

Theorem 1.1 *For any non-negative integer k the sequence*

$$\left(\frac{1}{N}\sum_{n<N}(-1)^{s_2(n)}(-1)^{s_2(n+k)}\right)_{N\geqslant 1}$$

converges and its limit is non-zero for infinitely many k.

This work has paved the way for the spectral analysis of substitutional dynamical systems. Let T denote the shift operator $T(u_n) = u_{n+1}$ on the space of all sequences $(u_n)_{n\in\mathbb{N}}$ with values in $\{-1, 1\}$ and endow the space $\{1-, 1\}^{\mathbb{N}}$ with the metric $d((u_n)_{n\in\mathbb{N}}, (v_n)_{n\in\mathbb{N}}) = 2^{-\inf\{n\in\mathbb{N}:u_n\neq v_n\}}$ if the two sequences are different and $d((u_n)_{n\in\mathbb{N}}, (v_n)_{n\in\mathbb{N}}) = 0$ otherwise. This induces a substitutional dynamical system which is called dynamical system of Thue-Morse (see for example [45]). In fact, the convergence of the considered sequence in Theorem 1.1 can be understood as a consequence of the unique ergodicity of this dynamical system.

In the middle of the twentieth century, first results about the summatory function of the sum of digits function were shown. In 1947, Bellman and Shapiro [2] proved the following relation (in base $q = 2$),

$$\sum_{0 \leqslant n < x} s_2(n) = \frac{x \log x}{2 \log 2} + O(x \log \log x).$$

S. C. Tang [50] extended this result to the general case where q is arbitrary and improved the error term

$$\sum_{0 \leqslant n < x} s_q(n) = \frac{q-1}{2 \log q} x \log x + O(x).$$

In 1975, Delange [11] showed the interesting result, that the summatory function of the sum of digits function can be written in the form,

$$\sum_{0 \leqslant n < x} s_q(n) = \frac{q-1}{2 \log q} x \log x + x F\left(\frac{\log x}{\log q}\right),$$

where $F : \mathbb{R} \to \mathbb{R}$ is periodic of period 1, continuous and nowhere differentiable.

Next, we want to address two related topics to the sum of digits function, namely, normal numbers and the uniform distribution modulo 1.

Normal Numbers

The notion of normal numbers was introduced by Émile Borel in his paper [4] (1909). See [29, Chapter 1.8] for a short introduction and exact definitions. Following the introduction in Harold Davenport's and Paul Erdős' paper "Note on normal decimals" [10], a real number α, expressed as a decimal (in base q), is said to be normal in base q if every combination of digits occurs in the decimal with the proper frequency. If $a_1 a_2 \ldots a_k$ is any combination of k digits, and $N(t)$ is the number of times this combination occurs among the first t digits, the condition is that

$$\lim_{t \to \infty} \frac{N(t)}{t} = \frac{1}{q^k}.$$

It was also Borel, who showed in [4] that almost all real numbers in the sense of Lebesgue measure are normal in base q. D.G. Champernowne [5] proved in 1933 that the number

$$0,12345678910111213141516 17\ldots$$

is normal in base 10 (which is now known as Champernowne's number). Copeland and Erdős [7] showed in 1952 that also the number

$$0,2357111317192329313741434 7\ldots,$$

which digits are formed by the concatenation of all primes is normal in base 10 (Copeland-Erdős constant). From these facts, one can derive results on the summatory function of the sum of digits function (see next section). However, it is not known whether classical arithmetical constants such as π, e or $\sqrt{2}$ are normal numbers.

Uniform Distribution modulo 1

Definition 1.1 *The sequence* $(x_n)_{n\in\mathbb{N}}$ *of real numbers is said to be uniformly distributed modulo 1, if for every pair* a, b *of real numbers with* $0 \leqslant a < b \leqslant 1$ *we have*

$$\lim_{N\to\infty} \frac{\#\{x_n : 1 \leqslant n \leqslant N, x_n \in [a,b)\}}{N} = b - a. \tag{1.1}$$

This common definition of the uniform distribution modulo 1 was given by Weyl in his famous paper "Über die Gleichverteilung von Zahlen mod. Eins." [54], where he also introduced a convenient criterion (now known as Weyl's criterion) to check whether a sequence is uniformly distributed modulo 1 or not. In fact, it suffices to consider the exponential sum $\sum_{n=1}^{N} \mathrm{e}(hx_n)$ for every integer $h \neq 0$ (for the exact statement and a proof see Theorem A.3). We will see in Chapter 2, that Weyl's paper also provides a practicable method to treat such sums. Nevertheless it wasn't Weyl's paper [54] which was the first work on this topic. Some special sequences have already been studied earlier, for example, Bohl, Sierpiński and Weyl proved with elementary methods independently in 1909-1910 that the sequence $(\alpha n)_{n\in\mathbb{N}}$ is uniformly distributed modulo 1 for irrational α. This result also follows immediately from Weyl's criterion. The distribution of this sequence has been studied copiously and a lot of subsequences have been considered. For instance, Vindogradov showed (see [53]) that the sequence of prime numbers (arranged in ascending order) multiplied by a irrational number is uniformly distributed modulo 1, too.

There exists an interesting connection between normal numbers and the uniform distribution modulo 1. A real number α is normal in base q, if and only if the sequence $(q^n\alpha)_{n\in\mathbb{N}}$ is uniformly distributed modulo 1 (see [29, Theorem 8.1]). For further information regarding this topic see [29].

1.2 The Distribution of the Sum of Digits Function in Residue Classes

The first work dealing with the distribution of the sum of digits function in residue classes goes back to Nathan Jacob Fine. He answered in [17] Stanislav Marcin Ulam's question whether the number of $n < x$ for which $s_{10}(n) \equiv n \equiv 0 \bmod 13$ is asymptotically $x/13^2$. Indeed, he could even show that

$$\lim_{x\to\infty} \frac{1}{x} \#\{n < x : n \equiv a \bmod p,\ s_q(n) \equiv c \bmod p\} = \frac{1}{p^2},$$

where a and c are arbitrary integers and p is a prime satisfying $p \nmid (q-1)$.

Nevertheless, it was the Russian mathematician Alexander Osipovich Gelfond (1906 – 1968), who could show a more general version of this assertion. In his paper *Sur les nombres qui ont des propriétés additives et multiplicatives données* [21], which was published by Acta Arithmetica in 1968, he proved the following theorem.

Theorem 1.2 (Gelfond, 1968 [21]) *Let* $q, m > 1$ *and* r, l, a *be integers and* $(m, q-1) = 1$*, then we have*

$$\#\{1 \leqslant n \leqslant N : n \equiv l \bmod r,\ s_q(n) \equiv a \bmod m\} = \frac{N}{mr} + O_q(N^{\lambda}), \tag{1.2}$$

where $\lambda = \frac{1}{2\log q} \log \frac{q\sin(\pi/2m)}{\sin(\pi/2mq)} < 1$ *is a positive constant depending only on* q *and* m*.*

Since his work is of particularly interest in the study of the distribution of the sum of digits function, we reproduce his proof in Section 1.3. Moreover, we show in that section some further results which can be obtained from Gelfond's theorem, and sharpen his result in the case $r = 1$ (we obtain a better constant λ and do not need the additional condition $(m, q-1) = 1$, see also [28]). We want to note at this point, that in the case that $m \mid q-1$ the statement is trivial. This follows from the following easy observation.

Lemma 1.1 *Let q be an integer $\geqslant 2$. Then we have for all $n \in \mathbb{N}$ and for all d with $d \mid q-1$*

$$s_q(n) \equiv n \mod d.$$

Proof. Writing n in its unique base-q expansion and using the fact that $q^k \equiv 1 \bmod q-1$, we have

$$s_q(n) = \sum_{k\geqslant 0} n_k \equiv \sum_{k\geqslant 0} n_k q^k \mod (q-1).$$

Since the last term is n and $d \mid q-1$, we are done. ∎

A crucial part in Gelfond's proof is the estimation of exponential sums. At least since Vinogradov's work on the method of trigonometrical sums in the theory of numbers (see [53]), exponential sums are intrinsically tied to analytic number theory. One plain reason for it is the following simple but crucial observation. Let us assume that we have positive integers m and n such that $m \mid n$. Then the sum $\sum_{h=0}^{m-1} \mathrm{e}\left(\frac{n}{m}h\right)$ is trivially equal to m. If, on the other hand, m does not divide n, then the sum is a geometric series and is equal to zero. For example, this allows us to count all numbers n between 1 and N, such that the sum of digits of n in base q is congruent a modulo m. Since this result is of particular importance in our work, we state it as a lemma.

Lemma 1.2 *For any positive integer m and n we have*

$$\frac{1}{m}\sum_{k=0}^{m-1} \mathrm{e}\left(\frac{n}{m}k\right) = \begin{cases} 1 & \text{if } m \mid n, \\ 0 & \text{otherwise}. \end{cases}$$

At the end of his paper, Gelfond stated three problems which seemed to be very interesting for him. Indeed, many mathematicians worked and still work on his problems.

Problem 1 - The joint distribution of the sum of digits function in residue classes.

First he conjectured that if q_1, q_2, m_1 and m_2 are positive integers $\geqslant 2$ satisfying $(q_1, q_2) = 1$, $(m_1, q_1 - 1) = 1$ and $(m_2, q_2 - 1) = 1$, then for any integers a_1, a_2 one has

$$\#\{1 \leqslant n \leqslant N : s_{q_1}(n) \equiv a_1 \bmod m_1 \text{ and } s_{q_2}(n) \equiv a_2 \bmod m_2\} = \frac{N}{m_1 m_2} + O(N^\lambda),$$

with $\lambda < 1$.

In 1972, Bésineau made a first, very important contribution to this problem by showing the following asymptotic result (see [3]).

Theorem 1.3 *Let $q_1, \ldots, q_l$ and $m_1, \ldots, m_l$ be positive integers $\geqslant 2$ satisfying the conditions $(q_i, q_j) = 1$ for $i \neq j$ and $(m_j, q_j - 1) = 1$ for $1 \leqslant j \leqslant l$. Then we have*

$$\#\{1 \leqslant n \leqslant N : s_{q_j}(n) \equiv a_j \bmod m_j \text{ for } 1 \leqslant j \leqslant l\} \sim \frac{N}{m_1 m_2 \cdots m_l} \quad (N \to \infty).$$

He obtained this result as a consequence of a general theorem on so-called pseudo-random arithmetic functions. But it took almost another 20 years until Dong-Hyun Kim solved Gelfond's conjecture. In particular, he showed a more general result, which uses the notion of completely q-additive functions. A function $f : \mathbb{N} \to \mathbb{C}$ is called *completely q-additive* if $f(0) = 0$ and $f(aq^k + b) = f(a) + f(b)$ for any integers $a \geqslant 1$, $k \geqslant 1$, and $0 \leqslant b < q^k$. Such functions were introduced independently by Bellman and

Shapiro [2] (1948) and Gelfond [21] (1968) and further studied by Delange, Bésineau, Coquet, Kátai and others.

In order to be able to state Kim's result, we have to define the notion of an admissible tuple of integers. Let $\mathbf{q} = (q_1, \dots, q_l)$ and $\mathbf{m} = (m_1, \dots, m_l)$ be tuples of integers satisfying $q_j, m_j \geqslant 2$ and $(q_i, q_j) = 1$ for $i \neq j$. For each j, let f_j be a completely q_j-additive function with integer values. Furthermore, we define $F_j = f_j(1)$ and $d_j = gcd\{m_j, (q_j - 1)F_j, f_j(r) - rF_j\,(2 \leqslant r \leqslant q_j - 1)\}$ and write $\mathbf{f} = (f_1, \dots, f_l)$. An l-tuple $\mathbf{a}$ of integers is called *admissible with respect to the l-tuples* $\mathbf{q}$,$\mathbf{m}$ *and* $\mathbf{f}$ if the system of congruences $F_j\, n \equiv a_j \bmod d_j$, $1 \leqslant j \leqslant l$ has a solution. We write $\mathcal{A} = \{\mathbf{a} : 0 \leqslant a_j \leqslant m_j - 1\ (1 \leqslant j \leqslant l),\ \mathbf{a} \text{ admissible}\}$.

Theorem 1.4 (Kim [28]) *Let* $\mathbf{q}, \mathbf{m}$ *and* $\mathbf{f}$ *be given as above. For any l-tuple* $\mathbf{a}$ *of integers and all positive integers N we have*

$$\#\{0 \leqslant n < N : f_j(n) \equiv a_j \bmod m_j,\ 1 \leqslant j \leqslant l\} = \begin{cases} N/|\mathcal{A}| + O_{\mathbf{q},l}(N^{1-\delta}) & \text{if } \mathbf{a} \text{ is admissible,} \\ 0 & \text{otherwise,} \end{cases}$$

where $\delta = 1/(120l^2\bar{q}^3\bar{m}^2)$ *with* $\bar{q} = \max\{q_j : 1 \leqslant j \leqslant l\}$ *and* $\bar{m} = \max\{m_j : 1 \leqslant j \leqslant l\}$.

One can easily see, that this really solves Gelfond's first problem and generalizes Bésineau's result. If we take for f_j the sum of digits function s_{q_j} (which is one of the most famous representatives of completely q_j-additive functions), and if we additionally demand $(m_j, q_j - 1) = 1$ for all j, then we have $\mathbf{d} = (1, \dots, 1)$ and hence every l-tuple $\mathbf{a}$ is admissible. Thus, we have $|\mathcal{A}| = m_1 m_2 \cdots m_l$, which proves Gelfond's conjecture ($l = 2$). In Chapter 4, we will prove Kim's result in the special case of sum of digits functions.

Problem 2 - The distribution of the sum of digits function of primes.

Gelfond remarked that it would be interesting to find the number of primes p less than or equal to N, such that $s_q(p) \equiv a \bmod m$.

Prime numbers fascinate mathematicians within living memory and the research into particulate sequences of prime numbers is a classical problem in the theory of numbers. One of the most famous theorems in number theory is the prime number theorem. Gauss (1792) and Legendre (1798) conjectured, that $\lim_{x\to\infty} \pi(x)(x/\log x)^{-1} = 1$. Over hundred years later, De La Vallèe-Poussin and Hadamard proved this separately in 1896. Now there are more accurate results known (see for example Theorem A.1). Dirichlet showed in 1837 (see for example [12]), that there are infinitely many primes p, such that $p \equiv a \bmod k$ whenever $(a, k) = 1$. This result was sharpened by Page, Siegel and Walfisz (see Theorem A.2). In the context of prime numbers there are a lot of famous unsolved problems. We want to state some important conjectures and refer to Paulo Ribenboim's book "The little book of bigger primes" [47], which also gives a good overview about recent records concerning prime numbers. Bernhard Riemann conjectured in 1859 that any non-trivial zero of the zeta-function has real part $1/2$ (Riemann hypothesis). It is deeply connected with prime numbers, and it is considered as one of the most famous problems in mathematics. In 1742, Goldbach enunciated in a letter to Euler, that every integer $n > 5$ is the sum of three primes (which is equivalent to the fact that every even integer $\geqslant 4$ is sum of two primes). Using a modified form of the Riemann hypothesis, Hardy and Littlewood showed in 1923 that every sufficient large odd integer is the sum of three primes. In 1937, Vinogradov gave a proof of this theorem without resorting to any hypothesis [53]. In spite of this achievements, Goldbach's conjecture is still unsolved. Another famous problem deals with primes p such that $p+2$ is also a prime. It is unknown whether there are infinitely many such primes (called twin-primes). Neither is it shown if there are infinitely many primes of the form $2^n + 1$ (Fermat numbers) and $2^n - 1$ (Mersenne numbers).

In the analysis of the sum of digits function in combination with prime numbers there are only few results known. As mentioned earlier, one can derive from Copeland's and Erdős' work on normal numbers that

$$\sum_{p\leqslant x} s_q(p) \sim \frac{1}{2}(q-1)\frac{x}{\log q} \quad (x\to\infty).$$

In 1967, Katai showed in [27] that

$$\sum_{p\leqslant x} s_q(p) = \frac{(q-1)x}{2\log q} + O\left(\frac{x}{(\log\log x)^{1/3}}\right),$$

but he assumed the validity of the density hypothesis for the Riemann zeta-function. Shiokawa [49] could show this relation without any unsolved hypothesis and with an improved error term. Heppner [25] improved and generalized Shiokawa's result further.

Gelfond's second problem was for a long time unsolved. If we suppose that the sum of digits of primes is "randomly distributed", we get the conjecture

$$\#\{p\leqslant x : s_q(p)\equiv a \bmod m\} \sim \frac{(m,q-1)}{m}\,\pi(x;d,a).$$

To obtain this result, note that every prime p with $s_q(p)\equiv a \bmod m$ also satisfies $p\equiv a \bmod d$ (this can be easily derived from Lemma1.1). The pictures below underline these conjectures, where we see the number of primes less than or equal $N = 17209$ ($\pi(N) = 1983$), such that $s_q(p)$ is in a special residue classes modulo m. On the left hand side we have $q = 26$ and $m = 7$. Although N is rather small, we can already see that there are approximately the same number of primes in each residue class. The second example considers the case $(m, q-1) \neq 1$ and also confirms the conjecture. We have $q = 26$, $m = 10$, and hence $(m, q-1) = 5$ (note, that $\pi(17209; 5, 0) = 1$).

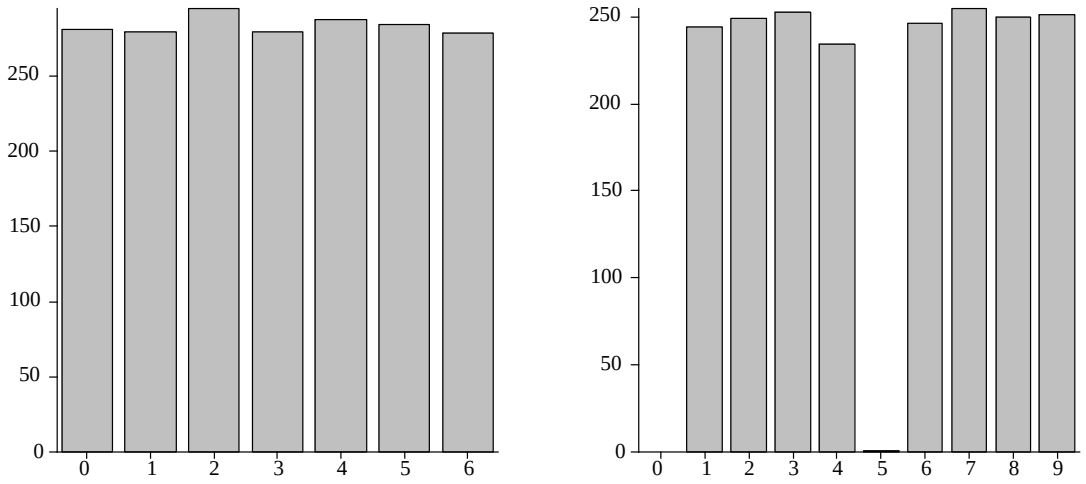

Table 1.1: $\#\{1\leqslant n\leqslant N : s_q(p)\equiv a \bmod m\}$

Montgomery mentioned this problem in [37, p. 208, number 67], where he stated some unsolved problems.

> Let $\omega(n)$ denote the number of 1's in the binary expansion of n; this is called the binary weight of n. Show that $\omega(p)$ is odd for asymptotically half of the primes.

Furthermore, he noted that Olivier [40, 41] had attacked this problem by using Vinogradov's method of prime number sums, but it seemed that the type II sums had been never estimated. Mauduit, one of the two authors who solved this problem recently, wrote in a paper in 2001 [31, p. 147], that it was not even known whether or not there are infinitely many prime numbers satisfying $s_q(p) \equiv a \bmod m$. But he and Fouvry studied in [18, 19] the same problem where prime numbers are replaced by numbers with at most two prime factors (denote the set of these numbers by $\mathbb{P}_2$). In particular, they could show the following theorem, using sophisticated linear sieve methods and the spectral theory of some special quasi-compact operators.

Theorem 1.5 *Let q, m be integers $\geqslant 2$ with $(m, q-1) = 1$. Then we have for all integers a and $x \to \infty$*

$$\#\{n \leqslant x : \ s_q(n) \equiv a \bmod m, \ n \in \mathbb{P}_2\} \gg_{q,m} \frac{x}{\log x}.$$

Replacing prime numbers by numbers with at most two prime factors yields also interesting results in classical problems. For instance, Chen showed in [6] that there are infinitely many primes p, such that $p+2$ is in $\mathbb{P}_2$.

In a recent work [33], Mauduit and Rivat solved Gelfond's second problem. In particular, they could show that

$$\#\{p \leqslant x : p \text{ prime and } s_q(p) \equiv a \bmod m\} = \frac{d}{m}\pi(x; d, a) + O_{q,m}(x^{1-\sigma_{q,m}}).$$

where $d = (q-1, m)$ and $\sigma_{q,m} > 0$ is effective. We will state and prove this result in Chapter 5.

Problem 3 - The distribution of the sum of digits function of squares.

Finally, Gelfond alluded the problem of giving an estimate of the number of values of a polynomial P (P takes only integer values on the set $\mathbb{N}$) satisfying the condition $s_q(P(n)) \equiv a \bmod m$.

In the field of integer sequences $(x_n)_{n\in\mathbb{N}}$ which have only few members (in the sense that $n \ll x_n$) are only few results known (for example, Mauduit's and Rivat's solution of Gelfond's second problem). Concentrating on polynomials, Davenport and Erdős [10] showed in 1952 the following result. Let $f(x)$ be a polynomial which takes only positive integer values on the set $\mathbb{N}$, then the decimal $0, f(1)f(2)f(3)\ldots$ is normal. Peter showed in [42] the related result

$$\sum_{0\leqslant n\leqslant N} s_q(n^k) = \frac{q-1}{2} N \frac{\log N^k}{\log q} + cN + NF_{q,k}\left(\frac{\log N^k}{\log q}\right) + O(N^{1-\varepsilon}),$$

where $c \in \mathbb{R}$, $\varepsilon > 0$ and $F_{q,k} : \mathbb{R} \to \mathbb{R}$ is periodic of period 1, continuous and nowhere differentiable.

In 1953 Piatetski-Shapiro studied in [43] the sequence $(\lfloor n^c \rfloor)_{n\in\mathbb{N}}$. In particular he showed that for every $c \in [1, 12/11)$ the number of positive integers less than N such that $\lfloor n^c \rfloor$ is a prime is asymptotically $N/(c \log N)$. By using van der Corput's method of exponential sums (see Chapter 2), Mauduit and Rivat [34, 35] proved the following theorem.

Theorem 1.6 *If $c \in [1, 7/5)$, q and m are integers greater than* 1*, then we have for all integers a*

$$\lim_{N\to\infty} \frac{1}{N} \#\{n < N : s_q(\lfloor n^c \rfloor) \equiv a \bmod m\} = \frac{1}{m}.$$

Furthermore, they could show that the sequence $(\alpha s_q(\lfloor n^c \rfloor))_{n\in\mathbb{N}}$ is uniformly distributed modulo 1 ($c \in [1, 7/5)$). For $c \in [1, 2)$, these sequences are intermediate cases between polynomials of degree 1 and 2 and the treatment of them can be considered as a first contribution to Gelfond's third problem. Mauduit, who solved with Rivat Gelfond's problem in the case $P(n) = n^2$, wrote in [31, p. 149], that the method used in the proof of Theorem 1.6 was good enough to obtain an interval for c independent of q and m, but that it seemed that new ideas were needed to cover at least the whole interval $[1, 2)$.

If follows from a result of Harman and Rivat [24] that we have for almost all $c \in [1, 2)$

$$\lim_{N\to\infty} \frac{1}{N} \#\{n < N : s_q(\lfloor n^c \rfloor) \equiv a \bmod m\} = \frac{1}{m},$$

but it is still a conjecture if this result holds for almost every $c > 1$ (see [31]). Nevertheless, Dartyge and Tennenbaum could show in [9] a first result in the case $c = 2$.

Theorem 1.7 *Let q and m be integers $\geqslant 2$ satisfying $(m, q-1) = 1$. Then there exists a constant $C = C(q, m)$ and an integer $N_0 = N_0(q, m) \geqslant 1$ such that for all integers a and $N \geqslant N_0$, we have*

$$\#\{n < N : s_q(n^2) \equiv a \bmod m\} \geqslant CN.$$

The two authors also generalized this result to sequences of the form $(f(n))_{n\in\mathbb{N}}$, where f is a polynomial with integer coefficients such that $f(\mathbb{N}) \subseteq \mathbb{N}$.

Recently, Mauduit and Rivat solved in [32] Gelfond's problem in the case $P(n) = n^2$ (using the above notion, in the case $c = 2$). In particular, they showed that

$$\#\{n \leqslant x : s_q(n^2) \equiv a \bmod m\} = \frac{x}{m} Q(a, d) + O_{q,m}\left(x^{1-\sigma_{q,m}}\right),$$

where $\sigma_{q,m} > 0$ is effective and $Q(a, d) = \#\{0 \leqslant n < d : n^2 \equiv a \bmod d\}$. For a proof of Mauduit's and Rivat's results, see Chapter 6.

1.3 Proofs and further Results

In this section we want to prove Theorem 1.2. In order to be able to do this, we have to treat estimates of exponential sums. The following theorem is the main part of the proof and of special interest (as we see later).

Theorem 1.8 *Let $m, q > 1$ be integers with $(m, q-1) = 1$ and $\gamma \in \mathbb{R}$. Then we have for $1 \leqslant h \leqslant m-1$*

$$\left|\sum_{n=1}^{N} \mathrm{e}\left(\gamma n + \frac{h}{m} s_q(n)\right)\right| = O_q(N^{\lambda}),$$

where $\lambda = \frac{1}{2\log q} \log \frac{q \sin(\pi/2m)}{\sin(\pi/2mq)} < 1$.

Proof. Let $f(n) = \mathrm{e}\left(\gamma n + \alpha s_q(n)\right)$ and $N = \sum_{k=0}^{\nu} n_k q^k$ ($n_\nu \neq 0$). Then we have

$$\sum_{n=1}^{N} f(n) = \sum_{i_0,\dots,i_{\nu-1}=0}^{q-1} \sum_{i_\nu=0}^{n_\nu-1} f(i_0 + i_1 q + \cdots + i_\nu q^\nu) + \sum_{i_0,\dots,i_{\nu-2}=0}^{q-1} \sum_{i_{\nu-1}=0}^{n_{\nu-1}-1} f(i_0 + \cdots + i_{\nu-1}q^{\nu-1} + n_\nu q^\nu)$$
$$+ \ldots + \sum_{i_0=0}^{n_0-1} f(i_0 + n_1 q + \cdots + n_\nu q^\nu) + f(N) - f(0).$$

One can readily show (s_q is q-additive) that we have $f(aq^i + bq^j) = f(aq^i)f(bq^j)$ for $0 \leqslant a, b \leqslant q-1$ and $i \neq j$. Thus, we can write

$$\sum_{n=0}^{N-1} f(n) = \prod_{k=0}^{\nu-1} [f(0) + f(q^k) + \cdots + f((q-1)q^k)][f(0) + f(q^\nu) \cdots + f((n_\nu - 1)q^\nu)]$$
$$+ \prod_{k=0}^{\nu-2} [f(0) + f(q^k) + \cdots + f((q-1)q^k)][f(0) + f(q^{\nu-1}) + \cdots + f((n_{\nu-1} - 1)q^{\nu-1})] f(n_\nu q^\nu)$$
$$+ \ldots + [f(0) + f(1) + \cdots + f(n_0 - 1)] f(n_1 q) \cdot \cdots \cdot f(n_\nu q^\nu)$$
$$+ f(n_0) \cdot \cdots \cdot f(n_\nu q^\nu) - 1.$$

Since $|f(n)| \leqslant 1$ we get the following estimation

$$\left|\sum_{n=1}^{N} f(n)\right| \leqslant q \sum_{i=1}^{\nu-1} \left|\prod_{k=0}^{i} [f(0) + f(q^k) + \cdots + f((q-1)q^k)]\right| + q + 2.$$

Calculating the geometric series (note, that $s_q(aq^k) = a$ for $0 \leqslant a \leqslant q-1$)

$$\left|\sum_{j=0}^{q-1} f(jq^k)\right| = \left|\sum_{j=0}^{q-1} \mathrm{e}(j(\gamma q^k + \alpha))\right| = \left|\frac{\sin \pi q(\gamma q^k + \alpha)}{\sin \pi(\gamma q^k + \alpha)}\right|,$$

we obtain the following estimate of our considered sum

$$\left|\sum_{n=1}^{N} f(n)\right| \leqslant q \sum_{i=1}^{\nu-1} \prod_{k=0}^{i} \left|\frac{\sin \pi q(\gamma q^k + \alpha)}{\sin \pi(\gamma q^k + \alpha)}\right| + q + 2 \quad \text{with} \quad \nu = \left\lfloor \frac{\log N}{\log q} \right\rfloor. \tag{1.3}$$

The function $\frac{\sin \pi q(\gamma q^k + \alpha)}{\sin \pi(\gamma q^k + \alpha)}$ is vitally important in this work. We study it in-depth in Chapter 3 and only refer here to the obtained results.

We set $\beta = \gamma q^k + h/m$ and $\beta_1 = \gamma q^{k+1} + h/m$, where $0 < h < m$. First we show that $\|q\beta - \beta_1\| \geqslant 1/m$. We can write $q\beta - \beta_1 = \frac{h}{m}(q-1)$. If $m(q-1) = hk$ ($k \in \mathbb{Z}$), the condition $(m, q-1) = 1$ implies that $h \geqslant m$. Thus we have proved the claim. Hence, we get $\|\beta\| \geqslant (2mq)^{-1}$ or $\|\beta_1\| \geqslant (2mq)^{-1}$. Indeed, if both numbers are smaller than $(2mq)^{-1}$, we get a contradiction to $\|q\beta - \beta_1\| \geqslant 1/m$. This allows us to apply Lemma 3.1 with $\delta = 1/(2mq)$ to one of the two following factors (note, that the factors are trivially bounded by q)

$$\left|\frac{\sin \pi q\beta}{\sin \pi\beta} \cdot \frac{\sin \pi q\beta_1}{\sin \pi\beta_1}\right| \leqslant q \frac{\sin(\pi/2m)}{\sin(\pi/2mq)} = q^{2\lambda},$$

where $\lambda = \frac{1}{2\log q}\log\frac{q\sin(\pi/2m)}{\sin(\pi/2mq)}$.

If we take these facts into consideration and use (1.3) with $\alpha = \frac{h}{m}$, we obtain

$$\left|\sum_{n=1}^{N} f(n)\right| \leqslant q\sum_{i=1}^{\nu-1}\prod_{k=0}^{i}\left|\frac{\sin\pi q(\gamma q^k + \frac{h}{m})}{\sin\pi(\gamma q^k + \frac{h}{m})}\right| + q + 2 \leqslant q\sum_{i=1}^{\nu-1} q^{\lambda i+1} + q + 2 \ll_q q^{\lambda\nu} \ll_q N^{\lambda}.$$

■

Proof (of Theorem 1.2). Let $S(N) = \#\{1 \leqslant n \leqslant N : n \equiv l \bmod r,\ s_q(n) \equiv a \bmod m\}$. By Lemma 1.2 we have

$$\begin{aligned} S(N) =& \frac{1}{rm}\sum_{t=0}^{r-1}\sum_{h=0}^{m-1}\sum_{n=1}^{N}\mathrm{e}\left(\frac{n-l}{r}t + \frac{s_q(n)-a}{m}h\right) = \frac{1}{rm}\sum_{t=0}^{r-1}\sum_{h=0}^{m-1}\mathrm{e}\left(-\frac{lt}{r} - \frac{ah}{m}\right)\sum_{n=1}^{N}\mathrm{e}\left(\frac{nt}{r} + \frac{h}{m}s_q(n)\right) \\ =& \frac{N}{rm} + \frac{1}{rm}\sum_{t=1}^{r-1}\sum_{n=1}^{N}\mathrm{e}\left(\frac{n-l}{r}t\right) + \frac{1}{rm}\sum_{t=0}^{r-1}\sum_{h=1}^{m-1}\mathrm{e}\left(-\frac{lt}{r} - \frac{ah}{m}\right)\sum_{n=1}^{N}\mathrm{e}\left(\frac{nt}{r} + \frac{h}{m}s_q(n)\right). \end{aligned} \tag{1.4}$$

Since $t/r \not\equiv 0 \bmod 1$, there exists an integer $N_1 < r$, such that

$$\left|\frac{1}{mr}\sum_{t=1}^{r-1}\sum_{n=1}^{N}\mathrm{e}\left(\frac{n-l}{r}t\right)\right| = \left|\frac{1}{mr}\sum_{t=1}^{r-1}\sum_{n=1}^{N_1}\mathrm{e}\left(\frac{n-l}{r}t\right)\right|.$$

This follows from the fact, that $\sum_{n=M}^{M+r-1}\mathrm{e}\left(\frac{n}{r}t\right) = 0$ for $M \geqslant 0$. Exchanging the summation order, we can apply Lemma 1.2 again

$$\begin{aligned} \left|\frac{1}{mr}\sum_{t=1}^{r-1}\sum_{n=1}^{N_1}\mathrm{e}\left(\frac{n-l}{r}t\right)\right| =& \frac{1}{m}\left|\sum_{n=1}^{N_1}\frac{1}{r}\sum_{t=0}^{r-1}\mathrm{e}\left(\frac{n-l}{r}t\right) - \frac{N_1}{r}\right| \\ \leqslant& \frac{1}{m}\#\{1 \leqslant n \leqslant N_1 : n \equiv l \bmod r\} + \frac{N_1}{mr} < \frac{1}{m} + \frac{1}{m} = \frac{2}{m}. \end{aligned}$$

To see the last inequality, note that $\#\{1 \leqslant n \leqslant N_1 : n \equiv l \bmod r\} \leqslant 1$ since $N_1 < r$. Finally, applying Theorem 1.8 to the last sum in (1.4) yields the desired estimation with λ as stated. ■

Remark. Gelfond showed additionally for the special case $q = m = 2$, that λ can be chosen as $\log 3/(2\log 2)$.

In the case that $r = 1$, i.e. we are interested in $\#\{0 \leqslant n < N : s_q(n) \equiv a \bmod m\}$, we can obtain a much better value for λ than Gelfond and do not need the additional condition $(m, q-1) = 1$. Therefore we prove a similar result as stated in Theorem 1.8.

Theorem 1.9 *Let $N > 0$, $q \geqslant 2$ and $m \geqslant 2$ be integers and $\alpha \in \mathbb{R} \setminus \mathbb{Z}$. Then we have*

$$\left|\sum_{n=1}^{N}\mathrm{e}(\alpha s_q(n))\right| = O_q(N^{\lambda}),$$

where $\lambda < 1$. If in addition $\|\alpha\| \geqslant 1/m$, then we have $\lambda = \frac{1}{\log q}\log\frac{\sin(\pi/m)}{\sin(\pi/mq)} < 1$.

Proof. Note, that by Lemma 3.1 $|(\sin \pi q\alpha)/(\sin \pi\alpha)| \leqslant q^{\lambda}$, where $\lambda < 1$. If we have $\|\alpha\| > (qm)^{-1}$, then we can apply Lemma 3.1 with $\delta = (qm)^{-1}$ and we get the same estimation with $\lambda = \frac{1}{\log q} \log \frac{\sin(\pi/m)}{\sin(\pi/mq)} < 1$. If we use the same notation as in the proof of Theorem 1.8, we obtain (1.3) (with $\gamma = 0$). Hence, we finally get

$$\left|\sum_{n=1}^{N} \mathrm{e}\left(\alpha s_q(n)\right)\right| \leqslant q \sum_{i=1}^{\nu-1} \left|\frac{\sin \pi q\alpha}{\sin \pi\alpha}\right|^{i+1} + q + 2 \leqslant q \sum_{i=1}^{\nu-1} q^{\lambda(i+1)} + q + 2 \ll_q q^{\nu\lambda} \ll_q N^{\lambda}.$$

■

Theorem 1.10 *Let $q, m > 1$ and a be integers. Then we have*

$$\#\{1 \leqslant n \leqslant N : s_q(n) \equiv a \bmod m\} = \frac{N}{m} + O_q(N^{\lambda}),$$

where $\lambda = \frac{1}{\log q} \log \frac{\sin(\pi/m)}{\sin(\pi/mq)} < 1$.

Proof. Let $S(N) = \#\{0 \leqslant n < N : s_q(n) \equiv a \bmod m\}$. By Lemma 1.2 we have

$$S(N) = \sum_{n=1}^{N} \frac{1}{m} \sum_{h=0}^{m-1} \mathrm{e}\left(\frac{h}{m}(s_q(n) - a)\right).$$

For $h = 0$ we get $\frac{N}{m}$. If we consider the remaining sum, we have

$$\begin{aligned}\left|\sum_{n=1}^{N} \frac{1}{m} \sum_{h=1}^{m-1} \mathrm{e}\left(\frac{h}{m}(s_q(n) - a)\right)\right| &= \frac{1}{m}\left|\sum_{h=1}^{m-1} \mathrm{e}\left(\frac{-ah}{m}\right) \sum_{n=1}^{N} \mathrm{e}\left(\frac{h}{m} s_q(n)\right)\right| \\ &\leqslant \frac{1}{m} \sum_{h=1}^{m-1} \left|\sum_{n=1}^{N} \mathrm{e}\left(\frac{h}{m} s_q(n)\right)\right| \ll N^{\lambda}.\end{aligned}$$

The last inequality is a consequence of Theorem 1.9 with $\lambda = \frac{1}{\log q} \log \frac{\sin(\pi/m)}{\sin(\pi/mq)}$, and the desired result is proved. ■

Remark. In the case $m = q = 2$, we obtain $\lambda = 1/2$, which is considerable better than Gelfond's result ($\log 3/(2 \log 2) \approx 0,792$). In other words, we have that the number of 1's (and 0's) in the first N members of the Thue-Morse sequence is $N/2 + O(\sqrt{N})$.

It was first shown by Michel Mendès-France [36] (published in 1968), that $(\alpha s_q(n))_{n\in\mathbb{N}}$ is uniformly distributed modulo 1 for irrational α. In 1980, Coquet [8] showed the interesting theorem, that if $(\lambda(n))_{n\in\mathbb{N}}$ is uniformly distributed modulo 1, then also the sequence $(\lambda(s_q(n)))_{n\in\mathbb{N}}$ is (which of course also proves Mendès-France's result). However, we can use Theorem 1.9 to show the same statement in an easy way. Furthermore, we show that a special subsequence of $(\alpha n)_{n\in\mathbb{N}}$ is uniformly distributed modulo 1 (stated as a remark in Gelfond's paper). We will see later, that $(\alpha s_q(p))_{p\in\mathbb{P}}$ (see chapter 5) and $(\alpha s_q(n^2))_{n\in\mathbb{N}}$ (chapter 6) also have the same property.

Theorem 1.11 *For $q \geqslant 2$ the sequence $(\alpha s_q(n))_{n\in\mathbb{N}}$ is uniformly distributed modulo* 1, *if and only if $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.*

Proof. If $\alpha \in \mathbb{Q}$, then the sequence $(\alpha s_q(n))_{n\in\mathbb{N}}$ takes modulo 1 only a finite number of values and is therefore not uniformly distributed modulo 1. Conversely, if $\alpha \in \mathbb{R}\setminus\mathbb{Q}$, then we have for every $h \in \mathbb{Z}\setminus\{0\}$ that $h\alpha \in \mathbb{R}\setminus\mathbb{Z}$. According to Theorem 1.9, there exists $\lambda < 1$, such that $\sum_{n\leqslant N} \mathrm{e}\left(h\alpha s_q(n)\right) = O(N^\lambda)$. Using Weyl's criterion, this proves that $(\alpha s_q(n))_{n\in\mathbb{N}}$ is uniformly distributed modulo 1 (see Theorem A.3). ■

Theorem 1.12 *Let q, m and a be integers satisfying $q, m \geqslant 2$ and $(q, m-1) = 1$. Furthermore, set $\mathbb{M} = \{n \in \mathbb{N} : s_q(n) \equiv a \bmod m\}$. Then the sequence $(\alpha n)_{n\in\mathbb{M}}$ is uniformly distributed modulo 1, if and only if $\alpha \in \mathbb{R}\setminus\mathbb{Q}$.*

Proof. As in the previous theorem, the sequence $(\alpha n)_{n\in\mathbb{M}}$ takes modulo 1 only a finite number of values if $\alpha \in \mathbb{Q}$ (and is therefore not uniformly distributed modulo 1). Suppose now, that $\alpha \in \mathbb{R}\setminus\mathbb{Q}$. According to Weyl's criterion (Theorem A.3), we have to show that

$$\sum_{\substack{1\leqslant n\leqslant N\\ s_q(n)\equiv a \bmod m}} \mathrm{e}(k\alpha n) = o(N)$$

for every integer $k \neq 0$. Note, that this is already sufficient, since by Theorem 1.2 $\#\{1 \leqslant n \leqslant N : s_q(n) \equiv a \mod m\} = N/m + O(N^\lambda)$, where $\lambda < 1$. Using Lemma 1.2, we can write

$$\begin{aligned}\sum_{\substack{1\leqslant n\leqslant N\\ s_q(n)\equiv a \bmod m}} \mathrm{e}(k\alpha n) &= \frac{1}{m}\sum_{n=1}^{N}\mathrm{e}(k\alpha n)\sum_{h=0}^{m-1}\mathrm{e}\left(\frac{h(s_q(n)-a)}{m}\right)\\ &= \frac{1}{m}\sum_{n=1}^{N}\mathrm{e}(k\alpha n) + \frac{1}{m}\sum_{h=1}^{m-1}\mathrm{e}\left(-\frac{ha}{m}\right)\sum_{n=1}^{N}\mathrm{e}\left(k\alpha n+\frac{h}{m}s_q(n)\right).\end{aligned}$$

The sum in the first term is bounded for all $k \neq 0$ if (and only if) $\alpha \in \mathbb{R}\setminus\mathbb{Q}$. The inner sum in the second term is $\ll N^\lambda$, with $\lambda < 1$ (see Theorem 1.8). Hence, we finally get the desired estimation and the theorem is proved. ■

At the end of this chapter, we want to state and prove another interesting theorem, which was treated in Gelfond's paper.

Theorem 1.13 ([21]) *Let $q, m, z > 1$ and a be integers, then we have*

$$\#\{1 \leqslant n \leqslant N : n \text{ is not divisible by a } z\text{-th power of a prime},\ s_q(n) \equiv a \bmod m\} = \frac{N}{m\zeta(z)} + O_q(N^{\lambda_1}), \tag{1.5}$$

where $\lambda_1 = \frac{1+(z-1)\lambda}{z}$, $\lambda = \lambda(m,q) < 1$ and $\zeta(.)$ denotes Riemann's zeta-function.

Proof. Set $T(N)$ as the considered expression in (1.5). Then we have $T(N) = \sum_{n=1}^{N}\varphi(n)\psi(n)$, where $\varphi(n) = 1$ if $s_q(n) \equiv a \bmod m$ and $\varphi(n) = 0$ otherwise and $\psi(n) = 1$ if n is not divisible by a z-th power of a prime and $\psi(n) = 0$ otherwise.

Using Lemma A.3, we can write $\psi(n) = \sum_{d^z|n}\mu(d)$, where $\mu(.)$ denotes the Möbius function. Therefore we have (set $N_1 = \lfloor N^{1/z}\rfloor$ and choose $N_2 < N_1$ later)

$$\begin{aligned}T(N) &= \sum_{n=1}^{N}\varphi(n)\sum_{d^z|n}\mu(d) = \sum_{d=1}^{N_1}\mu(d)\sum_{k\leqslant N/d^z}\varphi(d^z k)\\ &= \sum_{d=1}^{N_2}\mu(d)\sum_{k\leqslant N/d^z}\varphi(d^z k) + \sum_{d=N_2+1}^{N_1}\mu(d)\sum_{k\leqslant N/d^z}\varphi(d^z k).\end{aligned} \tag{1.6}$$

Using Theorem 1.2 (with $r = d^z$) and the connection between $\mu(.)$ and $\zeta(.)$ (see Lemma A.4), we can bound the first sum by

$$\begin{aligned}\sum_{d=1}^{N_2}\mu(d)\sum_{k\leqslant N/d^z}\varphi(d^z k) &= \sum_{d=1}^{N_2}\mu(d)\left[\frac{N}{md^z}+O_q(N^\lambda)\right]\\ &= \frac{N}{m}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^z}+O_q(N_2N^\lambda)-\frac{N}{m}\sum_{d=N_2+1}^{\infty}\frac{\mu(d)}{d^z}\\ &= \frac{N}{m\zeta(z)}+O_q(N_2N^\lambda)+O(NN_2^{1-z}).\end{aligned}$$

where $\lambda = \lambda(q,m) < 1$. Lemma A.6 yields the last O-Term in the above expression. Indeed, since the series and the integral are convergent, we get for $M \to \infty$

$$\left|\sum_{d=N_2+1}^{M}\frac{\mu(d)}{d^z}\right| \leqslant \sum_{d=N_2+1}^{M}\frac{1}{d^z} \leqslant \int_{N_2}^{M}\frac{1}{u^z}\,du = \frac{N_2^{1-z}-M^{1-z}}{z-1}.$$

By Lemma (A.6) again, we get for the second sum in (1.6)

$$\left|\sum_{d=N_2+1}^{N_1}\mu(d)\sum_{k\leqslant N/d^z}\varphi(d^z k)\right| \leqslant \sum_{n=N_2+1}^{N_1}\frac{N}{d^z} \leqslant N\int_{N_2}^{N_1}\frac{1}{u^z}\,du \leqslant N\frac{N_2^{1-z}}{z-1} = O(NN_2^{1-z}).$$

Setting $N_2 = \lfloor N^{/1-\lambda)/z}\rfloor$ ($< N_1$ if N is big enough), we obtain

$$T(N) = \frac{N}{m\zeta(z)}+O(N^{\lambda_1}),\quad \lambda_1 = \frac{1+(z-1)\lambda}{z},\ \lambda = \lambda(m,q) < 1.$$

■

Chapter 2

Exponential Sums

In this chapter we consider exponential sums of special linear and quadratic functions. First we treat sums with two variables, which are linear in one of them. Then we study so called Gauss sums, which play a major role in proving Gelfond's problem on the sum of digits function of squares. Finally, we outline a method that allows us to treat exponential sums in an efficient way (Van der Corput inequality).

2.1 A First Inequality

In this section, we want to find an upper bound of

$$\left|\sum_{0\leqslant n<m}\sum_{M'<l\leqslant M}\mathrm{e}\left(\frac{l(an+b)}{m}\right)\right|. \tag{2.1}$$

The function $\frac{l(an+b)}{m}$ is linear in l and since exponential sums of linear functions are geometric series, they are easy to handle. We get for the inner sum

$$\begin{aligned}\left|\sum_{M'<l\leqslant M}\mathrm{e}\left(\frac{l(an+b)}{m}\right)\right| &= \left|\sum_{0\leqslant l<M-M'}\mathrm{e}\left(\frac{l(an+b)}{m}\right)\right| \leqslant \min\left(M-M', \left|\frac{\mathrm{e}\left(\frac{(M-M')(an+b)}{m}\right)-1}{\mathrm{e}\left(\frac{an+b}{m}\right)-1}\right|\right)\\ &\leqslant \min\left(M, \frac{1}{\left|\sin\pi\frac{an+b}{m}\right|}\right).\end{aligned}$$

Hence, the following lemma provides an upper bound of (2.1) (see [33]).

Lemma 2.1 *Let $a, m \in \mathbb{Z}$ with $m \geqslant 1$ and $d = (a, m)$. Let $b \in \mathbb{R}$, then we have for every real number $M > 0$,*

$$\sum_{0\leqslant n<m}\min\left(M, \frac{1}{\left|\sin\pi\frac{an+b}{m}\right|}\right) \ll d\min\left(M, \frac{1}{\sin\pi\frac{d}{m}\left\|\frac{b}{d}\right\|}\right) + m\log m.$$

Proof. The inequality is trivial for $d = m$ because in this case $\left|\sin\pi\frac{an+b}{m}\right| = \sin\pi\left\|\frac{b}{d}\right\|$ for every n. When $d \neq m$, we have $1 \leqslant d \leqslant \frac{m}{2}$. Put $a' = \frac{a}{d}$, $m' = \frac{m}{d}$, and $b = b'd + r$ where $b' \in \mathbb{Z}$, $r \in \mathbb{R}$, $-\frac{d}{2} < r \leqslant \frac{d}{2}$, and

$$S = \sum_{0\leqslant n<m}\min\left(M, \frac{1}{\left|\sin\pi\frac{an+b}{m}\right|}\right) = \sum_{0\leqslant n<m}\min\left(M, \frac{1}{\left|\sin\frac{\pi}{m'}\left(a'n+b'+\frac{r}{d}\right)\right|}\right).$$

The numbers $a'n + b'$, where n takes m' consecutive values, cover all possible residual classes modulo m'. Indeed, this follows from the fact that $(a', m') = 1$. Hence we can write the sum S in the form

$$S = d \sum_{0 \leqslant n < m'} \min\left(M, \frac{1}{\left|\sin \frac{\pi}{m'}\left(n + \frac{r}{d}\right)\right|}\right).$$

If r is negative, we can also take $-n$ instead of n since it covers also all residual classes modulo m'. Therefore, we can from now on assume that $0 \leqslant r \leqslant d/2$ and subsequently suppress the absolute values. Isolating the first and the last term in this sum yields

$$S = d \min\left(M, \frac{1}{\sin \frac{\pi r}{m'd}}\right) + d \min\left(M, \frac{1}{\sin \frac{\pi}{m'}\left(1 - \frac{r}{d}\right)}\right) + d \sum_{1 \leqslant n < m'-1} \min\left(M, \frac{1}{\sin \frac{\pi}{m'}\left(n + \frac{r}{d}\right)}\right).$$

Since $t \mapsto \frac{1}{\sin t}$ is convex on $(0, \pi)$, we can apply Lemma A.7

$$S \leqslant d \min\left(M, \frac{1}{\sin \frac{\pi r}{m'd}}\right) + \frac{d}{\sin \frac{\pi}{m'}\left(1 - \frac{r}{d}\right)} + d \int_{\frac{1}{2}}^{m'-\frac{3}{2}} \frac{dt}{\sin \frac{\pi}{m'}\left(t + \frac{r}{d}\right)}.$$

Using again that $t \mapsto \frac{1}{\sin t}$ is convex on $(0, \pi)$ we observe in the first place that

$$h(x) = \frac{1}{\sin \frac{\pi}{m'}(1 - x)} + \int_{\frac{1}{2}}^{m'-\frac{3}{2}} \frac{dt}{\sin \frac{\pi}{m'}(t + x)}$$

is convex on $[0, 1/2]$ and therefore attains the maximum at the endpoints of the interval. Furthermore it shows that the maximum is equal to $h(1/2)$, since

$$\begin{aligned} h\left(\frac{1}{2}\right) - h(0) &= \frac{1}{\sin \frac{\pi}{2m'}} - \frac{1}{\sin \frac{\pi}{m'}} + \int_{m'-\frac{3}{2}}^{m'-1} \frac{dt}{\sin \frac{\pi t}{m'}} - \int_{\frac{1}{2}}^{1} \frac{dt}{\sin \frac{\pi t}{m'}} \\ &\geqslant \frac{1}{\sin \frac{\pi}{2m'}} - \frac{1}{\sin \frac{\pi}{m'}} + \frac{1}{2 \sin \frac{3\pi}{2m'}} - \frac{1}{2 \sin \frac{\pi}{2m'}} \\ &\geqslant \frac{1}{2 \sin \frac{\pi}{2m'}} - \frac{1}{\sin \frac{\pi}{m'}} + \frac{1}{2 \sin \frac{3\pi}{2m'}} \geqslant 0. \end{aligned}$$

Using that $\left(\log \tan \frac{t}{2}\right)' = \frac{1}{\sin t}$ in turn gives

$$\begin{aligned} S &\leqslant d \min\left(M, \frac{1}{\sin \frac{\pi r}{m'd}}\right) + \frac{d}{\sin \frac{\pi}{2m'}} + d \int_{1}^{m'-1} \frac{du}{\sin \frac{\pi u}{m'}} \\ &\leqslant d \min\left(M, \frac{1}{\sin \frac{\pi r}{m'd}}\right) + \frac{d}{\sin \frac{\pi}{2m'}} + \frac{2dm'}{\pi} \log \cot \frac{\pi}{2m'}. \end{aligned}$$

Replacing m' by m/d, using that $\cot u \leqslant 1/u$ on $(0, \pi/2)$ and noticing that $r/d = \|b/d\|$ ($0 \leqslant b/d - b' = r/d \leqslant 1/2$) we finally obtain

$$S \leqslant d \min\left(M, \frac{1}{\sin \pi \frac{d}{m} \left\|\frac{b}{d}\right\|}\right) + \frac{d}{\sin \frac{\pi d}{2m}} + \frac{2m}{\pi} \log \frac{2m}{\pi d} \ll d \min\left(M, \frac{1}{\sin \pi \frac{d}{m} \left\|\frac{b}{d}\right\|}\right) + m \log m.$$

■

2.2 Gauss Sums

In this section we want to prove an upper bound of Gauss sums. These sums are exponential sums and of the form

$$G(a,l;m)=\sum_{n=0}^{m-1}\mathrm{e}\left(\frac{an^2+ln}{m}\right),$$

where $a,l,m\in\mathbb{Z}$ with $m\geqslant 1$. Note, that it does not matter if we sum over n from 0 to $m-1$ or over any other representation system modulo m.

Theorem 2.1 *Let $a,l,m\in\mathbb{Z}$, satisfying $m\geqslant 1$ and $(a,m)=1$. Then we have*

$$|G(a,l;m)|\leqslant\sqrt{2m}.$$

We follow the proof of Graham and Kolesnik [22, Chapter 7.4]. First we state several lemmas.

Lemma 2.2 *If $(m_1,m_2)=1$, then we have*

$$G(a,l;m_1m_2)=G(am_1,l;m_2)\,G(am_2,l;m_1).$$

Proof. The crucial point is, that we have

$$\sum_{n=0}^{m_1m_2-1}\mathrm{e}\left(\frac{an^2+ln}{m_1m_2}\right)=\sum_{j=0}^{m_1-1}\sum_{k=0}^{m_2-1}\mathrm{e}\left(\frac{a(jm_2+km_1)^2+l(jm_2+km_1)}{m_1m_2}\right).$$

This follows from the fact that the integers jm_2+km_1, $j=0,\dots,m_1-1$, $k=0,\dots,m_2-1$ run through all equivalence classes modulo m_1m_2. But this already implies the desired result. ∎

Lemma 2.3 *Suppose that $(a,m)=1$. If m is odd or l is even, then we have*

$$|G(a,l;m)|=|G(a,0;m)|.$$

Proof. First we consider the case $m\equiv 1 \bmod 2$. Then we have $(4a,m)=1$ and $4a$ has an inverse element modulo m, say $\tilde{a}$. Replacing n by $n+2\tilde{a}l$ in the index of summation yields

$$G(a,l;m)=\sum_{n=0}^{m-1}\mathrm{e}\left(\frac{an^2+ln}{m}\right)=\sum_{n=0}^{m-1}\mathrm{e}\left(\frac{a(n-2\tilde{a}l)^2+l(n-2\tilde{a}l)}{m}\right)=\mathrm{e}\left(-\frac{\tilde{a}l^2}{m}\right)\sum_{n=0}^{m-1}\mathrm{e}\left(\frac{an^2}{m}\right).$$

In the second case we denote the inverse element of a modulo m by $\overline{a}$ and replace n by $n+\overline{a}l/2$ in the index of summation. The result follows using similar calculations as before. ∎

In order to be able to prove the next lemma, we need the notion of the Legendre symbol. Let p be an odd prime number and a an integer satisfying $p\nmid a$. Then the Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right)=\begin{cases}+1, & \text{if } a\equiv x^2 \bmod p \text{ for some integer } x,\\ -1, & \text{if there is no such } x.\end{cases}$$

For further information and properties of the Legendre symbol see for example [23, Chapter 6.5].

Lemma 2.4 *Suppose that p is an odd prime and $(a, p) = 1$. If $r \geqslant 1$, then we have*

$$|G(a, 0; p^r)| = \begin{cases} p^{r/2}, & \text{if } r \text{ is even} \\ p^{(r-1)/2}|G(1, 0; p)| & \text{otherwise.} \end{cases}$$

Proof. First we show that if $r \geqslant 2$, then $G(a, 0; p^r) = p\, G(a, 0; p^{r-2})$. Indeed, we can write

$$G(a, 0; p^r) = \sum_{j=0}^{p-1} \sum_{k=0}^{p^{r-1}-1} \mathrm{e}\left(\frac{a(jp^{r-1} + k)^2}{p^r}\right) = \sum_{k=0}^{p^{r-1}-1} \mathrm{e}\left(\frac{ak^2}{p^r}\right) \sum_{j=0}^{p-1} \mathrm{e}\left(\frac{2ajk}{p}\right).$$

Since the inner sum is p if $p \mid k$ and 0 otherwise, the claim follows. Furthermore this implies the desired result if r is even. Contrary, if r is odd, it suffices to show that

$$G(a, 0; p) = \left(\frac{a}{p}\right) G(1, 0; p).$$

If $0 \leqslant k < p$, the number of solutions of $an^2 \equiv k \bmod p$ is $1 + \left(\frac{ak}{p}\right)$. Hence, we have

$$G(a, 0; p) = \sum_{n=0}^{p-1} \mathrm{e}\left(\frac{an^2}{p}\right) = \sum_{k=0}^{p-1} \mathrm{e}\left(\frac{k}{p}\right)\left(1 + \left(\frac{ak}{p}\right)\right) = \left(\frac{a}{p}\right) \sum_{k=0}^{p-1} \mathrm{e}\left(\frac{k}{p}\right)\left(\frac{k}{p}\right).$$

Using $\sum_{k=0}^{p-1} \mathrm{e}\left(\frac{k}{p}\right) = 0$, we obtain

$$\sum_{k=0}^{p-1} \mathrm{e}\left(\frac{k}{p}\right)\left(\frac{k}{p}\right) = 1 + 2 \sum_{\substack{0<k<p \\ \left(\frac{k}{p}\right)=1}} \mathrm{e}\left(\frac{k}{p}\right) = \sum_{n=0}^{p-1} \mathrm{e}\left(\frac{n^2}{p}\right).$$

The last equality follows from the fact that n^2 assumes the value 0 once and the other considered values twice. ∎

Lemma 2.5 *We have for any positive m,*

$$|G(1, 0; m)| = \sqrt{m}.$$

Proof. By Poisson's summation formula (Lemma A.8), we have

$$\sum_{n=0}^{m-1} \mathrm{e}\left(\frac{n^2}{m}\right) = \sum_{k=-\infty}^{\infty} \int_0^m \mathrm{e}\left(\frac{x^2}{m} - kx\right) dx.$$

Changing the variables ($y = x/m$ and subsequently $z = (y - k/2)$), we obtain

$$\sum_{n=0}^{m-1} \mathrm{e}\left(\frac{n^2}{m}\right) = m \sum_{k=-\infty}^{\infty} \mathrm{e}\left(-\frac{mk^2}{4}\right) \int_0^1 \mathrm{e}(m(y - k/2)^2)\, dy = m \sum_{k=-\infty}^{\infty} \mathrm{e}\left(-\frac{mk^2}{4}\right) \int_{-k/2}^{1-k/2} \mathrm{e}(mz^2)\, dz.$$

Now we can split the last sum up into odd and even terms. Thus we get

$$\sum_{n=0}^{m-1} \mathrm{e}\left(\frac{n^2}{m}\right) = m(1 + i^{-m}) \int_{-\infty}^{\infty} \mathrm{e}(mz^2)\, dz = (i + i^{-m})(1 + i)\frac{\sqrt{m}}{2}.$$

Indeed, the last integral can be readily calculated using the residue theorem. Hence, the desired result is shown. ∎

Lemma 2.6 *Suppose that a is an odd integer. If l is odd, then we have $G(a,l;2)=2$ and $G(a,l;2^r)=0$ for $r\geqslant 2$. If l is even, we have $|G(a,l;2^r)|\leqslant \sqrt{2}\,2^{r/2}$.*

Proof. Suppose that l is odd. Then we have trivially $G(a,l;2)=2$. If $r\geqslant 2$, we can write

$$G(a,l;2^r)=\sum_{j=0}^{1}\sum_{k=0}^{2^{r-1}-1}\mathrm{e}\left(\frac{a(j2^{r-1}+k)^2+l(j2^{r-1}+k)}{2^r}\right)=\sum_{k=0}^{2^{r-1}-1}\mathrm{e}\left(\frac{ak^2+lk}{2^r}\right)\sum_{j=0}^{1}\mathrm{e}\left(\frac{lj}{2}\right),$$

which is equal to 0 since the inner sum vanishes. Contrary, if l is even, we can assume by Lemma 2.3 that $l=0$. We prove the statement by induction on r. If $r\leqslant 3$, one can readily check that the claim is true. Hence, let us assume that $r\geqslant 4$. We can write

$$\begin{aligned}G(a,0;2^r)&=\sum_{j=0}^{1}\sum_{k=0}^{2^{r-1}-1}\mathrm{e}\left(\frac{a(j2^{r-1}+k)^2}{2^r}\right)=2\sum_{k=0}^{2^{r-1}-1}\mathrm{e}\left(\frac{ak^2}{2^r}\right)\\&=2\sum_{n=0}^{2^{r-2}-1}\left(\mathrm{e}\left(\frac{a(2n)^2}{2^r}\right)+\mathrm{e}\left(\frac{a(2n+1)^2}{2^r}\right)\right)=2G(a,0;2^{r-2})+2\,\mathrm{e}\left(\frac{a}{2^r}\right)G(a,a;2^{r-2}).\end{aligned}$$

Since the last term is 0 (note, that a is odd and $r-2\geqslant 2$), we get the desired result using the induction hypothesis. ∎

Proof (of Theorem 2.1). By Lemma 2.2 we only have to consider the case $m=p^r$, where p is a prime number and $r\geqslant 1$ an integer. If p is an odd prime, then we have

$$|G(a,l;p^r)|=2^{r/2}$$

by Lemma 2.3, Lemma 2.4 and Lemma 2.5. If p=2, Lemma 2.6 already gives the required answer

$$|G(a,l;2^r)|\leqslant \sqrt{2}\,2^{r/2}.$$

∎

Corollary 2.1 *Let $a,l,m\in\mathbb{Z}$ with $m\geqslant 1$ and set $d=(a,m)$. Then we have*

$$|G(a,l;m)|\leqslant \sqrt{2dm},$$

and

$$|G(a,l;m)|=0\quad \text{if } d\nmid l.$$

Proof. Setting $m'=m/d,\ a'=a/d$, we can use the Euclidean algorithm ($n=km'+r$) to get

$$\begin{aligned}G(a,l;m)&=\sum_{0\leqslant r<m'}\sum_{0\leqslant k<d}\mathrm{e}\left(\frac{da'(km'+r)^2+l(km'+r)}{dm'}\right)\\&=\sum_{0\leqslant r<m'}\mathrm{e}\left(\frac{a'r^2+\frac{l}{d}r}{m'}\right)\sum_{0\leqslant k<d}\mathrm{e}\left(\frac{lk}{d}\right).\end{aligned}$$

If $d\nmid l$, the inner sum is 0, and the desired inequality is trivially satisfied. In the other case (set $l'=l/d$) we have $G(a,l;m)=d\,G(a',l';m')$ with $(a',m')=1$. Hence we can use Theorem 2.1 to obtain

$$|G(a,l;m)|=d\,|G(a',l';m')|\leqslant d\sqrt{2m'}=\sqrt{2dm}.$$

∎

2.3 Van der Corput's Inequality

Weyl introduced in [54] a useful transformation that arises upon squaring an exponential sum. If f is a real-valued function, than we have

$$\left|\sum_{1\leqslant n\leqslant N} \mathrm{e}(f(n))\right|^2 = \sum_{1\leqslant m,n\leqslant N} \mathrm{e}(f(n)-f(m)) = \sum_{|h|<N} \sum_{\substack{1\leqslant n\leqslant N\\ 1\leqslant n+h\leqslant N}} \mathrm{e}(f(n+h)-f(n)).$$

Van der Corput (1922) modified and improved Weyl's method. He used the simple idea, that for an arbitrary positive integer R one has $R\sum_{1\leqslant n\leqslant N}\mathrm{e}(f(n)) = \sum_{r=0}^{R-1}\sum_{-r<n\leqslant N-r}\mathrm{e}(f(n+r))$. Then he employed the Cauchy-Schwarz inequality and Weyl's concept. For further information on van der Corput's method of exponential sums see [22]. The next lemma is a generalization of van der Corput's result, where the special case $k=1$ is named after him.

Lemma 2.7 ([32]) *Let $z_1,\dots,z_N$ be complex numbers. For any integers $k\geqslant 1$ and $R\geqslant 1$ we have*

$$\left|\sum_{1\leqslant n\leqslant N} z_n\right|^2 \leqslant \frac{N+k(R-1)}{R}\sum_{|r|<R}\left(1-\frac{|r|}{R}\right)\sum_{\substack{1\leqslant n\leqslant N\\ 1\leqslant n+kr\leqslant N}} z_{n+kr}\overline{z_n}.$$

Proof. We take for convenience $z_n=0$ for n $\leqslant 0$ and for $n\geqslant N+1$. Then we can write

$$R\sum_{n\in\mathbb{Z}} z_n = \sum_{r=0}^{R-1}\sum_{n\in\mathbb{Z}} z_{n+kr} = \sum_{n\in\mathbb{Z}}\sum_{r=0}^{R-1} z_{n+kr}.$$

If the last sum is not zero, then n satisfies $1-k(R-1)\leqslant n\leqslant N$ and there are at most $N+k(R-1)$ such values for n. Hence, applying Cauchy-Schwarz and changing the summation index yields to

$$\begin{aligned}
R^2\left|\sum_{n\in\mathbb{Z}} z_n\right|^2 &\leqslant (N+k(R-1))\sum_{n\in\mathbb{Z}}\left|\sum_{r=0}^{R-1} z_{n+kr}\right|^2\\
&\leqslant (N+k(R-1))\sum_{r_1=0}^{R-1}\sum_{r_2=0}^{R-1}\sum_{n\in\mathbb{Z}} z_{n+kr_1}\overline{z_{n+kr_2}}\\
&\leqslant (N+k(R-1))\sum_{r_1=0}^{R-1}\sum_{r_2=0}^{R-1}\sum_{m\in\mathbb{Z}} z_{m+k(r_1-r_2)}\overline{z_m}\\
&\leqslant (N+k(R-1))\sum_{|r|<R}(R-|r|)\sum_{m\in\mathbb{Z}} z_{m+kr}\overline{z_m}.
\end{aligned}$$

■

The next lemma is a variant of van der Corput's inequality and is based on [39] (see [32]). We consider sums of the form $\sum_{A\leqslant n\leqslant B} z_n$, where $1\leqslant A\leqslant B\leqslant N$ are integers. It has the big advantage, that we can find an upper bound where the summation domain does not depend on A and B any more.

Lemma 2.8 ([32]) *Let $1\leqslant A\leqslant B\leqslant N$ be integers and $z_1,\dots,z_N$ complex numbers with absolute value $\leqslant 1$. Then we have for any $R\geqslant 1$*

$$\left|\sum_{A\leqslant n\leqslant B} z_n\right| \leqslant \left(\frac{B-A+1}{R}\sum_{|r|<R}\left(1-\frac{|r|}{R}\right)\sum_{\substack{1\leqslant n\leqslant N\\ 1\leqslant n+r\leqslant N}} z_{n+kr}\overline{z_n}\right)^{1/2} + \frac{R}{2}.$$

Proof. As in the proof of the last lemma, we take for convenience $z_n = 0$ for n $\leqslant 0$ and for $n \geqslant N + 1$. Since the absolute values of the considered complex numbers are $\leqslant 1$, we obtain

$$\left| R \sum_{n=A}^{B} z_n - \sum_{-\frac{R}{2}<r\leqslant\frac{R}{2}} \sum_{n=A}^{B} z_{n+r} \right| \leqslant \sum_{-\frac{R}{2}<r\leqslant\frac{R}{2}} 2|r| \leqslant \frac{R^2}{2},$$

and hence

$$\left| \sum_{1\leqslant n\leqslant N} z_n \right| \leqslant \frac{1}{R} \sum_{n=A}^{B} \left| \sum_{-\frac{R}{2}<r\leqslant\frac{R}{2}} z_{n+r} \right| + \frac{R}{2}.$$

Using the Cauchy-Schwarz inequality, we finally get

$$\begin{aligned}
\left(\sum_{n=A}^{B} \left| \sum_{-\frac{R}{2}<r\leqslant\frac{R}{2}} z_{n+r} \right| \right)^2 &\leqslant (B-A+1) \sum_{n=A}^{B} \left| \sum_{-\frac{R}{2}<r\leqslant\frac{R}{2}} z_{n+r} \right|^2 \leqslant (B-A+1) \sum_{n\in\mathbb{Z}} \left| \sum_{-\frac{R}{2}<r\leqslant\frac{R}{2}} z_{n+r} \right|^2 \\
&= (B-A+1) \sum_{-\frac{R}{2}<r_1\leqslant\frac{R}{2}} \sum_{-\frac{R}{2}<r_2\leqslant\frac{R}{2}} \sum_{n\in\mathbb{Z}} z_{n+r_1} \overline{z_{n+r_2}} \\
&= (B-A+1) \sum_{-\frac{R}{2}<r_1\leqslant\frac{R}{2}} \sum_{-\frac{R}{2}<r_2\leqslant\frac{R}{2}} \sum_{m\in\mathbb{Z}} z_{m+r_1-r_2} \overline{z_m} \\
&= (B-A+1) \sum_{-R<r<R} (R-|r|) \sum_{m\in\mathbb{Z}} z_{m+r} \overline{z_m}.
\end{aligned}$$

■

Chapter 3

Trigonometric Products

In this chapter, we want to state and prove some average estimates of trigonometric products which are essential for solving Gelfond's problems. They are a crucial part of the later proofs and of independent interest.

Before we begin to study these products we define and consider the following function, which we have already seen in Chapter 1.

Definition 3.1 *For $q \geqslant 2$ we define φ_q by*

$$\varphi_q(t) = \begin{cases} \frac{|\sin \pi q t|}{|\sin \pi t|} & \text{if } t \in \mathbb{R} \setminus \mathbb{Z} \\ q & \text{if } t \in \mathbb{Z}. \end{cases} \tag{3.1}$$

Lemma 3.1 *Let $q \geqslant 2$ be an integer and $\delta \in [0, \frac{2}{3q}]$. Then, $\varphi_q(t)$ is periodic of period 1, continuous and continuously differentiable on $\mathbb{R}$ and we have*

$$\max_{\|t\| \geqslant \delta} \varphi_q(t) \leqslant \varphi_q(\delta) \leqslant q.$$

Furthermore, $\varphi_q(\delta) < q$ if $\delta \neq 0$.

Proof. Since $\varphi_q(t) = \left|\sum_{0 \leqslant v < q} e(vt)\right|$ (geometric series), we obtain that φ_q is periodic of period 1, continuous and continuously differentiable on $\mathbb{R}$. We have for $t > 0$

$$\left(\frac{\sin \pi q t}{\sin \pi t}\right)' = \frac{\pi q \sin(\pi t)\cos(\pi q t) - \pi \cos(\pi t)\sin(\pi q t)}{\sin^2(\pi t)}.$$

The derivative is trivially negative if $t \in [1/(2q), 1/q)$. If $t \in (0, 1/(2q))$, the derivative is negative if and only if $\tan \pi t < (1/q)\tan \pi q t$. But this is true, since tan is convex on $[0, \pi/2]$. Hence, we obtain that $\varphi_q(t)$ is strictly monotone decreasing on the interval $[0, 1/q]$ and we have that $\varphi_q(\delta) < q$ if $\delta \neq 0$ ($\varphi_q(0) = q$). Moreover, it suffices to show that

$$\max_{\|t\| \geqslant \frac{1}{q}} \varphi_q(t) \leqslant \varphi_q\left(\frac{2}{3q}\right).$$

Since $t \mapsto \frac{\sin t}{\sin \frac{2}{3}t}$ is decreasing on $[0, \frac{\pi}{2}]$ (for the same reason as before) and $\|t\| \geqslant \frac{1}{q}$, we obtain

$$\varphi_q(t) \leqslant \frac{1}{\sin \pi t} \leqslant \frac{1}{\sin \frac{\pi}{q}} = \frac{\sin \frac{2\pi}{3}}{\sin \frac{\pi}{q}} \frac{\sin \frac{\pi}{2}}{\sin \frac{2}{3}\frac{\pi}{2}} \leqslant \frac{\sin \frac{2\pi}{3}}{\sin \frac{\pi}{q}} \frac{\sin \frac{\pi}{q}}{\sin \frac{2\pi}{3q}} = \varphi_q\left(\frac{2}{3q}\right).$$

■

Remark. From the fact that $\varphi_q(x) = |U_{q-1}(\cos(\pi x))|$, the Chebyshev polynomial of the second kind, one can also show that $\varphi_q(.)$ is strictly monotone decreasing on the interval $[0, 1/q]$.

3.1 Fourier Transform of e$(f_\lambda(.))$

In this chapter, as in the rest of this work, we set $f(n) = \alpha s_q(n)$ and define the truncated function

$$f_\lambda(n) = \sum_{k<\lambda} f(n_k q^k) = \alpha \sum_{k<n} n_k,$$

where λ is an integer greater than zero and the integers n_k denote the digits of n in basis q. As we will see later, this last function f_λ is of particular interest, since it is periodic of period q^λ. In this section, we turn our main attention to the discrete Fourier transform of e$(f_\lambda(n))$.

Definition 3.2 *Let $q \geqslant 2$, $\alpha \in \mathbb{R}$ and $\lambda \in \mathbb{N}$. The discrete Fourier transform $F_\lambda(.,\alpha)$ of the function $u \mapsto e(f_\lambda(u))$ is defined for all $h \in \mathbb{Z}$ by*

$$F_\lambda(h,\alpha) = \frac{1}{q^\lambda} \sum_{0\leqslant u<q^\lambda} \mathrm{e}\left(f_\lambda(u) - huq^{-\lambda}\right).$$

Since $f(u) = f_\lambda(u)$ for $0 \leqslant u < q^\lambda$, the discrete Fourier transform of e$(f(.))$ is the same as of e$(f_\lambda(.))$. A crucial point of our further studies is the fact, that we can represent $F_\lambda(h,\alpha)$ as a trigonometric product. Indeed, we get a recursive definition of the Fourier transform using the circumstance that $s_q(n)$ is completely q-additive. In particular, we have for $v = qu + i$, where $0 \leqslant i < q$, $s_q(v) = s_q(u) + i$. Therefore we get for $\lambda \geqslant 0$ (assume that $\alpha - hq^{-(\lambda+1)} \in \mathbb{R} \setminus \mathbb{Z}$)

$$\begin{aligned}
|F_{\lambda+1}(h,\alpha)| &= \frac{1}{q^{\lambda+1}} \left| \sum_{0\leqslant i<q} \sum_{0\leqslant u<q^\lambda} \mathrm{e}\left(\alpha(s_q(u)+i) - h(qu+i)q^{-(\lambda+1)}\right)\right| \\
&= \frac{1}{q} \left| \sum_{0\leqslant i<q} \mathrm{e}\left(i\left(\alpha - hq^{-(\lambda+1)}\right)\right)\right| |F_\lambda(h,\alpha)| \\
&= \frac{1}{q} \left| \frac{\sin \pi q\left(\alpha - hq^{-(\lambda+1)}\right)}{\sin \pi\left(\alpha - hq^{-(\lambda+1)}\right)}\right| |F_\lambda(h,\alpha)|.
\end{aligned}$$

Hence, we can write the following equation for all $\alpha \in \mathbb{R}$ and $h \in \mathbb{Z}$

$$|F_{\lambda+1}(h,\alpha)| = \frac{1}{q}\, \varphi_q\left(\alpha - \frac{h}{q^{\lambda+1}}\right) |F_\lambda(h,\alpha)|. \tag{3.2}$$

If we iterate this procedure, we obtain (note, that $F_0(h,\alpha) = 1$)

$$|F_\lambda(h,\alpha)| = q^{-\lambda} \prod_{1\leqslant j\leqslant\lambda} \varphi_q\left(\alpha - hq^{-j}\right). \tag{3.3}$$

We can easily derive the following lemma from these facts.

Lemma 3.2 *Let $0 \leqslant \theta \leqslant \lambda$. Then we have*

$$|F_\lambda(q^\theta b,\alpha)| \leqslant |F_{\lambda-\theta}(b,\alpha)|.$$

Proof. If $\theta = \lambda$, then this inequality is trivial by Lemma 3.1. If $0 \leqslant \theta < \lambda$, we use (3.3) to get

$$|F_\lambda(q^\theta b,\alpha)| = q^{-\lambda} \prod_{1\leqslant j\leqslant\theta} \varphi_q\left(\alpha - bq^{\theta-j}\right) \prod_{\theta<j\leqslant\lambda} \varphi_q\left(\alpha - bq^{\theta-j}\right).$$

Since $\varphi_q(t)$ is periodic of period 1, we obtain

$$\begin{aligned}|F_\lambda(q^\theta b,\alpha)| &= q^{-\theta}\varphi_q(\alpha)^\theta\, q^{-(\lambda-\theta)} \prod_{1\leqslant j\leqslant \lambda-\theta} \varphi_q\left(\alpha - bq^{-j}\right)\\ &= q^{-\theta}\varphi_q(\alpha)^\theta\, |F_{\lambda-\theta}(b,\alpha)|.\end{aligned}$$

Again by Lemma 3.1 ($\varphi_q(t) \leqslant q$ for all $t \in \mathbb{R}$), we finally obtain the desired result. ■

In order to get an upper bound of $F_\lambda(h,\alpha)$ uniformly for all $h \in \mathbb{Z}$, we have to prove several properties of $\varphi_q(t)$. The following lemmas are from Mauduit's and Rivat's work on the sum of digits function of squares [32]. We will see in Chapter 5 that these results, or being more accurate, Lemma 3.6 and Lemma 3.14 (which can be derived from the first one) are very useful for proving not only Gelfond's problem on the sum of digits function of squares but also his problem on the sum of digits function of prime numbers.

Lemma 3.3 *Let $q \geqslant 2$ be an integer and $t \in \mathbb{R}$. Then we have*

$$\varphi_q(t) \leqslant q\exp\left(-\frac{(q^2-1)\pi^2\|t\|^2}{6}\right) \quad \textit{for} \quad \|t\| \leqslant \sqrt{\frac{6}{\pi^2(q^2-1)}}.$$

Proof. Since φ_q is periodic of period 1 and symmetric with respect to 0, we only have to consider t in the range

$$0 \leqslant t \leqslant \sqrt{\frac{6}{\pi^2(q^2-1)}}.$$

Easy calculations and the Leibniz criterion give us the following estimations for $u \in \mathbb{R}$,

$$\begin{aligned}&0 \leqslant \sin u \leqslant u - \frac{u^3}{6} + \frac{u^5}{120} \quad \text{for} \quad 0 \leqslant u \leqslant \pi,\\ &0 \leqslant u - \frac{u^3}{6} \leqslant \sin u \quad \text{for} \quad 0 \leqslant u \leqslant \sqrt{6},\\ &0 \leqslant 1 - u + \frac{u^2}{3} \leqslant 1 - u + \frac{u^2}{2} - \frac{u^3}{6} \leqslant e^{-u} \quad \text{for} \quad 0 \leqslant u \leqslant 1.\end{aligned}$$

We have to show that $\sin(\pi qt) \leqslant q\sin(\pi t)\exp(-(q^2-1)(\pi t)^2)/6)$. Due to the fact that we have $0 \leqslant \pi qt \leqslant \pi$ and $0 \leqslant \pi t \leqslant \sqrt{6}$, we can use these estimations for $\sin(\pi qt)$ and $\sin(\pi t)$ and therefore it suffices to prove

$$\pi qt - \frac{(\pi qt)^3}{6} + \frac{(\pi qt)^5}{120} \leqslant q\left(\pi t - \frac{(\pi t)^3}{6}\right)\left(1 - \frac{q^2-1}{6}(\pi t)^2 + \frac{(q^2-1)^2}{3\cdot 6^2}(\pi t)^4\right).$$

Expanding the right hand side, we see that the above inequality is true if and only if

$$\frac{(q\pi t)^5}{3\cdot 6^2} - \frac{(q\pi t)^5}{4\cdot 5\cdot 6} + \frac{q^3(\pi t)^5}{3\cdot 6^2} - \frac{2q(\pi t)^5}{3\cdot 6^2} - \frac{q(q^2-1)^2(\pi t)^7}{3\cdot 6^3} \geqslant 0.$$

Multiplying this inequality with $(3\cdot 6^3\cdot 5)/(q(\pi t)^5)$ for $t \neq 0$ ($t = 0$ is trivial), we obtain

$$3q^4 + 30q^2 - 60 \geqslant 5(q^2-1)^2(\pi t)^2.$$

But this inequality is true if $0 \leqslant t \leqslant \sqrt{\frac{6}{\pi^2(q^2-1)}}$, since $3q^4 + 30q^2 - 60 \geqslant 30(q^2-1)$ for $q \geqslant 2$. ■

Lemma 3.4 *We have for $q \geqslant 2$ and $t \in \mathbb{R}$*

$$\varphi_q\left(\frac{t}{q}\right) \leqslant \varphi_q\left(\frac{\|t\|}{q}\right).$$

Proof. Set $t = \theta + l$, where $-\frac{1}{2} < \theta \leqslant \frac{1}{2}$ and $l \in \mathbb{Z}$. If $l \equiv 0 \bmod q$, we already have the desired equality because of the periodicity of φ_q. If $l \not\equiv 0 \bmod q$, we have

$$\frac{1}{2} \geqslant \left\|\frac{t}{q}\right\| = \left\|\frac{\theta + l}{q}\right\| \geqslant \left\|\frac{l}{q}\right\| - \left\|\frac{\theta}{q}\right\| \geqslant \frac{1}{q} - \frac{1}{2q} = \frac{1}{2q} \geqslant \left|\frac{\theta}{q}\right| = \frac{\|t\|}{q}.$$

Since $\sin u$ is increasing on $[0, \pi/2]$, we obtain

$$\varphi_q\left(\frac{t}{q}\right) = \varphi_q\left(\left\|\frac{t}{q}\right\|\right) = \frac{|\sin \pi\theta|}{\sin \pi\left\|\frac{\theta+l}{q}\right\|} \leqslant \frac{|\sin \pi\theta|}{\sin \pi\frac{\|t\|}{q}} = \varphi_q\left(\frac{\|t\|}{q}\right).$$

■

Lemma 3.5 *We have for $q \geqslant 2$ and $\alpha \in \mathbb{R}$*

$$\max_{t\in\mathbb{R}} \varphi_q(\alpha - t)\,\varphi_q(\alpha - qt) \leqslant q\,\varphi_q\left(\frac{\|(q-1)\alpha\|}{q+1}\right).$$

Proof. Setting $\delta = \frac{\|(q-1)\alpha\|}{q+1} \leqslant \frac{1}{2q}$ and $u = \alpha - t$, we have to prove

$$\max_{t\in\mathbb{R}} \varphi_q(\alpha - t)\,\varphi_q(\alpha - qt) = \max_{u\in\mathbb{R}} \varphi_q(u)\,\varphi_q(qu - (q-1)\alpha) \leqslant q\,\varphi_q(\delta).$$

Since $\varphi_q(t)$ is always bounded by q, it suffices to show that one of the factors is bounded by $\varphi_q(\delta)$. If $\|qu - (q-1)\alpha\| \geqslant \delta$, we get the desired estimation for the second factor by Lemma 3.1. In the other case we have

$$\begin{aligned}\|qu\| = \|qu - (q-1)\alpha + (q-1)\alpha\| &\geqslant \|(q-1)\alpha\| - \|qu - (q-1)\alpha\| \\ &\geqslant (q+1)\delta - \delta = q\delta.\end{aligned}$$

Hence, we can bound the first factor using Lemma 3.4 and the monotony of $\varphi_q(t)$ on the interval $[0, 1/q]$

$$\varphi_q(u) = \varphi_q\left(\frac{qu}{q}\right) \leqslant \varphi_q\left(\frac{\|qu\|}{q}\right) \leqslant \varphi_q\left(\frac{q\delta}{q}\right) = \varphi_q(\delta).$$

■

Lemma 3.6 *Let $q \geqslant 2$, $\alpha \in \mathbb{R}$, $h \in \mathbb{Z}$, $\lambda \geqslant 1$ and $c_q = \frac{\pi^2}{12\log q}\left(1 - \frac{2}{q+1}\right)$. Then we have*

$$|F_\lambda(h, \alpha)| \leqslant e^{\pi^2/48} q^{-c_q\|(q-1)\alpha\|^2\lambda}. \tag{3.4}$$

Proof. To prove this lemma, we first note that

$$\max_{t\in\mathbb{R}} \varphi_q(\alpha - t)\varphi_q(\alpha - qt) \leqslant q^2 \exp\left(-\frac{\pi^2(q-1)}{6(q+1)}\|(q-1)\alpha\|^2\right).$$

This is a direct consequence of Lemma 3.5 in combination with Lemma 3.3 since all assumptions are satisfied. Indeed, we have $\frac{\|(q-1)\alpha\|}{q+1} \leqslant \frac{1}{2q} \leqslant \frac{\sqrt{3}}{\pi q} \leqslant \sqrt{\frac{3}{\pi^2(q^2-1)}}$. Thus

$$\max_{t\in\mathbb{R}} \varphi_q(\alpha - t)\varphi_q(\alpha - qt) \leqslant q\varphi_q\left(\frac{\|(q-1)\alpha\|}{q+1}\right) \leqslant q^2 \exp\left(-\frac{\pi^2(q-1)}{6(q+1)}\|(q-1)\alpha\|^2\right).$$

Let $\lambda \geqslant 2$. We can finish the proof by using (3.3) (and noticing that $\varphi_q(t) \leqslant q$ in the case that λ is odd). We have

$$|F_\lambda(h,\alpha)| \leqslant \prod_{1\leqslant j\leqslant\lfloor\lambda/2\rfloor} \frac{\varphi_q\left(\alpha - q^{-2j}\right)\varphi_q\left(\alpha - q^{-2j+1}\right)}{q^2},$$

and finally obtain (note, that $\lfloor\lambda/2\rfloor \geqslant (\lambda-1)/2$)

$$|F_\lambda(h,\alpha)| \leqslant \exp\left(-\frac{\pi^2(q-1)}{6(q+1)}\lfloor\lambda/2\rfloor\|(q-1)\alpha\|^2\right) \leqslant e^{\pi^2/48} q^{-c_q\|(q-1)\alpha\|^2\lambda},$$

where $c_q = \frac{\pi^2}{12\log q}\left(1 - \frac{2}{q+1}\right)$. Since $c_q\|(q-1)\alpha\|^2 \leqslant \frac{\pi^2}{48\log q}$, this inequality holds trivially for $\lambda = 1$. ∎

Average estimates of first order

In the next lemmas, we want to study more precisely φ_q and some average estimates of φ_q in order to find an upper bound of

$$\sum_{\substack{0\leqslant h<q^\lambda \\ h\equiv a \bmod kq^\delta}} |F_\lambda(h,\alpha)|. \tag{3.5}$$

It turns out, that the cases $q = 2$ and $q \geqslant 3$ are essentially different. We need the following function, that has been already studied accurately by Fouvry and Mauduit in [18].

Definition 3.3 *Let $q \geqslant 2$. Then we define the function Ψ_q on $\mathbb{R}$ by*

$$\Psi_q(t) = \frac{1}{q}\sum_{0\leqslant r<q} \varphi_q\left(t + \frac{r}{q}\right). \tag{3.6}$$

Lemma 3.7 *Let $q \geqslant 2$. Then, the function Ψ_q is periodic of period $1/q$ and continuous on $\mathbb{R}$. Moreover, we have*

$$\max_{t\in\mathbb{R}} \Psi_q(t) \leqslant \frac{2}{q\sin\frac{\pi}{2q}} + \frac{2}{\pi}\log\frac{2q}{\pi} \ll \log q. \tag{3.7}$$

Proof. First, we note that $\Psi_q(t)$ is obviously continuous and periodic of period $1/q$, since φ_q is continuous and periodic of period 1. Our first claim to get (3.7) is, that the maximum of this function is attained at $1/2q$. Fouvry and Mauduit (see [18, Lemma 2]) used a ingenious idea to show that $\Psi_q(t)$ is concave and symmetric with respect to $1/(2q)$ for $t \in [0, 1/q]$. Using the periodicity, we only have to look at this interval. For $t \in [0, 1/q]$, we can write

$$\Psi_q(t) = \frac{1}{q}\sum_{0\leqslant r<q} \frac{\sin\pi qt}{\sin\pi(t + r/q)} = \frac{1}{q}\sum_{0\leqslant r<q} (-1)^r \frac{\sin\pi q(t + r/q)}{\sin\pi(t + r/q)}.$$

If $q = 2n$, we obtain

$$\begin{aligned}
2\sum_{j=0}^{n-1}\cos\left((2j+1)\left(t+\frac{r}{2n}\right)\pi\right) &= \sum_{j=0}^{n-1}\left(e^{i\pi\left((2j+1)\left(t+\frac{r}{2n}\right)\right)}+e^{-i\pi\left((2j+1)\left(t+\frac{r}{2n}\right)\right)}\right)\\
&= e^{i\pi\left(t+\frac{r}{2n}\right)}\sum_{j=0}^{n-1}e^{2i\pi j\left(t+\frac{r}{2n}\right)}+e^{-i\pi\left(t+\frac{r}{2n}\right)}\sum_{j=0}^{n-1}e^{-2i\pi j\left(t+\frac{r}{2n}\right)}\\
&= e^{i\pi\left(t+\frac{r}{2n}\right)}\frac{e^{2i\pi n\left(t+\frac{r}{2n}\right)}-1}{e^{2i\pi\left(t+\frac{r}{2n}\right)}-1}+e^{-i\pi\left(t+\frac{r}{2n}\right)}\frac{e^{-2i\pi n\left(t+\frac{r}{2n}\right)}-1}{e^{-2i\pi\left(t+\frac{r}{2n}\right)}-1}\\
&= \frac{e^{i\pi q\left(t+\frac{r}{2n}\right)}-1-e^{-i\pi q\left(t+\frac{r}{2n}\right)}+1}{e^{i\pi\left(t+\frac{r}{2n}\right)}-e^{-i\pi\left(t+\frac{r}{2n}\right)}}\\
&= \frac{\sin\pi q(t+\frac{r}{q})}{\sin\pi(t+\frac{r}{q})}.
\end{aligned} \tag{3.8}$$

Hence, we can write $\Psi_q(t)$ in the form

$$\begin{aligned}
\Psi_q(t) &= \frac{2}{2n}\sum_{r=0}^{2n-1}(-1)^r\sum_{j=0}^{n-1}\cos\left((2j+1)\left(t+\frac{r}{2n}\right)\pi\right)\\
&= \frac{2}{2n}\sum_{j=0}^{n-1}\sum_{r=0}^{2n-1}(-1)^r\cos\left((2j+1)\left(t+\frac{r}{2n}\right)\pi\right).
\end{aligned}$$

Using the equality (which can be similar proved as (3.8))

$$\sum_{r=0}^{m-1}(-1)^r\cos(a+hr) = \frac{\cos\left(a+\frac{m-1}{2}h+\frac{m-1}{2}\pi\right)\sin\left(\frac{mh}{2}+\frac{m\pi}{2}\right)}{\cos\frac{h}{2}}, \tag{3.9}$$

we get

$$\begin{aligned}
\Psi_q(t) &= \frac{2}{2n}\sum_{j=0}^{n-1}\frac{\cos\left((2j+1)\pi t+\frac{2n-1}{2}\frac{2j+1}{2n}\pi+\frac{2n-1}{2}\pi\right)\sin\left(n\frac{(2j+1)\pi}{2n}+n\pi\right)}{\cos\frac{(2j+1)\pi}{4n}}\\
&= \frac{2}{2n}\sum_{j=0}^{n-1}\frac{\cos\left((2j+1)\pi t-\frac{2j+1}{4n}\pi\right)(-1)^{j+1}(-1)^{n+1}(-1)^j(-1)^n}{\cos\frac{(2j+1)\pi}{4n}}\\
&= \frac{2}{2n}\sum_{j=0}^{n-1}\frac{\cos\left((2j+1)\pi t-\frac{2j+1}{4n}\pi\right)}{\cos\frac{(2j+1)\pi}{4n}}.
\end{aligned}$$

Since $j = 0,\dots,n-1$ and $t \in [0, 1/2n]$, we have $-\frac{\pi}{2} < (2j+1)\left(t-\frac{1}{4n}\right)\pi < \frac{\pi}{2}$. Hence, $\Psi_q(t)$ is a sum of concave functions and therefore itself a concave function. We also see from this representation, that $\Psi_q(t) = \Psi_q(1/q - t)$. Thus, we can conclude, that the maximum is attained at the point $t = 1/4n = 1/2q$. The case $q = 2n+1$ is almost the same as the first case, we only have to notice that

$$(-1)^r + 2(-1)^r\sum_{j=0}^{n}\cos\left(2j\pi\left(t+\frac{r}{2n+1}\right)\right) = (-1)^r\frac{\sin\pi q\left(t+\frac{r}{q}\right)}{\sin\pi\left(t+\frac{r}{q}\right)}.$$

This can be proved in the same way as we proved (3.8). Using (3.9), one gets again a representation for $\Psi_q(t)$ as a sum of concave functions where it is once more easy to see, that it is symmetric with respect

to $t = 1/(4n+2) = 1/2q$. Hence, we have proved the first claim. Thus we have

$$\max_{t\in\mathbb{R}} \Psi_q(t) = \Psi_q\left(\frac{1}{2q}\right) = \frac{1}{q}\sum_{r=0}^{q-1} \frac{1}{\sin\frac{\pi}{q}\left(\frac{1}{2}+r\right)}. \tag{3.10}$$

Separating the first and the last summand in the last sum, we can use Lemma A.7 since $u \mapsto 1/(\sin u)$ is convex on the interval $[0,\pi]$. We obtain

$$\begin{aligned}\max_{t\in\mathbb{R}} \Psi_q(t) &\leqslant \frac{1}{q\sin\frac{\pi}{2q}} + \frac{1}{q\sin\frac{\pi}{q}\left(q-\frac{1}{2}\right)} + \frac{1}{q}\int_{1/2}^{q-3/2} \frac{dt}{\sin\frac{\pi}{q}\left(\frac{1}{2}+t\right)} \\ &= \frac{2}{q\sin\frac{\pi}{2q}} + \frac{2}{\pi}\log\cot\frac{\pi}{2q} \leqslant \frac{2}{q\sin\frac{\pi}{2q}} + \frac{2}{\pi}\log\frac{2q}{\pi}.\end{aligned}$$

The last inequality is obtained from the fact that $\cot\frac{\pi}{2q} \leqslant \frac{2q}{\pi}$. Since $q\sin\frac{\pi}{2q} \geqslant q\frac{2\sqrt{2}}{\pi}\frac{\pi}{2q} = \sqrt{2}$ (note, that $q \geqslant 2$) we finally have

$$\max_{t\in\mathbb{R}} \Psi_q(t) \ll \log q.$$

■

Remark. In particular, one can easily calculate that $\max_{t\in\mathbb{R}} \Psi_2(t) = \sqrt{2}$ and $\max_{t\in\mathbb{R}} \Psi_3(t) = \frac{5}{3}$. As we will see later, the value for $\max_{t\in\mathbb{R}} \Psi_2(t)$ is not sufficient for our further studies. Hence we have to treat the case $q = 2$ in a separate way. At first, we study the case $q \geqslant 3$, which allows us to state the following lemma.

Lemma 3.8 *For $q \geqslant 3$, we define η_q by $q^{\eta_q} = \max_{t\in\mathbb{R}} \Psi_q(t)$. Then we have for $q \geqslant 4$*

$$0 < \eta_q < \eta_3 \quad \textit{and} \quad 0,4649 < \eta_3 = \frac{\log 5}{\log 3} - 1 < 0,465. \tag{3.11}$$

Proof. By Lemma 3.7, we have $q^{\eta_q} = \max_{t\in\mathbb{R}} \Psi_q(t) \leqslant \frac{2}{q\sin\frac{\pi}{2q}} + \frac{2}{\pi}\log\frac{2q}{\pi}$. Since sin is concave on the interval $(0,\pi)$ and $q \geqslant 4$, we can write $\sin\frac{\pi}{2q} = \sin\left(\frac{4}{q}\frac{\pi}{8}\right) \geqslant \frac{4}{q}\sin\frac{\pi}{8}$. Thus we obtain

$$q^{\eta_q} - q^{\eta_3} \leqslant \frac{1}{2\sin\frac{\pi}{8}} + \frac{2}{\pi}\log\frac{2q}{\pi} - q^{\eta_3}.$$

The function in q on the right hand side is decreasing for $q \geqslant 4$ and is approximately $-0,004 < 0$ for $q = 4$. Hence we get the desired inequality in (3.11). ■

We also need a generalization of Ψ_q in order to handle the case $q \geqslant 3$.

Definition 3.4 *Let $q \geqslant 3$ and $2 \leqslant R \leqslant q$ with $R \mid q$. Then we define for $t \in \mathbb{R}$*

$$\Psi_{q,R}(t) = \frac{1}{q}\sum_{1\leqslant r\leqslant R} \varphi_q\left(t + \frac{r}{R}\right).$$

Lemma 3.9 *If $q \geqslant 3$, $R \mid q$ and $2 \leqslant R \leqslant q$, then we have*

$$\max_{t\in\mathbb{R}} \Psi_{q,R}(t) \leqslant R^{\eta_3},$$

where η_3 is defined in Lemma 3.8.

Proof. We begin the proof with reducing $\Psi_{q,R}$ to the known function Ψ_q.

$$\Psi_{q,R}(t) = \frac{R}{q}\left|\frac{\sin \pi q t}{\sin \pi R t}\right| \frac{1}{R} \sum_{1 \leqslant r \leqslant R} \varphi_R\left(t + \frac{r}{R}\right) = \frac{R}{q}\varphi_{q/R}(Rt)\Psi_R(t) \leqslant \psi_R(t).$$

The last inequality follows from the fact that $\varphi_{q/R} \leqslant q/R$. We split the proof of this lemma up into two parts. First, we consider $R \geqslant 3$. In this case, we have already enough information to get our desired result. Using Lemma 3.7 and Lemma 3.8, we obtain

$$\Psi_{q,R}(t) \leqslant \Psi_R(t) \leqslant R^{\eta_q} \leqslant R^{\eta_3}.$$

Assume now that $R = 2$. Since $\Psi_{q,2}$ is periodic of period $1/2$ and satisfies $\Psi_{q,2}(1/2 - t) = \Psi_{q,2}(t)$, it suffices to look at the interval $[0, \frac{1}{4}]$. To be able to find an upper bound, we split it up into three parts. First we consider the interval $[0, \frac{1}{3q}]$. From the initial estimation, we know that

$$\Psi_{q,2}(t) \leqslant \Psi_2(t) = \cos \pi t + \sin \pi t.$$

Hence, wo obtain (note, that $q \geqslant 4$)

$$\max_{t \in [0, \frac{1}{3q}]} \Psi_{q,2}(t) \leqslant \max_{t \in [0, \frac{1}{3q}]} (\cos \pi t + \sin \pi t) = \max_{t \in [0, \frac{1}{3q}]} \sqrt{1 + \sin 2\pi t} \leqslant \sqrt{1 + \sin \frac{\pi}{6}} = \sqrt{\frac{3}{2}}.$$

In the next step, we are interested in $[\frac{1}{3q}, \frac{1}{q}]$. We know that $\Psi_2(t) \leqslant \sqrt{2}$ and $\varphi_{\frac{q}{2}}$ is decreasing on $[0, \frac{2}{q}]$ (see Lemma 3.1). Furthermore we can use that *sin* is concave on $[0, \pi]$ and derive

$$\begin{aligned}\max_{t \in [\frac{1}{3q}, \frac{1}{q}]} \Psi_{q,2}(t) &\leqslant \max_{t \in [\frac{1}{3q}, \frac{1}{q}]} \frac{2}{q}\varphi_{q/2}(2t)\Psi_2(t) \leqslant \frac{2\sqrt{2}}{q}\varphi_{q/2}\left(\frac{2}{3q}\right) = \frac{2\sqrt{2}}{q}\frac{\sin \frac{\pi}{3}}{\sin \frac{4}{q}\frac{\pi}{6}} \\ &\leqslant \frac{2\sqrt{2}}{q}\frac{\sin \frac{\pi}{3}}{\frac{4}{q}\sin \frac{\pi}{6}} = \frac{2\sqrt{2}}{q}\frac{\sqrt{3}q}{4} = \sqrt{\frac{3}{2}}.\end{aligned}$$

On the remaining interval, we have

$$\max_{t \in [\frac{1}{q}, \frac{1}{4}]} \Psi_{q,2}(t) \leqslant \max_{t \in [\frac{1}{q}, \frac{1}{4}]} \frac{2}{q}\varphi_{q/2}(2t)\Psi_2(t) \leqslant \frac{2\sqrt{2}}{q} \max_{t \in [\frac{1}{q}, \frac{1}{4}]} \frac{1}{\sin 2\pi t} = \frac{2\sqrt{2}}{q}\frac{1}{\sin \frac{2\pi}{q}} \leqslant \frac{2\sqrt{2}}{q}\frac{q}{4} \leqslant \sqrt{\frac{3}{2}}.$$

Since $\sqrt{\frac{3}{2}} < 1,23 < 1,38 < 2^{\frac{\log 5}{\log 3} - 1} = R^{\eta_3}$, we are done. ∎

Lemma 3.10 *For $q \geqslant 3$, $\alpha \in \mathbb{R}$, $a \in \mathbb{Z}$, $0 \leqslant \delta \leqslant \lambda$, $k \mid q^{\lambda-\delta}$ and $k \nmid q$, we have*

$$\sum_{\substack{0 \leqslant h < q^\lambda \\ h \equiv a \bmod kq^\delta}} |F_\lambda(h, \alpha)| \leqslant k^{-\eta_3} q^{\eta_3(\lambda-\delta)} |F_\delta(a, \alpha)|. \tag{3.12}$$

Proof. If $\lambda = \delta$, then the condition $k \mid q^{\lambda-\delta}$ implies $k = 1$ and the statement holds trivially. If $\lambda > \delta$, then we define $d_\theta = (q^\theta, kq^\delta)$ and $u_\theta = q^\theta/d_\theta$ whenever $\delta \leqslant \theta \leqslant \lambda$. Additionally we define $\rho_\theta = d_\theta/d_{\theta-1}$ and it is easy to see that the following claims hold: ρ_θ is an integer satisfying $\rho_\theta \mid q$ and $\rho_\theta < q$. Indeed, we have $d_{\theta-1} = (q^{\theta-1}, d_\theta) \mid d_\theta$ which implies that ρ_θ is an integer. Since $d_{\theta-1}(\rho_\theta, q) = (d_\theta, qd_{\theta-1}) = (q^\theta, kq^\theta, q^\theta, kq^{\theta+1}) = d_\theta = \rho_\theta d_{\theta-1}$, we obtain that $\rho_\theta \mid q$. Finally, if we assume that $\rho_\theta = q$, we see from the last equation that q has to be a divisor of k. This contradicts our hypothesis $q \nmid k$ and proves the last claim.

The main idea of the proof is to find a recursion. For $\delta < \theta \leqslant \lambda$, we can write

$$\sum_{\substack{0\leqslant h<q^\theta \\ h\equiv a \bmod d_\theta}} |F_\theta(h,\alpha)| = \sum_{0\leqslant u<u_\theta} |F_\theta(a+ud_\theta,\alpha)| = \sum_{0\leqslant u<u_\theta} |F_\theta(a+u\rho_\theta d_{\theta-1},\alpha)|$$

$$\overset{(*)}{=} \sum_{\substack{0\leqslant v<qu_{\theta-1} \\ v\equiv 0 \bmod \rho_\theta}} |F_\theta(a+vd_{\theta-1},\alpha)|$$

$$\overset{(**)}{=} \sum_{0\leqslant u<u_{\theta-1}} \sum_{\substack{0\leqslant w<q \\ u+wu_{\theta-1}\equiv 0 \bmod \rho_\theta}} |F_\theta(a+(u+wu_{\theta-1})d_{\theta-1},\alpha)|.$$

In $(*)$ we replaced $u\rho_\theta$ by v and used that $\rho_\theta u_\theta = qu_{\theta-1}$. In $(**)$ we employed the Euclidean algorithm to obtain the last expression. Since $d_{\theta-1}(\rho_\theta, u_{\theta-1}) = (d_\theta, q^{\theta-1}) = (q^\theta, kq^\delta, q^{\theta-1}) = d_{\theta-1}$, we see that $(\rho_\theta, u_{\theta-1}) = 1$. This implies that $u_{\theta-1}$ has an inverse modulo ρ_θ (say $\tilde{u}_{\theta-1}$). Thus we can rewrite the condition $u + wu_{\theta-1} \equiv 0 \bmod \rho_\theta$ to $w = -u\tilde{u}_{\theta-1} - r\rho_\theta$, where $0 \leqslant r < q/\rho_\theta$. Indeed, this follows from the fact that we have originally $0 \leqslant w < q$. Noticing that $u_{\theta-1}d_{\theta-1} = q^{\theta-1}$ and that $F_{\theta-1}(.,\alpha)$ is periodic of period $q^{\theta-1}$, we obtain by (3.2)

$$\sum_{\substack{0\leqslant h<q^\theta \\ h\equiv a \bmod d_\theta}} |F_\theta(h,\alpha)| = \sum_{0\leqslant u<u_{\theta-1}} |F_{\theta-1}(a+ud_{\theta-1},\alpha)| \sum_{\substack{0\leqslant r<q/\rho_\theta \\ w=-u\tilde{u}_{\theta-1}-r\rho_\theta}} \frac{1}{q}\,\varphi_q\left(\alpha - \frac{a+ud_{\theta-1}}{q^\theta} - \frac{w}{q}\right)$$

$$= \sum_{0\leqslant u<u_{\theta-1}} |F_{\theta-1}(a+ud_{\theta-1},\alpha)|\, \Psi_{q,q/\rho_\theta}\left(\alpha - \frac{a+ud_{\theta-1}-u\tilde{u}_{\theta-1}q^{\theta-1}}{q^\theta}\right). \tag{3.13}$$

By Lemma 3.9, we obtain

$$\sum_{\substack{0\leqslant h<q^\theta \\ h\equiv a \bmod d_\theta}} |F_\theta(h,\alpha)| \leqslant \rho_\theta^{-\eta_3} q^{\eta_3} \sum_{\substack{0\leqslant h<q^{\theta-1} \\ h\equiv a \bmod d_{\theta-1}}} |F_{\theta-1}(h,\alpha)|.$$

Iterating this process $\lambda - \delta$ times, and noticing that $d_\lambda = kq^\delta$, we get

$$\sum_{\substack{0\leqslant h<q^\lambda \\ h\equiv a \bmod kq^\delta}} |F_\lambda(h,\alpha)| \leqslant \rho_{\delta+1}^{-\eta_3} \cdots \rho_\lambda^{-\eta_3} q^{\eta_3(\lambda-\delta)} |F_\delta(a,\alpha)|.$$

But since

$$\rho_{\delta+1}\cdots\rho_\lambda = \frac{d_{\delta+1}}{d_\delta}\cdots\frac{d_\lambda}{d_{\lambda-1}} = \frac{d_\lambda}{d_\delta} = \frac{kq^\delta}{q^\delta} = k,$$

we have proved the desired estimation. ∎

If q is a prime, then k has to be 1 ($k \mid q^{\lambda-\delta}$ but $k \nmid q$). In this case, the proof is much easier. We have $d_\theta = (q^\theta, q^\delta) = q^\delta$ for all $\delta \leqslant \theta \leqslant \lambda$ and therefore $\rho_\theta = 1$. Hence, we consider the function $\Psi_{q,q} = \Psi_q$ in (3.13). But this implies, that we get the better constant η_q since $q^{\eta_q} = \max_t \Psi_q(t)$.

We will see in Chapter 5 that the crucial point in this lemma is the matter of fact that we have (3.12) with $\eta_3 < 1/2$. Here we see the reason why we cannot use the same procedure for $q = 2$. If we defined η_2 in the same way, we would have the same inequality with $\eta_2 = 1/2$. The next lemma gives us an answer, how we can deal with this problem. Actually, the simplified form of the Fourier transform in case $q = 2$ helps us to obtain the following statement, where we define η_2 in a completely different manner to get a similar result.

Lemma 3.11 *For $q = 2$ we define η_2 by the equation*

$$2^{\eta_2} = (2 + \sqrt{2})^{1/4} \quad \textit{(in particular } 0,4428 < \eta_2 < 0,4429\textit{).}$$

Then we have for all $\alpha \in \mathbb{R}$, $a \in \mathbb{Z}$ and $0 \leqslant \delta \leqslant \lambda$

$$\sum_{\substack{0 \leqslant h < 2^\lambda \\ h \equiv a \bmod 2^\delta}} |F_\lambda(h,\alpha)| \leqslant 2^{\eta_2(\lambda-\delta)+1/2} |F_\delta(h,\alpha)|.$$

Proof. If $\lambda = 0$ we have $|F_0(h,\alpha)| = 1$, and the desired inequality holds trivially. If $\lambda \geqslant 1$ (3.2) allows us to write

$$|F_\lambda(h,\alpha)| = \prod_{j=1}^{\lambda} |\cos \pi(\alpha - h2^{-j})| = |\cos \pi(\alpha - h2^{-\lambda})||F_{\lambda-1}(h,\alpha)|.$$

Hence, we get for $0 \leqslant \delta \leqslant \lambda$

$$\begin{aligned}\sum_{\substack{0 \leqslant h < 2^{\lambda+1} \\ h \equiv a \bmod 2^\delta}} |F_{\lambda+1}(h,\alpha)| &= \sum_{\substack{0 \leqslant h < 2^{\lambda} \\ h \equiv a \bmod 2^\delta}} |F_{\lambda+1}(h,\alpha)| + \sum_{\substack{0 \leqslant h < 2^{\lambda} \\ h \equiv a \bmod 2^\delta}} |F_{\lambda+1}(h+2^\lambda,\alpha)| \\ &= \sum_{\substack{0 \leqslant h < 2^{\lambda} \\ h \equiv a \bmod 2^\delta}} |F_\lambda(h,\alpha)\left(\left|\cos \pi\left(\alpha - h2^{-(\lambda+1)}\right)\right| + \left|\sin \pi\left(\alpha - h2^{-(\lambda+1)}\right)\right|\right).\end{aligned}$$

We obtain from $|\cos x| + |\sin x| = \sqrt{1 + |\sin 2x|} \leqslant \sqrt{2}$ that

$$\sum_{\substack{0 \leqslant h < 2^{\lambda+1} \\ h \equiv a \bmod 2^\delta}} |F_{\lambda+1}(h,\alpha)| \leqslant \sqrt{2} \sum_{\substack{0 \leqslant h < 2^{\lambda} \\ h \equiv a \bmod 2^\delta}} |F_\lambda(h,\alpha). \tag{3.14}$$

Applying this inequality $\lambda - \delta$ times would again yield an exponent $1/2$. Hence we iterate the recurrence relation a second time and can write for $\sum_{\substack{0 \leqslant h < 2^{\lambda+1} \\ h \equiv a \bmod 2^\delta}} |F_{\lambda+1}(h,\alpha)|$

$$\begin{aligned}&\sum_{\substack{0 \leqslant h < 2^{\lambda-1} \\ h \equiv a \bmod 2^\delta}} |F_\lambda(h,\alpha)| \left(\left|\cos \pi\left(\alpha - h2^{-(\lambda+1)}\right)\right| + \left|\sin \pi\left(\alpha - h2^{-(\lambda+1)}\right)\right|\right) \\ &+ \sum_{\substack{0 \leqslant h < 2^{\lambda-1} \\ h \equiv a \bmod 2^\delta}} |F_\lambda(h+2^{\lambda-1},\alpha)| \left(\left|\cos \pi\left(\alpha - (h+2^{\lambda-1})2^{-(\lambda+1)}\right)\right| + \left|\sin \pi\left(\alpha - (h+2^{\lambda-1})2^{-(\lambda+1)}\right)\right|\right) \\ = &\sum_{\substack{0 \leqslant h < 2^{\lambda-1} \\ h \equiv a \bmod 2^\delta}} |F_{\lambda-1}(h,\alpha)| \left(\left|\cos \pi\left(\alpha - h2^{-\lambda}\right)\right| \left(\left|\cos \pi\left(\alpha - h2^{-(\lambda+1)}\right)\right| + \left|\sin \pi\left(\alpha - h2^{-(\lambda+1)}\right)\right|\right)\right. \\ &\left. + \left|\sin \pi\left(\alpha - h2^{-\lambda}\right)\right| \left(\left|\cos \pi\left(\alpha - h2^{-(\lambda+1)} - 1/4\right)\right| + \left|\sin \pi\left(\alpha - h2^{-(\lambda+1)} - 1/4\right)\right|\right)\right).\end{aligned}$$

Using again $(|\cos x| + |\sin x|)^2 = 1 + |\sin 2x|$ and its conclusion $|\cos x| + |\sin x| \leqslant \sqrt{2}$ as well as $(|\cos\theta|a + |\sin\theta|b)^2 \leqslant a^2 + b^2$, we obtain

$$\begin{aligned}&\left|\cos \pi\left(\alpha - h2^{-\lambda}\right)\right| \left(\left|\cos \pi\left(\alpha - h2^{-(\lambda+1)}\right)\right| + \left|\sin \pi\left(\alpha - h2^{-(\lambda+1)}\right)\right|\right) \\ &+ \left|\sin \pi\left(\alpha - h2^{-\lambda}\right)\right| \left(\left|\cos \pi\left(\alpha - h2^{-(\lambda+1)} - 1/4\right)\right| + \left|\sin \pi\left(\alpha - h2^{-(\lambda+1)} - 1/4\right)\right|\right) \\ \leqslant &\sqrt{\left(1 + \left|\sin 2\pi\left(\alpha - h2^{-(\lambda+1)}\right)\right|\right) + \left(1 + \left|\cos 2\pi\left(\alpha - h2^{-(\lambda+1)}\right)\right|\right)} \leqslant \sqrt{2 + \sqrt{2}}.\end{aligned}$$

Hence we have derived

$$\sum_{\substack{0\leqslant h<2^{\lambda+1}\\ h\equiv a \bmod 2^\delta}} |F_{\lambda+1}(h,\alpha)| \leqslant (2+\sqrt{2})^{1/2} \sum_{\substack{0\leqslant h<2^{\lambda-1}\\ h\equiv a \bmod 2^\delta}} |F_{\lambda-1}(h,\alpha)|.$$

Applying this inequality $\left\lfloor \frac{\lambda-\delta}{2} \right\rfloor$-times (and if $\lambda-\delta$ is odd (3.14) one more time), we finally showed the desired estimation. ∎

Average estimates of second order

Using Lemma 3.6, we can give an upper bound of the following average of second order

$$\sum_{\substack{0\leqslant h<q^\lambda\\ h\not\equiv 0 \bmod q}} \frac{|F_\lambda(h,\alpha)|^2}{\left|\sin\frac{\pi h a}{q^\lambda}\right|}.$$

Before we can state and prove the exact result, we illustrate two useful observations.

Lemma 3.12 *For every $q\geqslant 2$ and $t\in\mathbb{R}$, we have*

$$\sum_{0\leqslant r<q} \varphi_q^2\left(t+\frac{r}{q}\right) = q^2. \tag{3.15}$$

Proof. Writing φ_q again as a geometric series, we obtain

$$\begin{aligned}\sum_{0\leqslant r<q} \varphi_q^2\left(t+\frac{r}{q}\right) &= \sum_{0\leqslant r<q}\left|\sum_{0\leqslant v<q} \mathrm{e}\left(v\left(t+\frac{r}{q}\right)\right)\right|^2\\ &= \sum_{0\leqslant r<q}\sum_{0\leqslant u<q}\sum_{0\leqslant v<q} \mathrm{e}\left((v-u)\left(t+\frac{r}{q}\right)\right)\\ &= q\sum_{0\leqslant u<q}\sum_{0\leqslant v<q} \mathrm{e}((v-u)t)\frac{1}{q}\sum_{0\leqslant r<q}\mathrm{e}\left(\frac{v-u}{q}r\right) = q^2.\end{aligned}$$

Indeed, by Lemma 1.2, we get the last equality since $q \mid u-v$ only if $u=v$. ∎

Lemma 3.13 *Let $q\geqslant 2$, $a\in\mathbb{Z}$ and $0\leqslant\delta\leqslant\lambda$. Then we have*

$$\sum_{\substack{0\leqslant h<q^\lambda\\ h\equiv a \bmod q^\delta}} |F_\lambda(h,\alpha)|^2 = |F_\delta(a,\alpha)|^2. \tag{3.16}$$

Proof. We observe, that for $\lambda>\delta$ by Euclid's algorithm

$$\sum_{\substack{0\leqslant h<q^\lambda\\ h\equiv a \bmod q^\delta}} |F_\lambda(h,\alpha)|^2 = \sum_{0\leqslant r<q}\sum_{\substack{0\leqslant h<q^{\lambda-1}\\ h\equiv a \bmod q^\delta}} |F_\lambda(h+rq^{\lambda-1},\alpha)|^2.$$

Using the recursive definition of $|F_\lambda(h + rq^{\lambda-1}, \alpha)|$ (see (3.2)), the periodicity of the Fourier transform and (3.15) we get

$$\begin{aligned}\sum_{\substack{0\leqslant h<q^\lambda\\ h\equiv a \bmod q^\delta}} |F_\lambda(h,\alpha)|^2 &= \sum_{\substack{0\leqslant h<q^{\lambda-1}\\ h\equiv a \bmod q^\delta}} |F_{\lambda-1}(h,\alpha)|^2 \frac{1}{q^2} \sum_{0\leqslant r<q} \varphi_q^2\left(\alpha - \frac{h}{q^\lambda} - \frac{r}{q}\right)\\ &= \sum_{\substack{0\leqslant h<q^{\lambda-1}\\ h\equiv a \bmod q^\delta}} |F_{\lambda-1}(h,\alpha)|^2.\end{aligned}$$

Applying this equality $\lambda - \delta$ times, we obtain (3.16). ∎

The proof of the following lemma, which gives us the desired average estimate of second order, is different from Mauduit's and Rivat's proof in [33]. It follows the idea of Drmota, Rivat and Stoll, where they showed an analogous result in $\mathbb{Z}[i]$ (see [15, Corollary 6.5]).

Lemma 3.14 *Let $q \geqslant 2$, $\alpha \in \mathbb{R}$ such that $(q-1)\alpha \notin \mathbb{Z}$ and $a \in \mathbb{Z}$ with $(a,q) = 1$. Then we have for $\lambda \geqslant 1$*

$$\sum_{\substack{0\leqslant h<q^\lambda\\ h\not\equiv 0 \bmod q}} \frac{|F_\lambda(h,\alpha)|^2}{\left|\sin\frac{\pi h a}{q^\lambda}\right|} \ll q^{(1-c_q\|(q-1)\alpha\|^2)\lambda}. \tag{3.17}$$

where $c_q = \frac{\pi^2}{12\log q}\left(1 - \frac{2}{q+1}\right)$ and $0 < c_q\|(q-1)\alpha\|^2 < 1$.

Proof. We write $ah = iq^\lambda + j$, where $0 \leqslant j < q^\lambda$ in a unique way, since $0 \leqslant h < q^\lambda$. Because $(a,q) = 1$ and $h \not\equiv 0 \bmod q$, we have $j \neq 0$ and $j \not\equiv 0 \bmod q$. Hence we get

$$\frac{1}{\left|\sin\frac{\pi h a}{q^\lambda}\right|} = \frac{1}{\left|\sin\pi\frac{iq^\lambda + j}{q^\lambda}\right|} = \frac{1}{\left|\sin\frac{\pi j}{q^\lambda}\right|} \leqslant \frac{1}{\frac{2}{\pi}\pi\left\|\frac{j}{q^\lambda}\right\|} \leqslant \frac{q^\lambda}{2}\frac{1}{\min\{j, q^\lambda - j\}}.$$

Hence, by writing again h for j, the left hand side of (3.17) is bounded by

$$\frac{q^\lambda}{2}\sum_{0\leqslant h<q^\lambda} \frac{|F_\lambda(h,\alpha)|^2}{\min\{h, q^\lambda - h\}}.$$

Let $M < q^\lambda$ be an integer. Using Lemma 3.6 with c_q as defined there, we can write

$$\begin{aligned}\sum_{\substack{0\leqslant h<q^\lambda\\ h\not\equiv 0 \bmod q}} \frac{|F_\lambda(h,\alpha)|^2}{\left|\sin\frac{\pi h a}{q^\lambda}\right|} &\leqslant \frac{q^\lambda}{2}\left(\sum_{\substack{0\leqslant h<q^\lambda\\ \min\{h,q^\lambda-h\}\geqslant M}} \frac{|F_\lambda(h,\alpha)|^2}{\min\{h,q^\lambda-h\}} + \sum_{\substack{0\leqslant h<q^\lambda\\ \min\{h,q^\lambda-h\}<M}} \frac{e^{\pi^2/24}q^{-2c_q\|(q-1)\alpha\|^2\lambda}}{\min\{h,q^\lambda-h\}}\right)\\ &\leqslant \frac{q^\lambda}{2}\left(\frac{1}{M}\sum_{0\leqslant h<q^\lambda} |F_\lambda(h,\alpha)|^2 + e^{\pi^2/24}q^{-2c_q\|(q-1)\alpha\|^2\lambda}2M\right)\\ &\ll q^\lambda\frac{1}{M} + q^{(1-2c_q\|(q-1)\alpha\|^2)\lambda}M.\end{aligned}$$

Choosing $M = q^{c_q\|(q-1)\alpha\|^2\lambda}$, we obtain

$$\sum_{\substack{0\leqslant h<q^\lambda\\ h\not\equiv 0 \bmod q}} \frac{|F_\lambda(h,\alpha)|^2}{\left|\sin\frac{\pi h a}{q^\lambda}\right|} \ll q^{(1-c_q\|(q-1)\alpha\|^2)\lambda}.$$

The inequalities $0 < c_q\|(q-1)\alpha\|^2 < 1$ finally follow from the fact that $(q-1)\alpha \notin \mathbb{Z}$ and $\|t\| \leqslant 1/2$ for all $t \in \mathbb{R}$. ∎

3.2 Fourier Transform of $\mathrm{e}\left(f_{\eta,\lambda}(.)\right)$

As we will see in the proof of Gelfond's problem on the sum of digits function of squares, it isn't sufficient to study the truncated function f_λ. Therefore we only use digits of squares from a special interval. For $1 \leqslant \eta < \lambda$ we define the double truncated function

$$f_{\eta,\lambda}(n) = f_\lambda(n) - f_\eta(n).$$

In this section, our main interest lies again on the discrete Fourier transform, but this time of $\mathrm{e}(f_{\eta,\lambda}(n))$.

Definition 3.5 *Let $q \geqslant 2$, $\alpha \in \mathbb{R}$ and $1 \leqslant \eta < \lambda$ be integers. The function $F_{\eta,\lambda}(.,\alpha)$ is defined for all $h \in \mathbb{Z}$ by*

$$F_{\eta,\lambda}(h,\alpha) = \frac{1}{q^\lambda} \sum_{0 \leqslant u < q^\lambda} \mathrm{e}\left(f_{\eta,\lambda}(u) - huq^{-\lambda}\right).$$

Using the Euclidean algorithm, we can write $u = q^\eta k + l$ for all $0 \leqslant u < q^\lambda$, where $0 \leqslant k < q^{\lambda-\eta}$ and $0 \leqslant l < q^\eta$. Since this implies $f_{\eta,\lambda} = f_\lambda(k)$, we get

$$\begin{aligned} F_{\eta,\lambda}(h,\alpha) &= q^{-\lambda} \sum_{0 \leqslant k < q^{\lambda-\eta}} \sum_{0 \leqslant l < q^\eta} \mathrm{e}\left(f_\lambda(a) - h\frac{q^\eta k + l}{q^\lambda}\right) \\ &= F_{\lambda-\eta}(h,\alpha) q^{-\eta} \sum_{0 \leqslant l < q^\eta} \mathrm{e}\left(\frac{-hl}{q^\lambda}\right), \end{aligned}$$

and hence

$$|F_{\eta,\lambda}(h,\alpha)| = |F_{\lambda-\eta}(h,\alpha)| q^{-\eta} \varphi_{q^\eta}(hq^{-\lambda}). \tag{3.18}$$

This fact allows us to prove the following two lemmas, which give us upper bounds for sums of the form

$$\sum_{\substack{0 \leqslant h < q^\lambda \\ h \equiv a \bmod q^\delta}} |F_{\eta,\lambda}(h,\alpha)|.$$

In the first Lemma we have $\delta = 0$, where we can only show a trivial bound. In the second lemma, we have $\delta \geqslant \lambda - \eta$, which allows us to give some better estimates.

Lemma 3.15 *Let α be a real number and $1 \leqslant \eta < \lambda$. Then we have*

$$\sum_{0 \leqslant h < q^\lambda} |F_{\eta,\lambda}(h,\alpha)| \ll_q \eta q^{\lambda-\eta}.$$

Proof. Employing the Euclidean algorithm ($h = kq^{\lambda-\eta} + l$, where $0 \leqslant k < q^\eta$ and $0 \leqslant l < q^{\lambda-\eta}$) and using (3.18), we can write

$$\begin{aligned} \sum_{0 \leqslant h < q^\lambda} |F_{\eta,\lambda}(h,\alpha)| &= \sum_{0 \leqslant k < q^{\lambda-\eta}} \sum_{0 \leqslant l < q^\eta} |F_{\lambda-\eta}(kq^{\lambda-\eta} + l, \alpha)| q^{-\eta} \varphi_{q^\eta}\left(\frac{kq^{\lambda-\eta} + l}{q^\lambda}\right) \\ &= \sum_{0 \leqslant l < q^{\lambda-\eta}} |F_{\lambda-\eta}(l,\alpha)| q^{-\eta} \sum_{0 \leqslant k < q^\eta} \varphi_{q^\eta}\left(\frac{l}{q^\lambda} + \frac{k}{q^\eta}\right). \end{aligned}$$

By Lemma 3.7 and the trivial estimation $|F_{\lambda-\eta}(l,\alpha)| \leqslant 1$, we finally obtain

$$\sum_{0\leqslant h<q^{\lambda}} |F_{\eta,\lambda}(h,\alpha)| = \sum_{0\leqslant l<q^{\lambda-\eta}} |F_{\lambda-\eta}(l,\alpha)|\Psi_{q^{\eta}}(lq^{-\lambda}) \ll \log q^{\eta} q^{\lambda-\eta} \ll_q \eta q^{\lambda-\eta}.$$

■

Lemma 3.16 *Let $a \in \mathbb{Z},\ \alpha \in \mathbb{R}$ and $\lambda - \eta \leqslant \delta \leqslant \lambda$. Then we have*

$$\sum_{\substack{0\leqslant h<q^{\lambda}\\ h\equiv a \bmod q^{\delta}}} |F_{\eta,\lambda}(h,\alpha)| \ll_q \eta q^{-\eta+\lambda-\delta} \varphi_{q^{\eta-\lambda+\delta}}(aq^{-\delta})|F_{\lambda-\eta}(a,\alpha)|, \tag{3.19}$$

and

$$\sum_{\substack{0\leqslant h<q^{\lambda}\\ h\equiv a \bmod q^{\delta}}} |F_{\eta,\lambda}(h,\alpha)| \ll_q \eta |F_{\lambda-\eta}(a,\alpha)|. \tag{3.20}$$

Proof. Since by assumption $\lambda - \eta \leqslant \delta$, we have $|F_{\lambda-\eta}(a + lq^{\delta})| = |F_{\lambda-\eta}(a,\alpha)|$. Thus we can write

$$\begin{aligned}\sum_{\substack{0\leqslant h<q^{\lambda}\\ h\equiv a \bmod q^{\delta}}} |F_{\eta,\lambda}(h,\alpha)| &= \sum_{0\leqslant l<q^{\lambda-\delta}} |F_{\lambda-\eta}(a+lq^{\delta},\alpha)|q^{-\eta}\varphi_{q^{\eta}}\left(\frac{a+lq^{\delta}}{q^{\lambda}}\right)\\ &= |F_{\lambda-\eta}(a,\alpha)|q^{-\eta}\sum_{0\leqslant l<q^{\lambda-\delta}} \varphi_{q^{\eta}}\left(\frac{a}{q^{\lambda}}+\frac{l}{q^{\lambda-\delta}}\right).\end{aligned}$$

Since $0 \leqslant \lambda - \delta \leqslant \eta$, we have for all $t \in \mathbb{R}$

$$\varphi_{q^{\eta}}(t + lq^{-(\lambda-\delta)}) = \varphi_{q^{\eta-\lambda+\delta}}(q^{(\lambda-\delta)}t)\varphi_{q^{\lambda-\delta}}(t + lq^{-(\lambda-\delta)}).$$

Thus, we derive (using again Lemma 3.7)

$$\begin{aligned}\sum_{\substack{0\leqslant h<q^{\lambda}\\ h\equiv a \bmod q^{\delta}}} |F_{\eta,\lambda}(h,\alpha)| &= |F_{\lambda-\eta}(a,\alpha)|q^{-\eta+\lambda-\delta}\varphi_{q^{\eta-\lambda+\delta}}\left(\frac{a}{q^{\delta}}\right)q^{-(\lambda-\delta)}\sum_{0\leqslant l<q^{\lambda-\delta}} \varphi_{q^{\lambda-\delta}}\left(\frac{a}{q^{\lambda}}+\frac{l}{q^{\lambda-\delta}}\right)\\ &= q^{-\eta+\lambda-\delta}\varphi_{q^{\eta-\lambda+\delta}}\left(\frac{a}{q^{\delta}}\right)\Psi_{q^{\lambda-\delta}}\left(\frac{a}{q^{\lambda}}\right)|F_{\lambda-\eta}(a,\alpha)|\\ &\ll \log q^{\lambda-\delta} q^{-\eta+\lambda-\delta}\varphi_{q^{\eta-\lambda+\delta}}\left(\frac{a}{q^{\delta}}\right)|F_{\lambda-\eta}(a,\alpha)|\\ &\ll_q \eta q^{-\eta+\lambda-\delta}\varphi_{q^{\eta-\lambda+\delta}}\left(\frac{a}{q^{\delta}}\right)|F_{\lambda-\eta}(a,\alpha)|.\end{aligned}$$

By Lemma 3.1, we have $\varphi_{q^{\eta-\lambda+\delta}}(aq^{-\delta}) \leqslant q^{\eta-\lambda+\delta}$. Thus, (3.20) is a direct consequence of (3.19). ■

We conclude this chapter with presenting two lemmas, which will play a crucial part in Chapter 6.

Lemma 3.17 *Let $a \in \mathbb{Z},\ m \in \mathbb{Z},\ \alpha \in \mathbb{R}$ and $0 \leqslant \delta \leqslant \lambda - \eta$. Then we have*

$$\sum_{\substack{0\leqslant h<q^{\lambda}\\ h\equiv a \bmod q^{\delta}}} |F_{\eta,\lambda}(h,\alpha)F_{\lambda-\eta}(h+m,\alpha)| \ll_q \eta |F_{\delta}(a,\alpha)F_{\delta}(a+m,\alpha)|.$$

Proof. First, we employ the Euclidean algorithm ($h = kq^{\lambda-\eta} + l$, where $0 \leqslant k < q^{\eta}$ and $0 \leqslant l < q^{\lambda-\eta}$). Here we note that $h \equiv a \bmod q^{\delta}$ is equivalent to $l \equiv a \bmod q^{\delta}$, since by assumption $\delta \leqslant \lambda - \eta$. Thus we can write

$$\begin{aligned}\sum_{\substack{0\leqslant h<q^{\lambda}\\ h\equiv a \bmod q^{\delta}}} |F_{\eta,\lambda}(h,\alpha)F_{\lambda-\eta}(h+m,\alpha)| &= \sum_{\substack{0\leqslant l<q^{\lambda-\eta}\\ l\equiv a \bmod q^{\delta}}} \sum_{0\leqslant k<q^{\eta}} |F_{\eta,\lambda}(kq^{\lambda-\eta}+l,\alpha)F_{\lambda-\eta}(kq^{\lambda-\eta}+l+m,\alpha)| \\ &= \sum_{\substack{0\leqslant l<q^{\lambda-\eta}\\ l\equiv a \bmod q^{\delta}}} |F_{\lambda-\eta}(l,\alpha)F_{\lambda-\eta}(l+m,\alpha)|q^{-\eta} \sum_{0\leqslant k<q^{\eta}} \varphi_{q^{\eta}}\left(\frac{kq^{\lambda-\eta}+l}{q^{\lambda}}\right) \\ &= \sum_{\substack{0\leqslant l<q^{\lambda-\eta}\\ l\equiv a \bmod q^{\delta}}} |F_{\lambda-\eta}(l,\alpha)F_{\lambda-\eta}(l+m,\alpha)|\Psi_{q^{\eta}}\left(\frac{l}{q^{\lambda}}\right).\end{aligned}$$

Therefore we get by Lemma 3.7 and the Cauchy Schwarz inequality

$$\begin{aligned}\sum_{\substack{0\leqslant h<q^{\lambda}\\ h\equiv a \bmod q^{\delta}}} |F_{\eta,\lambda}(h,\alpha)F_{\lambda-\eta}(h+m,\alpha)| &\ll \log q^{\eta} \sum_{\substack{0\leqslant l<q^{\lambda-\eta}\\ l\equiv a \bmod q^{\delta}}} |F_{\lambda-\eta}(l,\alpha)F_{\lambda-\eta}(l+m,\alpha)| \\ &\ll_q \eta \left(\sum_{\substack{0\leqslant l<q^{\lambda-\eta}\\ l\equiv a \bmod q^{\delta}}} |F_{\lambda-\eta}(l,\alpha)|^2\right)^{1/2} \left(\sum_{\substack{0\leqslant l<q^{\lambda-\eta}\\ l\equiv a \bmod q^{\delta}}} |F_{\lambda-\eta}(l+m,\alpha)|^2\right)^{1/2} \\ &\ll_q \eta |F_{\delta}(a,\alpha)F_{\delta}(a+m,\alpha)|.\end{aligned}$$

Lemma 3.13 finishes the proof. ∎

Lemma 3.18 *Let $a \in \mathbb{Z}$, $\alpha \in \mathbb{R}$ and $\lambda - \eta \leqslant \delta \leqslant \lambda$. Then we have*

$$\sum_{\substack{0\leqslant h_1,h_2<q^{\lambda}\\ h_1+h_2\equiv a \bmod q^{\delta}}} |F_{\eta,\lambda}(h_1,\alpha)F_{\eta,\lambda}(-h_2,\alpha)| \ll_q \eta^2.$$

Proof. We can write

$$\begin{aligned}\sum_{\substack{0\leqslant h_1,h_2<q^{\lambda}\\ h_1+h_2\equiv a \bmod q^{\delta}}} |F_{\eta,\lambda}(h_1,\alpha)F_{\eta,\lambda}(-h_2,\alpha)| &= \sum_{0\leqslant h_2<q^{\lambda}} |F_{\eta,\lambda}(-h_2,\alpha)| \sum_{\substack{0\leqslant h_1<q^{\lambda}\\ h_1\equiv -h_2+a \bmod q^{\delta}}} |F_{\eta,\lambda}(h_1,\alpha)| \\ &\ll_q \eta \sum_{0\leqslant h_2<q^{\lambda}} |F_{\eta,\lambda}(-h_2,\alpha)F_{\lambda-\eta}(-h_2+a,\alpha)|.\end{aligned}$$

To obtain the last inequality we employed Lemma 3.16. Finally, Lemma 3.17 with $\delta = 0$ yields the desired result. ∎

Chapter 4

The Joint Distribution of the Sum of Digits Function

In this chapter we want to prove Gelfond's conjecture concerning the joint distribution of the sum of digits function. In particular, we show Kim's result in the case where the arbitrary q-additive functions are replaced by sum of digits functions. We follow Kim's proof (see [28]), but obtain a better error term, since we can use some special properties of the sum of digits function.

4.1 Main Results

As in the proof of Gelfond's theorem, the crucial part is an exponential sum estimate.

Theorem 4.1 *Let* $\mathbf{q}$ *be an* l*-tuple of pairwise coprime integers satisfying* $q_j \geqslant 2$*, and* $\alpha_1, \dots, \alpha_l$ *be real numbers such that* $(q_j - 1)\alpha_j \in \mathbb{R} \setminus \mathbb{Z}$ *for at least one index* i*. Then we have for all positive integers* N

$$\sum_{n=0}^{N-1} \mathrm{e}\left(\sum_{j=1}^{l} \alpha_j s_{q_j}(n)\right) = O_{\mathbf{q},l}(N^{1-\lambda}),$$

where $\lambda = \max_{1\leqslant j\leqslant l} \frac{\|(q_j-1)\alpha_j\|^2}{240l^2 \log q_j} > 0$.

The proof, which we are going to show in Section 4.2, is organized as follows. First we use van der Corput's and the Hölder's inequality in order to smooth the sums. In doing so, we obtain expressions of the form $\alpha_j s_{q_j}(n+k) - \alpha_j s_{q_j}(n)$. If $\|(q_j - 1)\alpha_j\| \in \mathbb{R} \setminus \mathbb{Z}$, we show that the sum over n and k of such terms is small (see Proposition 4.1). The main idea thereby is to find upper bounds of some correlation functions (Lemma 4.1 – Lemma 4.5).

Before we start the proof, we present the solution of Gelfond's problem, which is a direct consequence of Kim's result.

Theorem 4.2 (Kim [28]) *Let* $\mathbf{q}$ *and* $\mathbf{m}$ *be* l*-tuples of integers satisfying* $q_j, m_j \geqslant 2$ *for each* j *and* $(q_i, q_j) = 1$ *for* $i \neq j$*. If we set* $d_j = (m_j, q_j - 1)$*, then we have for all positive integers* N *and for any* l*-tuple* $\mathbf{a}$ *of integers*

$$\begin{aligned}\#\{0 \leqslant n < N : s_{q_1}(n) \equiv a_1 \bmod m_1, \dots, s_{q_l}(n) \equiv a_l \bmod m_l\} \\ = \begin{cases} \frac{N}{m_1 \cdots m_l} \frac{d_1 \cdots d_l}{\operatorname{lcm}(d_1,\dots,d_l)} + O_{\mathbf{q},l}(N^{1-\lambda}) & \text{if } a_i \equiv a_j \bmod (d_i, d_j) \text{ for each } i \text{ and } j, \\ 0 & \text{otherwise,} \end{cases}\end{aligned}$$

where $\lambda = 1/(240l^2(\log \bar{q})\bar{m}^2)$ *with* $\bar{q} = \max\{q_j : 1 \leqslant j \leqslant l\}$ *and* $\bar{m} = \max\{m_j : 1 \leqslant j \leqslant l\}$.

Corollary 4.1 *Let* $\mathbf{q}$ *and* $\mathbf{m}$ *be* l*-tuples of integers satisfying* $q_j,\ m_j \geqslant 2$, $(m_j, q_j - 1) = 1$ *for each* j *and* $(q_i, q_j) = 1$ *for* $i \neq j$. *Then we have for all positive integers* N *and for any* l*-tuple* $\mathbf{a}$ *of integers*

$$\#\{0 \leqslant n < N : s_{q_1}(n) \equiv a_1 \bmod m_1, \dots, s_{q_l}(n) \equiv a_l \bmod m_l\} = \frac{N}{m_1 \cdots m_l} + O_{\mathbf{q},l}(N^{1-\lambda}),$$

where $\lambda = 1/(240l^2(\log \overline{q})\overline{m}^2)$ *with* $\overline{q} = \max\{q_j : 1 \leqslant j \leqslant l\}$ *and* $\overline{m} = \max\{m_j : 1 \leqslant j \leqslant l\}$.

Proof (of Theorem 4.2). Let $S(N) = \#\{0 \leqslant n < N : s_{q_1}(n) \equiv a_1 \bmod m_1, \dots, s_{q_l}(n) \equiv a_l \bmod m_l\}$. If there exists a pair of indices i and j such that $a_i \not\equiv a_j \bmod (d_i, d_j)$, then $S(N) = 0$. Indeed, let us assume that there is an integer n with $s_{q_i}(n) \equiv a_i \bmod m_i$ and $s_{q_j}(n) \equiv a_j \bmod m_j$. Lemma 1.1 implies that $s_{q_i}(n) \equiv n \bmod d_i$ and $s_{q_j}(n) \equiv n \bmod d_j$. These congruences are also true modulo (d_i, d_j). Thus, we have

$$a_i \equiv s_{q_i}(n) \equiv n \equiv s_{q_j}(n) \equiv a_j \bmod (d_i, d_j),$$

which proves that $S(N)$ has to be zero.

Let us now assume that $a_i \equiv a_j \bmod (d_i, d_j)$ for all indices i and j. Using Lemma 1.2, we can write

$$S(N) = \sum_{n=0}^{N-1} \prod_{j=1}^{l} \left(\frac{1}{m_j} \sum_{h_j=0}^{m_j-1} \mathrm{e}\left(\frac{h_j}{m_j}(s_{q_j}(n) - a_j) \right) \right).$$

Setting

$$\mathcal{H} = \{\mathbf{h} = (h_1, \dots, h_l) : 0 \leqslant h_j \leqslant m_j - 1 \text{ for each } j\},$$
$$\mathcal{H}_0 = \{\mathbf{h} = (h_1, \dots, h_l) : 0 \leqslant h_j \leqslant m_j - 1 \text{ and } m_j \mid d_j h_j \text{ for each } j\},$$

we get

$$\begin{aligned} S(N) &= \frac{1}{\prod_{j=1}^{l} m_j} \sum_{n=0}^{N-1} \sum_{\mathbf{h} \in \mathcal{H}} \mathrm{e}\left(\sum_{j=1}^{l} \frac{h_j}{m_j}(s_{q_j}(n) - a_j) \right) \\ &= \frac{1}{\prod_{j=1}^{l} m_j} \left(\sum_{n=0}^{N-1} \sum_{\mathbf{h} \in \mathcal{H}_0} \mathrm{e}\left(\sum_{j=1}^{l} \frac{h_j}{m_j}(s_{q_j}(n) - a_j) \right) + \sum_{n=0}^{N-1} \sum_{\mathbf{h} \in \mathcal{H} \setminus \mathcal{H}_0} \mathrm{e}\left(\sum_{j=1}^{l} \frac{h_j}{m_j}(s_{q_j}(n) - a_j) \right) \right). \end{aligned} \tag{4.1}$$

To estimate the first term in (4.1), we have to consider the set $\mathcal{H}_0$ more accurately. Since the condition $m_j \mid h_j d_j$ is equivalent to $(m_j/d_j) \mid h_j$, we can write $\mathcal{H}_0$ in the form

$$\mathcal{H}_0 = \left\{ \mathbf{h} = \left(\frac{m_1}{d_1} h_1', \dots, \frac{m_l}{d_l} h_l' \right) : 0 \leqslant h_j' \leqslant d_j - 1 \text{ for each } j \right\}.$$

Hence, setting $\mathcal{H}' = \{\mathbf{h}' = (h_1', \dots, h_l') : 0 \leqslant h_j' \leqslant d_j - 1 \text{ for each } j\}$, we have

$$\sum_{\mathbf{h} \in \mathcal{H}_0} \mathrm{e}\left(\sum_{j=1}^{l} \frac{h_j}{m_j}(s_{q_j}(n) - a_j) \right) = \sum_{\mathbf{h}' \in \mathcal{H}'} \mathrm{e}\left(\sum_{j=1}^{l} \frac{h_j'}{d_j}(s_{q_j}(n) - a_j) \right).$$

Since, by Lemma 1.1, $s_{q_j}(n) \equiv n \bmod d_j$, we can replace $s_{q_j}(n)$ by n in the last sum. We obtain

$$\begin{aligned}\sum_{n=0}^{N-1}\sum_{\mathbf{h}\in\mathcal{H}_0}\mathrm{e}\left(\sum_{j=1}^{l}\frac{h_j}{m_j}(s_{q_j}(n)-a_j)\right) &= \sum_{n=0}^{N-1}\sum_{\mathbf{h}'\in\mathcal{H}'}\mathrm{e}\left(\sum_{j=1}^{l}\frac{h'_j}{d_j}(n-a_j)\right) = \sum_{n=0}^{N-1}\prod_{j=1}^{l}\left(\sum_{h'_j=0}^{d_j-1}\mathrm{e}\left(\frac{h'_j}{d_j}(n-a_j)\right)\right)\\ &= \left(\prod_{j=1}^{l}d_j\right)\sum_{n=0}^{N-1}\prod_{j=1}^{l}\left(\frac{1}{d_j}\sum_{h'_j=0}^{d_j-1}\mathrm{e}\left(\frac{h'_j}{d_j}(n-a_j)\right)\right)\\ &= \left(\prod_{j=1}^{l}d_j\right)\#\{0\leqslant n<N : n\equiv a_j \bmod d_j \text{ for each } j\}.\end{aligned}$$

The last equality is a consequence of Lemma 1.2. By our assumption ($a_i \equiv a_j \bmod (d_i, d_j)$) and the Chinese remainder theorem (Theorem A.4), we obtain

$$\begin{aligned}\frac{1}{\prod_{j=1}^{l}m_j}\sum_{n=0}^{N-1}\sum_{\mathbf{h}\in\mathcal{H}_0}\mathrm{e}\left(\sum_{j=1}^{l}\frac{h_j}{m_j}(s_{q_j}(n)-a_j)\right) &= \left(\prod_{j=1}^{l}\frac{d_j}{m_j}\right)\left(\frac{N}{\operatorname{lcm}(d_1,\dots,d_l)}+O(1)\right)\\ &= \frac{N}{m_1\cdots m_l}\frac{d_1\cdots d_l}{\operatorname{lcm}(d_1,\dots,d_l)}+O(1).\end{aligned}$$

If we can show that the second term in (4.1) is $O(N^{1-\lambda})$, we are done. The condition $\mathbf{h}\in\mathcal{H}\setminus\mathcal{H}_0$ implies that there exists an index j, such that $m_j \nmid d_j h_j$. This condition is equivalent to $h_j(q_j-1)/m_j \in \mathbb{R}\setminus\mathbb{Z}$ and we can employ Theorem 4.1 with $\alpha_j = h_j/m_j$. Setting $\overline{q} = \max\{q_j : 1\leqslant j\leqslant l\}$ and $\overline{m} = \max\{m_j : 1\leqslant j\leqslant l\}$, we have $\|h_j(q_j-1)/m_j\| \geqslant 1/\overline{m}$ and $\log q_j \leqslant \log\overline{q}$. Thus, we have

$$\sum_{n=0}^{N-1}\mathrm{e}\left(\sum_{j=1}^{l}\frac{h_j}{m_j}s_{q_j}(n)\right) = O_{\mathbf{q},l}(N^{1-\lambda}),$$

with $\lambda = 1/(240l^2(\log\overline{q})\overline{m}^2)$. Hence, we get the desired estimation

$$\begin{aligned}\frac{1}{\prod_{j=1}^{l}m_j}\sum_{n=0}^{N-1}\sum_{\mathbf{h}\in\mathcal{H}\setminus\mathcal{H}_0}\mathrm{e}\left(\sum_{j=1}^{l}\frac{h_j}{m_j}(s_{q_j}(n)-a_j)\right) &= \frac{1}{\prod_{j=1}^{l}m_j}\sum_{\mathbf{h}\in\mathcal{H}\setminus\mathcal{H}_0}\mathrm{e}\left(-\sum_{j=1}^{l}\frac{h_j}{m_j}a_j\right)\sum_{n=0}^{N-1}\mathrm{e}\left(\sum_{j=1}^{l}\frac{h_j}{m_j}s_{q_j}(n)\right)\\ &= O_{\mathbf{q},l}(N^{1-\lambda}),\end{aligned}$$

and the proof is finished. ∎

4.2 Proof of Theorem 4.1

The main part of the proof of Theorem 4.1 is the the following correlation estimate, which is a quantitative and more general version of a result of Bésineau [3].

Proposition 4.1 *Let q, N and K be positive integers satisfying $q\geqslant 2$ and $\sqrt{N}\leqslant K\leqslant N$. Furthermore, let $\alpha\in\mathbb{R}$ with $\|(q-1)\alpha\|\notin\mathbb{Z}$. Then we have for all positive integers N*

$$\frac{1}{K}\sum_{k=1}^{K}\left|\frac{1}{N}\sum_{n=0}^{N-1}\mathrm{e}\left(\alpha s_q(n+k)-\alpha s_q(n)\right)\right|^2 = O(N^{-\delta}),$$

where $\delta = \|(q-1)\alpha\|^2/(20\log q)$.

Throughout this section, we suppose that $q \geqslant 2$, N and K are integers and $\alpha \in \mathbb{R}$. For brevity, we write $f(n) = \alpha s_q(n)$ where we can assume that $\alpha \in \mathbb{R} \setminus \mathbb{Z}$. The main point of the proof of this proposition is the accurate study of the correlation functions

$$\Phi_N(k) = \frac{1}{N}\sum_{n=0}^{N} \mathrm{e}\left(f(n+k) - f(n)\right),$$
$$\Phi_{K,N}(r) = \frac{1}{K}\sum_{n=0}^{N} \overline{\Phi_N(k)}\,\Phi_N(k+r).$$

Lemma 4.1 *Let $k \geqslant 0$ and $0 \leqslant r \leqslant q$ be integers. Then we have*

$$\Phi_{qN}(qk+r) = \mathrm{e}(r\alpha)\frac{q-r}{q}\,\Phi_N(k) + \mathrm{e}((r-q)\alpha)\frac{r}{q}\,\Phi_N(k+1).$$

Proof. First we can assume that $0 \leqslant r \leqslant q-1$ (if the equation holds for $r = 0$, it also holds trivially for $r = q$). Using the Euclidean algorithm and the fact that s_q is completely q-additive, we have

$$\begin{aligned}
qN\Phi_{qN}(qk+r) &= \sum_{j=0}^{q-1}\sum_{n=0}^{N-1} \mathrm{e}\left(f(qn+j+qk+r) - f(qn+j)\right)\\
&= \sum_{j=0}^{q-r-1}\sum_{n=0}^{N-1} \mathrm{e}(f(n+k) + f(j+r) - f(n) - f(j))\\
&\qquad + \sum_{j=q-r}^{q-1}\sum_{n=0}^{N-1} \mathrm{e}(f(n+k+1) + f(j+r-q) - f(n) - f(j))\\
&= \sum_{j=0}^{q-r-1} \mathrm{e}(f(j+r) - f(j)) \sum_{n=0}^{N-1} \mathrm{e}(f(n+k) - f(n))\\
&\qquad + \sum_{j=q-r}^{q-1} \mathrm{e}(f(j+r-q) - f(j)) \sum_{n=0}^{N-1} \mathrm{e}(f(n+k+1) - f(n)).
\end{aligned}$$

Since $s_q(n) = n$ for $0 \leqslant n < q$, we get

$$\frac{1}{q}\sum_{j=0}^{q-r-1} \mathrm{e}(f(j+r) - f(j)) = \frac{1}{q}\sum_{j=0}^{q-r-1} \mathrm{e}(r\alpha) = \mathrm{e}(r\alpha)\frac{q-r}{q},$$

and

$$\frac{1}{q}\sum_{j=q-r}^{q-1} \mathrm{e}(f(j+r-q) - f(j)) = \frac{1}{q}\sum_{j=q-r}^{q-1} \mathrm{e}((r-q)\alpha) = \mathrm{e}((r-q)\alpha)\frac{r}{q}.$$

Hence, we finally obtain

$$\Phi_{qN}(qk+r) = \mathrm{e}(r\alpha)\frac{q-r}{q}\,\Phi_N(k) + \mathrm{e}((r-q)\alpha)\frac{r}{q}\,\Phi_N(k+1).$$

■

Lemma 4.2 *Let $r = 0$ or $r = 1$. Then we have*

$$\Phi_{qK,qN}(r) = \mathrm{e}(r\alpha)\lambda_r\,\Phi_{K,N}(0) + \mathrm{e}((r-q)\alpha)\mu_r\,\Phi_{K,N}(1) + \mathrm{e}((r+q)\alpha)\nu_r\,\overline{\Phi_{K,N}(1)} + O(1/K),$$

where $\lambda_r = \frac{2q^2-3r+1}{3q^2}$, $\mu_r = \frac{q^2+3qr+3r-1}{6q^2}$ *and* $\nu_r = \frac{q^2-3qr+3r-1}{6q^2}$.

Proof. Using the Euclidean algorithm and applying Lemma 4.1 yields

$$\begin{aligned}
qK\Phi_{qK,qN}(r) &= \sum_{j=0}^{q-1}\sum_{k=0}^{K-1}\overline{\Phi_{qN}(qk+j)}\,\Phi_{qN}(qk+j+r)\\
&= \sum_{j=0}^{q-1}\sum_{k=0}^{K-1}\overline{\left(\mathrm{e}(j\alpha)\frac{q-j}{q}\,\Phi_N(k) + \mathrm{e}((j-q)\alpha)\frac{j}{q}\,\Phi_N(k+1)\right)}\\
&\qquad\cdot\left(\mathrm{e}((j+r)\alpha)\frac{q-j-r}{q}\,\Phi_N(k) + \mathrm{e}((j+r-q)\alpha)\frac{j+r}{q}\,\Phi_N(k+1)\right).
\end{aligned}$$

Thus, we have

$$\begin{aligned}
qK\Phi_{qK,qN}(r) &= \mathrm{e}(r\alpha)\sum_{j=0}^{q-1}\left(\frac{q-j}{q}\frac{q-j-r}{q} + \frac{j}{q}\frac{j+r}{q}\right)\sum_{k=0}^{K-1}\overline{\Phi_N(k)}\,\Phi_N(k)\\
&\quad + \mathrm{e}((r-q)\alpha)\sum_{j=0}^{q-1}\frac{q-j}{q}\frac{j+r}{q}\sum_{k=0}^{K-1}\overline{\Phi_N(k)}\,\Phi_N(k+1)\\
&\quad + \mathrm{e}((r+q)\alpha)\sum_{j=0}^{q-1}\frac{j}{q}\frac{q-j-r}{q}\sum_{k=0}^{K-1}\overline{\Phi_N(k+1)}\,\Phi_N(k)\\
&\quad + \mathrm{e}(r\alpha)\sum_{j=0}^{q-1}\frac{j}{q}\frac{j+r}{q}\sum_{k=0}^{K-1}\left(\overline{\Phi_N(k+1)}\,\Phi_N(k+1) - \overline{\Phi_N(k)}\,\Phi_N(k)\right).
\end{aligned}$$

Calculating the sums over j yields

$$\begin{aligned}
qK\Phi_{qK,qN}(r) &= \mathrm{e}(r\alpha)\frac{2q^3-3rq+q}{3q^2}\sum_{k=0}^{K-1}\overline{\Phi_N(k)}\,\Phi_N(k)\\
&\quad + \mathrm{e}((r-q)\alpha)\frac{q^3+3rq^2+3rq-q}{6q^2}\sum_{k=0}^{K-1}\overline{\Phi_N(k)}\,\Phi_N(k+1)\\
&\quad + \mathrm{e}((r+q)\alpha)\frac{q^3-3rq^2+3rq-q}{6q^2}\sum_{k=0}^{K-1}\overline{\Phi_N(k+1)}\,\Phi_N(k)\\
&\quad + \mathrm{e}(r\alpha)\frac{2q^3-3q^2+3rq^2+q-3rq}{6q^2}\sum_{k=0}^{K-1}\left(\overline{\Phi_N(k+1)}\,\Phi_N(k+1) - \overline{\Phi_N(k)}\,\Phi_N(k)\right).
\end{aligned}$$

Since the last sum over k is a telescoping series and $|\Phi_N(.)| \leqslant 1$, the last term is $\ll q$ and we obtain

$$\Phi_{qK,qN}(r) = \mathrm{e}(r\alpha)\lambda_r\Phi_{K,N}(0) + \mathrm{e}((r-q)\alpha)\mu_r\Phi_{K,N}(1) + \mathrm{e}((r+q)\alpha)\nu_r\overline{\Phi_{K,N}(1)} + O(1/K).$$

■

The next step is to bound $\Phi_{q^{2i}K,\,q^{2i}N}(r)$ for $i = 1$. Matrix calculations will provide us an upper bound for arbitrary positive integers i.

Lemma 4.3 *Let $r = 0$ or $r = 1$. Then we have*

$$|\Phi_{q^2K,\,q^2N}(r)| \leqslant \rho_r|\Phi_{K,\,N}(0)| + \sigma_r|\Phi_{K,\,N}(1)| + O(1/K),$$

where ρ_r and σ_r are non-negative integers satisfying $\rho_r + \sigma_r \leqslant 1 - \frac{\|(q-1)\alpha\|^2}{4}$.

Proof. By Lemma 4.2, we have

$$\begin{aligned}
&\Phi_{q^2K,\,q^2N}(r)\\
&\quad = \mathrm{e}(r\alpha)\lambda_r\Phi_{qK,\,qN}(0) + \mathrm{e}((r-q)\alpha)\mu_r\Phi_{qK,\,qN}(1) + \mathrm{e}((r+q)\alpha)\nu_r\overline{\Phi_{qK,\,qN}(1)} + O(1/K)\\
&\quad = \mathrm{e}(r\alpha)\lambda_r\left(\lambda_0\Phi_{K,\,N}(0) + \mathrm{e}(-q\alpha)\mu_0\Phi_{K,\,N}(1) + \mathrm{e}(q\alpha)\nu_0\overline{\Phi_{K,\,N}(1)} + O(1/K)\right) + O(1/K)\\
&\qquad + \mathrm{e}((r-q)\alpha)\mu_r\left(\mathrm{e}(\alpha)\lambda_1\Phi_{K,\,N}(0) + \mathrm{e}((1-q)\alpha)\mu_1\Phi_{K,\,N}(1) + \mathrm{e}((1+q)\alpha)\nu_1\overline{\Phi_{K,\,N}(1)} + O(1/K)\right)\\
&\qquad + \mathrm{e}((r+q)\alpha)\nu_r\overline{\left(\mathrm{e}(\alpha)\lambda_1\Phi_{K,\,N}(0) + \mathrm{e}((1-q)\alpha)\mu_1\Phi_{K,\,N}(1) + \mathrm{e}((1+q)\alpha)\nu_1\overline{\Phi_{K,\,N}(1)} + O(1/K)\right)}.
\end{aligned}$$

If we set

$$\begin{aligned}
\rho_r &= |\lambda_r\lambda_0 + \mathrm{e}(-(q-1)\alpha)\mu_r\lambda_1 + \mathrm{e}((q-1)\alpha)\nu_r\lambda_1|,\\
\sigma_r &= |\lambda_r\mu_0 + \mathrm{e}(-(q-1)\alpha)\mu_r\mu_1 + \mathrm{e}((q-1)\alpha)\nu_r\nu_1| + |\lambda_r\nu_0 + \mathrm{e}(-(q-1)\alpha)\mu_r\nu_1 + \mathrm{e}((q-1)\alpha)\nu_r\mu_1|,
\end{aligned}$$

we obtain (note that $0 \leqslant \lambda_r, \mu_r, \nu_r \leqslant 1$)

$$|\Phi_{q^2K,\,q^2N}(r)| \leqslant \rho_r|\Phi_{K,\,N}(0)| + \sigma_r|\Phi_{K,\,N}(1)| + O(1/K).$$

To finish the proof of this lemma, we have to check the additional property of $\rho_r + \sigma_r$. In order to be able to do this, we need the following elementary result. For any real numbers $a \geqslant b > 0$ and θ, we have

$$|a + b\mathrm{e}(\theta)| \leqslant a + b - 4b\|\theta\|^2.$$

This follows immediately from

$$\begin{aligned}
4a(a + b - |a + b\mathrm{e}(\theta)|) &\geqslant (a + b + |a + b\mathrm{e}(\theta)|)(a + b - |a + b\mathrm{e}(\theta)|)\\
&= (a+b)^2 - |a + b\mathrm{e}(\theta)|^2 = 2ab(1 - \cos(2\pi\theta))\\
&= 2ab(1 - \cos(2\pi\|\theta\|)) = 4ab(\sin\pi\|\theta\|)^2\\
&\geqslant 4ab\left(\frac{2}{\pi}\right)^2\pi^2\|\theta\|^2 = 16ab\|\theta\|^2.
\end{aligned}$$

Now we are able to prove the inequality $\rho_r + \sigma_r \leqslant 1 - \|(q-1)\alpha\|^2/4$. First, one can readily check that $\lambda_r + \mu_r + \nu_r = 1$. Furthermore, we have $\lambda_0 \geqslant \lambda_1 \geqslant 1/2$, $\mu_1 \geqslant \mu_0 \geqslant 1/8$ and $\lambda_r \geqslant \mu_r$ (note that $q \geqslant 2$). This implies $\lambda_r\lambda_0 \geqslant \mu_r\lambda_1$ and we are allowed to use the just obtained result. We have

$$\begin{aligned}
\rho_r &\leqslant |\lambda_r\lambda_0 + \mathrm{e}((1-q)\alpha)\mu_r\lambda_1| + \nu_r\lambda_1\\
&\leqslant \lambda_r\lambda_0 + \mu_r\lambda_1 - 4\mu_r\lambda_1\|(q-1)\alpha\|^2 + \nu_r\lambda_1.
\end{aligned}$$

Since $\mu_r\lambda_1 \geqslant 1/16$, we obtain

$$\rho_r \leqslant \lambda_r\lambda_0 + \mu_r\lambda_1 + \nu_r\lambda_1 - \frac{\|(q-1)\alpha\|^2}{4}.$$

The constant σ_r is trivially bounded by $\lambda_r\mu_0 + \mu_r\mu_1 + \nu_r\nu_1 + \lambda_r\nu_0 + \mu_r\nu_1 + \nu_r\mu_1$. Hence we finally get

$$\begin{aligned}\rho_r + \sigma_r &\leqslant \lambda_r(\lambda_0 + \mu_0 + \nu_0) + (\mu_r + \nu_r)(\lambda_1 + \mu_1 + \nu_1) - \frac{\|(q-1)\alpha\|^2}{4} \\ &= 1 - \frac{\|(q-1)\alpha\|^2}{4}.\end{aligned}$$

■

Lemma 4.4 *Let a, b, c and d be non-negative real numbers satisfying $a + b \leqslant 1 - \varepsilon$ and $c + d \leqslant 1 - \varepsilon$ for some $\varepsilon > 0$. Let*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^i = \begin{pmatrix} A_i & B_i \\ C_i & D_i \end{pmatrix} \quad (i \geqslant 1). \tag{4.2}$$

Then we have $A_i + B_i \leqslant (1-\varepsilon)^i$ and $C_i + D_i \leqslant (1-\varepsilon)^i$ for all positive integers i.

Proof. We prove this lemma by induction on i. When $i = 1$, the claim holds by assumption. Suppose now, that the result holds for all integers $i \geqslant 1$. Since

$$\begin{pmatrix} A_{i+1} & B_{i+1} \\ C_{i+1} & D_{i+1} \end{pmatrix} = \begin{pmatrix} A_i & B_i \\ C_i & D_i \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

we have

$$\begin{aligned}A_{i+1} + B_{i+1} &= (a+b)A_i + (c+d)B_i \leqslant (1-\varepsilon)(A_i + B_i) \leqslant (1-\varepsilon)^{i+1}, \\ C_{i+1} + D_{i+1} &= (a+b)C_i + (c+d)D_i \leqslant (1-\varepsilon)(C_i + D_i) \leqslant (1-\varepsilon)^{i+1},\end{aligned}$$

and the desired result is proved. ■

Lemma 4.5 *For $r = 0, 1$ and any positive integer i we have*

$$\Phi_{q^{2i}K,\, q^{2i}N}(r) = O\left(e^{-\tau i}\right),$$

where $\tau = \frac{\|(q-1)\alpha\|^2}{4}$.

Proof. Let

$$M = \begin{pmatrix} \rho_0 & \sigma_0 \\ \rho_1 & \sigma_1 \end{pmatrix}, \qquad M^i = \begin{pmatrix} A_i & B_i \\ C_i & D_i \end{pmatrix} \qquad (i \geqslant 1),$$

where ρ_r and σ_r are defined in Lemma 4.3 ($r = 0, 1$). We have by the same lemma $\rho_r + \sigma_r \leqslant 1 - \tau$ with $\tau = \|(q-1)\alpha\|^2/4$. Setting $P_i = |\Phi_{q^{2i}K,\, q^{2i}N}(0)|$ and $Q_i = |\Phi_{q^{2i}K,\, q^{2i}N}(1)|$ and applying Lemma 4.4 with $q^{2i-2}K$ and $q^{2i-2}N$ in place of K and N, we obtain for $i \geqslant 1$

$$\begin{pmatrix} P_i \\ Q_i \end{pmatrix} \leqslant M\begin{pmatrix} P_{i-1} \\ Q_{i-1} \end{pmatrix} + O\left(\frac{1}{q^{2i-2}K}\right)\begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

where the inequality is to be interpreted componentwise. Iterating this estimate i times, we get

$$\begin{pmatrix} P_i \\ Q_i \end{pmatrix} \leqslant M^i\begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} + \sum_{j=1}^{i} O\left(\frac{1}{q^{2(j-1)}K}\right) M^{i-j}\begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Since $P_0 \leqslant 1$ and $Q_0 \leqslant 1$, we have by Lemma 4.4

$$M^i \begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} \leqslant \begin{pmatrix} e^{-\tau i} \\ e^{-\tau i} \end{pmatrix} \qquad \text{and} \qquad M^{i-j} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \leqslant \begin{pmatrix} e^{-\tau(i-j)} \\ e^{-\tau(i-j)} \end{pmatrix}.$$

The inequality $e^\tau/q^2 \leqslant 1/2$ (note that $q \geqslant 2$ and $\tau \leqslant 1/16$) implies

$$\sum_{i=1}^{j} \frac{e^{-\tau(i-j)}}{q^{2(j-1)}K} = e^{-\tau i}\frac{e^\tau}{K} \sum_{j=0}^{i-1} \left(\frac{e^\tau}{q^2}\right)^i \ll e^{-\tau i},$$

and we finally obtain $\Phi_{q^{2i}K,\, q^{2i}N}(0) \ll e^{-\tau i}$ and $\Phi_{q^{2i}K,\, q^{2i}N}(1) \ll e^{-\tau i}$. ∎

Proof (of Proposition 4.1). By assumption we have $\sqrt{N} \leqslant K \leqslant N$. Furthermore, we can assume that $N \geqslant q^{45}$. If we set

$$t = \left\lfloor \frac{2\log N}{9\log q} \right\rfloor, \tag{4.3}$$

then $t \geqslant 1$ and $q^{2t} \leqslant \sqrt{N}$. Hence there exist integers $M \geqslant 1$, $L \geqslant 1$ and $0 \leqslant R,\, S < q^{2t}$, such that

$$N = q^{2t}M + R \qquad \text{and} \qquad K = q^{2t}L + S.$$

Next we want to show that

$$\overline{\Phi_N(k)}\,\Phi_N(k) = \overline{\Phi_{q^{2t}M}(k)}\,\Phi_{q^{2t}M}(k) + O\left(\frac{q^{2t}}{N}\right).$$

We can write

$$|\overline{\Phi_N(k)}\,\Phi_N(k) - \overline{\Phi_{q^{2t}M}(k)}\,\Phi_{q^{2t}M}(k)| \leqslant |\overline{\Phi_N(k)} + \overline{\Phi_{q^{2t}M}(k)}| \cdot |\Phi_N(k) - \Phi_{q^{2t}M}(k)| + 2|\operatorname{Im} \overline{\Phi_N(k)}\,\Phi_{q^{2t}M}(k)|.$$

The right hand side of the last inequality is $\ll q^{2t}/N$ since

$$\begin{aligned} |\Phi_N(k) - \Phi_{q^{2t}M}(k)| &= \left| \frac{1}{N}\sum_{n=0}^{N-1} \mathrm{e}(f(n+k) - f(n)) - \frac{1}{q^{2t}M} \sum_{n=0}^{q^{2t}M-1} \mathrm{e}(f(n+k) - f(n)) \right| \\ &= \left| \left(\frac{1}{N} - \frac{1}{q^{2t}M}\right) \sum_{n=0}^{q^{2t}M-1} \mathrm{e}(f(n+k) - f(n)) + \frac{1}{N} \sum_{n=q^{2t}M}^{N-1} \mathrm{e}(f(n+k) - f(n)) \right| \\ &\leqslant \left| \frac{1}{N} - \frac{1}{q^{2t}M} \right| q^{2t}M + \frac{N - q^{2t}M}{N} \leqslant \frac{2q^{2t}}{N}, \end{aligned} \tag{4.4}$$

and

$$\begin{aligned} |\operatorname{Im} \overline{\Phi_N(k)}\,\Phi_{q^{2t}M}(k)| &= \left| \operatorname{Im} \frac{1}{Nq^{2t}M} \sum_{n=0}^{N-1} \sum_{m=0}^{q^{2t}M-1} \mathrm{e}(f(n) - f(n+k) + f(m+k) - f(m)) \right| \\ &= \left| \operatorname{Im} \frac{1}{Nq^{2t}M} \sum_{n=q^{2t}M}^{N-1} \sum_{m=0}^{q^{2t}M-1} \mathrm{e}(f(n) - f(n+k) + f(m+k) - f(m)) \right| \\ &\leqslant \frac{1}{Nq^{2t}M}\, q^{2t}M(N - q^{2t}M) \leqslant \frac{q^{2t}}{N}. \end{aligned}$$

Hence, we obtain

$$\begin{aligned}\Phi_{K,N}(0) &= \frac{1}{K}\sum_{k=0}^{K-1}\overline{\Phi_N(k)}\,\Phi_N(k)\\ &= \frac{1}{K}\sum_{k=0}^{K-1}\overline{\Phi_{q^{2t}M}(k)}\,\Phi_{q^{2t}M}(k) + O\left(\frac{q^{2t}}{N}\right).\end{aligned}$$

The same calculations as in (4.4) show that

$$\left|\frac{1}{K}\sum_{k=0}^{K-1}\overline{\Phi_{q^{2t}M}(k)}\,\Phi_{q^{2t}M}(k) - \frac{1}{q^{2t}L}\sum_{k=0}^{q^{2t}L-1}\overline{\Phi_{q^{2t}M}(k)}\,\Phi_{q^{2t}M}(k)\right| \leqslant \frac{2q^{2t}}{K},$$

which implies

$$\frac{1}{K}\sum_{k=0}^{K-1}\overline{\Phi_{q^{2t}M}(k)}\,\Phi_{q^{2t}M}(k) = \frac{1}{q^{2t}L}\sum_{k=0}^{q^{2t}L-1}\overline{\Phi_{q^{2t}M}(k)}\,\Phi_{q^{2t}M}(k) + O\left(\frac{q^{2t}}{K}\right).$$

Combining these results and using the fact that $\sqrt{N} \leqslant K \leqslant N$, we obtain

$$\Phi_{K,N}(0) = \Phi_{q^{2t}L,\,q^{2t}M}(0) + O\left(\frac{q^{2t}}{\sqrt{N}}\right).$$

By Lemma 4.5 we have $\Phi_{q^{2t}L,\,q^{2t}M}(0) = O(e^{-\tau t})$, where $\tau = \|(q-1)\alpha\|^2/4$. Since $N \geqslant q^{45}$ and $t = \lfloor 2\log N/(9\log q)\rfloor$ (see (4.3)), we have

$$\frac{\log N}{5\log q} \leqslant \frac{2\log N}{9\log q} - 1 \leqslant t \leqslant \frac{2\log N}{9\log q},$$

which implies

$$e^{-\tau t} \leqslant e^{-\tau\frac{\log N}{5\log q}} = N^{-\frac{\tau}{5\log q}} = N^{-\frac{\|(q-1)\alpha\|^2}{20\log q}}$$

and

$$\frac{q^{2t}}{N} \leqslant \frac{N^{4/9}}{N^{1/2}} = N^{-1/18}.$$

Since $\|(q-1)\alpha\|^2/(20\log q) \leqslant 1/18$, we finally obtain

$$\Phi_{K,N}(0) = \frac{1}{K}\sum_{k=1}^{K}\left|\sum_{n=0}^{N-1}\mathrm{e}\left(\alpha s_q(n+k) - \alpha s_q(n)\right)\right|^2 = O(N^{-\delta}),$$

where $\delta = \|(q-1)\alpha\|^2/(20\log q)$. ∎

Proof (of Theorem 4.1). For brevity, we write $g(n) = \mathrm{e}\left(\sum_{j=0}^{l}\alpha_j s_{q_j}(n)\right)$. Furthermore, we set

$$S = \sum_{n=0}^{N-1}\mathrm{e}\left(\sum_{j=1}^{l}\alpha_j s_{q_j}(n)\right) = \sum_{n=0}^{N-1} g(n).$$

First, we use the van der Corput inequality in order to smooth the considered sum. In particular, we employ Lemma 2.7 with $k = 1$ and $R = K := \lfloor N^{1/(3l)} \rfloor$. We can write

$$|S|^2 \leqslant \frac{N+K}{K} \sum_{|k|<K} \left(1 - \frac{|k|}{K}\right) \sum_{\substack{0 \leqslant n < N \\ 0 \leqslant n+k < N}} \overline{g(n)}\, g(n+k).$$

Separating the case $k = 0$ and using the fact that $K \leqslant N$ and $(1 - |k|/K) \leqslant 1$, we get

$$|S|^2 \leqslant \frac{2N^2}{K} + \frac{2N}{K} \sum_{1 \leqslant k < K} \left| \sum_{0 \leqslant n < N-k} \overline{g(n)}\, g(n+k) \right| + \frac{2N}{K} \sum_{1 \leqslant k < K} \left| \sum_{k \leqslant n < N} \overline{g(n)}\, g(n-k) \right|.$$

If we changing the variable in the last term ($m = n - k$), we obtain

$$|S|^2 \leqslant \frac{2N^2}{K} + \frac{4N}{K} \sum_{1 \leqslant k \leqslant K} \left| \sum_{0 \leqslant n < N-k} \overline{g(n)}\, g(n+k) \right|. \tag{4.5}$$

Let us assume that $N \geqslant \max(q_1^{3l}, \dots, q_l^{3l}) \geqslant 2^{3l}$. If we set $t_j = \lfloor 2 \log K / \log q_j \rfloor$ and $Q_j = q_j^{t_j}$, then we have

$$q_j \leqslant K \leqslant K^2 q_j^{-1} \leqslant Q_j \leqslant K^2. \tag{4.6}$$

Let $\mathbf{r} = (r_1, r_2, \dots, r_l)$ be an l-tuple of integers. We define

$$P_{\mathbf{r}} = \{n \in \mathbb{Z} : n \equiv r_1 \bmod Q_1,\ n \equiv r_2 \bmod Q_2, \dots, n \equiv r_l \bmod Q_l\}.$$

Note, that by assumption the integers p_j are coprime and therefore the integers Q_j too. The Chinese remainder theorem (see Theorem A.4) implies, that the system of congruences $n \equiv r_1 \bmod Q_1, \dots, n \equiv r_l \bmod Q_l$ is equivalent to a single congruence modulo $\prod_{j=1}^{l} Q_j$. Hence, we have

$$\#\{0 \leqslant n < N : n \in P_{\mathbf{r}}\} = \frac{N}{\prod_{j=1}^{l} Q_j} + O(1). \tag{4.7}$$

Next we define

$$\mathcal{R} = \{\mathbf{r} = (r_1, r_2, \dots, r_l) : 0 \leqslant r_j \leqslant Q_j - 1 \text{ for } 1 \leqslant j \leqslant l\},$$
$$\mathcal{R}_0 = \{\mathbf{r} = (r_1, r_2, \dots, r_l) : 0 \leqslant r_j \leqslant Q_j - K - 1 \text{ for } 1 \leqslant j \leqslant l\}.$$

If $n \in P_{\mathbf{r}}$ with $\mathbf{r} \in \mathcal{R}_0$, we have by definition $n \equiv r_j \bmod q_j^{t_j}$ and $0 \leqslant r_j + k < q_j^{t_j}$ for $1 \leqslant k \leqslant K$ and $1 \leqslant j \leqslant l$. This implies (where u_j are appropriate integers, such that $n = r_j + u_j q_j^{t_j}$)

$$\begin{aligned}
\overline{g(n)}\, g(n+k) &= \mathrm{e}\left(\sum_{j=0}^{l} \alpha_j \left(s_{q_j}(n+k) - s_{q_j}(n)\right)\right) \\
&= \mathrm{e}\left(\sum_{j=0}^{l} \alpha_j \left(s_{q_j}(r_j + u_j q_j^{t_j} + k) - s_{q_j}(r_j + u_j q_j^{t_j})\right)\right) \\
&= \mathrm{e}\left(\sum_{j=0}^{l} \alpha_j \left(s_{q_j}(r_j + k) - s_{q_j}(r_j)\right)\right) = \prod_{j=1}^{l} \mathrm{e}\left(\alpha_j \left(s_{q_j}(r_j + k) - s_{q_j}(r_j)\right)\right),
\end{aligned}$$

where we used the q-additivity of the sum of digits funciton. Hence, splitting the inner sum in (4.5) according to the residue class of n modulo $(Q_1, \dots, Q_l)$ yields

$$\begin{aligned}
\sum_{0\leqslant n<N-k} \overline{g(n)}\, g(n+k) &= \sum_{\mathbf{r}\in\mathcal{R}} \sum_{\substack{0\leqslant n<N-k\\ n\in P_{\mathbf{r}}}} \overline{g(n)}\, g(n+k)\\
&= \sum_{\mathbf{r}\in\mathcal{R}} \sum_{\substack{0\leqslant n<N-k\\ n\in P_{\mathbf{r}}}} \left(\overline{g(n)}\, g(n+k) - \prod_{j=1}^{l} \mathrm{e}\left(\alpha_j \left(s_{q_j}(r_j+k) - s_{q_j}(r_j)\right)\right)\right)\\
&\qquad + \sum_{\mathbf{r}\in\mathcal{R}} \sum_{\substack{0\leqslant n<N-k\\ n\in P_{\mathbf{r}}}} \prod_{j=1}^{l} \mathrm{e}\left(\alpha_j \left(s_{q_j}(r_j+k) - s_{q_j}(r_j)\right)\right)\\
&= \sum_{\mathbf{r}\in\mathcal{R}\setminus\mathcal{R}_0} \sum_{\substack{0\leqslant n<N-k\\ n\in P_{\mathbf{r}}}} \left(\overline{g(n)}\, g(n+k) - \prod_{j=1}^{l} \mathrm{e}\left(\alpha_j \left(s_{q_j}(r_j+k) - s_{q_j}(r_j)\right)\right)\right)\\
&\qquad + \sum_{\mathbf{r}\in\mathcal{R}} \prod_{j=1}^{l} \mathrm{e}\left(\alpha_j \left(s_{q_j}(r_j+k) - s_{q_j}(r_j)\right)\right) \sum_{\substack{0\leqslant n<N-k\\ n\in P_{\mathbf{r}}}} 1.
\end{aligned}$$

In order to be able to bound this sum, we use the fact that $|g(n)| \leqslant 1$ and employ (4.7). Thus, we can write

$$\begin{aligned}
&\sum_{0\leqslant n<N-k} \overline{g(n)}\, g(n+k)\\
&\qquad \leqslant 2 \sum_{\mathbf{r}\in\mathcal{R}\setminus\mathcal{R}_0} \sum_{\substack{0\leqslant n<N-k\\ n\in P_{\mathbf{r}}}} 1 + \prod_{j=1}^{l} \sum_{r_j=0}^{Q_j-1} \mathrm{e}\left(\alpha_j \left(s_{q_j}(r_j+k) - s_{q_j}(r_j)\right)\right) \left(\frac{N}{\prod_{j=1}^{l} Q_j} + O(1)\right)\\
&\qquad \leqslant 2 \sum_{\mathbf{r}\in\mathcal{R}\setminus\mathcal{R}_0} \left(\frac{N}{\prod_{j=1}^{l} Q_j} + O(1)\right) + N \prod_{j=1}^{l} \frac{1}{Q_j} \sum_{r_j=0}^{Q_j-1} \mathrm{e}\left(\alpha_j \left(s_{q_j}(r_j+k) - s_{q_j}(r_j)\right)\right) + O\left(\prod_{j=1}^{l} Q_j\right).
\end{aligned}$$

Using (4.6), we have

$$\begin{aligned}
|\mathcal{R}\setminus\mathcal{R}_0| &\leqslant \sum_{j=1}^{l} \#\{\mathbf{r} : 0\leqslant r_i \leqslant Q_i - 1 (i\neq j), Q_j - K \leqslant r_j \leqslant Q_j - 1\}\\
&\leqslant \sum_{j=1}^{l} K \prod_{\substack{1\leqslant i\leqslant l\\ i\neq j}} Q_i \leqslant \sum_{j=1}^{l} \frac{K}{Q_j} \prod_{1\leqslant i\leqslant l} Q_i \leqslant \frac{(\max_{1\leqslant j\leqslant l} q_j)\, l}{K} \prod_{1\leqslant i\leqslant l} Q_i.
\end{aligned}$$

Since (again by (4.6) and the definition of K) $\prod_{j=1}^{l} Q_j \leqslant K^{2l} \leqslant N/K$, we finally obtain

$$\sum_{0\leqslant n<N-k} \overline{g(n)}\, g(n+k) = N \prod_{j=1}^{l} \frac{1}{Q_j} \sum_{r_j=0}^{Q_j-1} \mathrm{e}\left(\alpha_j \left(s_{q_j}(r_j+k) - s_{q_j}(r_j)\right)\right) + O_{\mathbf{q},l}\left(\frac{N}{K}\right).$$

Hence, we get (see (4.5))

$$|S|^2 \leqslant \frac{4N^2}{K} \sum_{k=1}^{K} \left| \prod_{j=1}^{l} \frac{1}{Q_j} \sum_{r_j=0}^{Q_j-1} \mathrm{e}\left(\alpha_j \left(s_{q_j}(r_j+k) - s_{q_j}(r_j)\right)\right)\right| + O_{\mathbf{q},l}\left(\frac{N^2}{K}\right).$$

Employing Hölder's inequality yields

$$|S|^2 \leqslant \frac{4N^2}{K} K^{1/(l+1)} \prod_{j=1}^{l} \left(\sum_{k=1}^{K} \left| \frac{1}{Q_j} \sum_{r_j=0}^{Q_j-1} \mathrm{e}\left(\alpha_j \left(s_{q_j}(r_j+k) - s_{q_j}(r_j)\right)\right) \right|^{l+1} \right)^{1/(l+1)} + O_{\mathbf{q},l}\left(\frac{N^2}{K}\right).$$

Using the fact that $|Q_j^{-1} \sum_{r_j=0}^{Q_j-1} \mathrm{e}\left(\alpha_j \left(s_{q_j}(r_j+k) - s_{q_j}(r_j)\right)\right)| \leqslant 1$, we get

$$|S|^2 \leqslant 4N^2 \prod_{j=1}^{l} \left(\frac{1}{K} \sum_{k=1}^{K} \left| \frac{1}{Q_j} \sum_{r_j=0}^{Q_j-1} \mathrm{e}\left(\alpha_j \left(s_{q_j}(r_j+k) - s_{q_j}(r_j)\right)\right) \right|^{2} \right)^{1/(l+1)} + O_{\mathbf{q},l}\left(\frac{N^2}{K}\right).$$

Let us consider now that index j, say $j = i$, such that $\|(q_j - 1)\alpha_j\|^2 / \log q_i$ is maximal. By assumption, this number is positive and we can employ Proposition 4.1 with $N = Q_i$. Formula (4.6) assures that $\sqrt{Q_i} \leqslant K \leqslant Q_i$. Furthermore, we can bound the other factors ($j \neq i$) trivially by 1. Thus, we obtain

$$|S|^2 = O\left(N^2 Q_i^{-\delta/(l+1)}\right) + O_{\mathbf{q},l}\left(N^2 K^{-1}\right),$$

where $\delta = \frac{\|(q_i-1)\alpha_i\|^2}{20 \log q_i} > 0$. Since the second term is smaller than the first one and $Q_i \geqslant K = \lfloor N^{1/(3l)} \rfloor \geqslant (1/2)N^{1/(3l)}$ (note, that we have assumed that $N \geqslant 2^{3l}$), we finally get

$$|S|^2 = O\left(N^{2-\delta/(3l(l+1))}\right) = O_{\mathbf{q},l}\left(N^{2\left(1-\delta/(12l^2)\right)}\right),$$

and Theorem 4.1 is shown. ∎

Chapter 5

The Sum of Digits Function of Prime Numbers

5.1 Main Theorems

The main contribution of solving Gelfond's problem is the following theorem, which gives a non-trivial upper bound of a sum involving von Mangoldt's Λ-function and the sum of digits function.

Theorem 5.1 (Mauduit, Rivat [33]) *Let $q \geqslant 2$ be an integer and α a real number with the property, that $(q-1)\alpha \in \mathbb{R} \setminus \mathbb{Z}$. Then there exists a constant $\sigma_q(\alpha) > 0$, such that*

$$\sum_{n \leqslant x} \Lambda(n) \mathrm{e}\left(\alpha s_q(n)\right) = O_{q,\alpha}(x^{1-\sigma_q(\alpha)}). \tag{5.1}$$

The proof of this theorem given in Section 5.2 – Section 5.5 is due to Mauduit and Rivat [33]. Using results Mauduit and Rivat obtained in [32] and Drmota, Rivat and Stoll showed in [15] (see Chapter 3), we are able to determine the constant $\sigma_q(\alpha)$ and get a simpler proof of Theorem 5.1.

The proof is organized as follows. In Section 5.2, we use Vaughan's identity to handle the problem which arises when treating sums of the form $\sum_{n \leqslant x} \Lambda(n) g(n)$. We transform them into three different sums that are from type I and type II. Sums of type I are in general easier to handle and we deal with them briefly in Section 5.2. Estimates of sums of type II are much more difficult to obtain and are the hardest part of proving Theorem 5.1. Using the Cauchy-Schwarz inequality and van der Corput's inequality, we have to consider expressions of the form $\alpha s_q(m(n+r)) - \alpha s_q(mn)$. The main idea in treating this differences is to work with a truncated sum of digits function which does not sum over digits of high weight and is periodic. It allows us to use the results obtained in Chapter 3 about trigonometric products. Adding the obtained facts together, we draw the final conclusions in Section 5.5.

Before we start the proof, we present the solution of Gelfond's problem concerning the sum of digits function of prime numbers. Using summation by parts and simple properties of exponential sums (already studied in the first chapter), it is a direct consequence of Theorem 5.1. Furthermore, we show that the sequence $(\alpha s_q(p))_{p \in \mathbb{P}}$ is uniformly distributed modulo 1 for any irrational number α.

Theorem 5.2 (Mauduit, Rivat [33]) *Let q and m be integers $\geqslant 2$ and set $d = (q-1, m)$. Then there exists a constant $\sigma_{q,m} > 0$, such that for every $a \in \mathbb{Z}$*

$$\#\{p \leqslant x : p \text{ prime and } s_q(p) \equiv a \bmod m\} = \frac{d}{m}\pi(x; d, a) + O_{q,m}(x^{1-\sigma_{q,m}}).$$

Proof. By Lemma 1.2 we have

$$\#\{p \leqslant x : p \text{ prime and } s_q(p) \equiv a \bmod m\} = \sum_{p\leqslant x} \frac{1}{m} \sum_{0\leqslant j<m} \mathrm{e}\Big(\frac{j}{m}(s_q(p)-a)\Big).$$

If we put $d = (m, q-1)$, $m' = \frac{m}{d}$, $J = \{km' : 0 \leqslant k < d\}$, $J' = \{0, \dots, m-1\} \setminus J = \{km' + r : 0 \leqslant k < d, 1 \leqslant r < m'\}$, than we have for $j = km' \in J$

$$\mathrm{e}\Big(\frac{j}{m}s_q(p)\Big) = \mathrm{e}\Big(\frac{km'}{dm'}s_q(p)\Big) = \mathrm{e}\Big(\frac{k}{d}s_q(p)\Big) = \mathrm{e}\Big(\frac{k}{d}p\Big).$$

Indeed, Lemma 1.1 gives us $s_q(p) \equiv p \bmod d$, which establishes the last equality. Hence,

$$\sum_{p\leqslant x} \frac{1}{m} \sum_{j\in J} \mathrm{e}\Big(\frac{j}{m}(s_q(p)-a)\Big) = \sum_{p\leqslant x} \frac{1}{m} \sum_{0\leqslant k<d} \mathrm{e}\Big(\frac{k}{d}(p-a)\Big) = \frac{d}{m}\pi(x; d, a).$$

The last equality can again be derived from Lemma 1.2. If we can therefore show that

$$\frac{1}{m} \sum_{j\in J'} \mathrm{e}\Big(-\frac{aj}{m}\Big) \sum_{p\leqslant x} \mathrm{e}\Big(\frac{j}{m}s_q(p)\Big) = O(x^{1-\sigma_{q,m}}), \tag{5.2}$$

where $\sigma_{q,m} > 0$, we are done. If $J' = \emptyset$, which corresponds to the degenerated case where $m \mid q-1$, then we have an error term equal to zero. Therefore we assume now, that $J' \neq \emptyset$. Putting $q' = \frac{q-1}{d}$, we have $(q', m') = 1$, and hence for $j = km' + r \in J'$

$$\frac{(q-1)j}{m} = \frac{dq'(km'+r)}{dm'} = q'k + \frac{q'r}{m'} \notin \mathbb{Z}.$$

By Theorem 5.1 and Lemma A.9, there exists a constant $\sigma_q(j/m)$ for every $j \in J'$, such that

$$\sum_{p\leqslant x} \mathrm{e}\Big(\frac{j}{m}s_q(p)\Big) = O(x^{1-\sigma_q(j/m)}).$$

Putting $\sigma_{q,m} = \min_{j\in J'} \sigma_q(j/m) > 0$ (recall, that $J' \neq \emptyset$), we get the desired estimation in (5.2). ∎

Theorem 5.3 (Mauduit, Rivat [33]) *For $q \geqslant 2$ the sequence $(\alpha s_q(p))_{p\in\mathbb{P}}$ is uniformly distributed modulo 1, if and only if $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.*

Proof. If $\alpha \in \mathbb{Q}$, then the sequence $(\alpha s_q(p))_{p\in\mathbb{P}}$ takes modulo 1 only a finite number of values and is therefore not uniformly distributed modulo 1. If in return $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, then for every $h \in \mathbb{Z}$ with $h \neq 0$ we have $(q-1)h\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and according to Theorem 5.1 there exists $\sigma_q(h\alpha) > 0$, such that

$$\sum_{n\leqslant x} \Lambda(n)\mathrm{e}\Big(h\alpha s_q(n)\Big) = O_{q,h\alpha}(x^{1-\sigma_q(h\alpha)}).$$

Lemma A.9 allows us to write

$$\sum_{p\leqslant x} \mathrm{e}\Big(h\alpha s_q(n)\Big) = O_{q,h\alpha}(x^{1-\sigma_q(h\alpha)}) + O(\sqrt{x}),$$

which proves that $(\alpha s_q(p))_{p\in\mathbb{P}}$ is uniformly distributed modulo 1 (see Theorem A.3). ∎

5.2 Vaughan's Method

In order to prove Theorem 5.1 we have to deal with sums of the form $\sum_n \Lambda(n)g(n)$, where $g(n)$ is an arithmetic function. A classical method to handle such sums goes back to Vinogradov. The main idea is to decompose the von Mangoldt function (or sometimes the Möbius function) judiciously into a sum of a small number of other functions, i.e.

$$\sum_n \Lambda(n)g(n) = \sum_{j=1}^{k} S_j, \quad \text{where } S_j = \sum_m \sum_n a_m b_n g(mn).$$

Traditionally, one calls the multiple sums S_j including at least one "smooth" variable sums of type I, the other sums of type II. In general, it is more difficult to estimate sums of type II. Vinogradov's method is often associated with sieve methods. Following John B. Friedlander [20], the sieve begins with the sieve of Eratosthenes. This method is based on a simply observation. Is n not a prime number, then it has a divisor $\leqslant \sqrt{n}$. Are all primes $p \leqslant \sqrt{x}$ known, then one can easy determine the primes between $\sqrt{x}$ and x. You only have to cancel out ("sieve") all numbers between $\sqrt{x}$ and x which have a prime divisor $p \leqslant \sqrt{x}$. But it needed more than two thousand years until the sieve of Eratosthenes has grown fundamentally. Subsequently Brun discovered some considerably more refined sieves and amongst others, Buchstab, Selberg, Bombieri and Iwaniec improved this theory. But with Vinogradov's work, the sieve theory grew also in a somewhat distinct direction, although the name "sieve methods" is usually applied to the direction Brun initiated. Vaughan gave an elegant formulation of Vinogradov's method, which was subsequently deepened by Heath-Brown. Some other mathematicians who worked on this method are Linnik and Gallagher. The sieve introduced by Friedlander and Iwaniec (see for instance [26, Theorem 13.12]) can be used to derive upper bounds for sums analogous to those of type I and type II, but on different summation intervals. Mauduit and Rivat use a version known as Vaughan's method (see for instance [26, Proposition 13.4]) to prove Theorem 5.1 which avoids the appearance of divisor functions which cannot be bounded individually by a logarithmic factor. The main idea comes from the following trivial identity for $Re(s) > 1$

$$-\frac{\zeta'(s)}{\zeta(s)} = F(s) - \zeta'(s)G(s) - \zeta(s)F(s)G(s) + \zeta(s)\left(\frac{1}{\zeta(s)} - G(s)\right)\left(-\frac{\zeta'(s)}{\zeta(s)} - F(s)\right), \tag{5.3}$$

where $F(s)$ and $G(s)$ are arbitrary functions defined on $Re(s) > 1$. But if we choose for F and G also Dirichlet series, comparing coefficients gives us a decomposition of $\Lambda(n)$. Indeed, the corresponding Dirichlet series of $\zeta'(s)/\zeta(s)$ is by Lemma A.4 $\sum_{n\geqslant 1} \Lambda(n)n^{-s}$. Multiplying this decomposition with $g(n)$ and summing up yields a decomposition of $\sum_n \Lambda(n)g(n)$. In particular, we choose for $1 \leqslant u \leqslant x$ and $Re(s) > 1$

$$G(s) = \sum_{n\leqslant u} \frac{\mu(s)}{n^s}, \quad F(s) = \sum_{n\leqslant u} \frac{\Lambda(n)}{n^s}.$$

Note, that $G(s)$ and $F(s)$ are the partial sums of $\frac{1}{\zeta(s)}$, respectively $-\frac{\zeta'(s)}{\zeta(s)}$ (see Lemma A.4) and that $\zeta'(s) = -\sum_{n\geqslant 1} \log n\, n^{-s}$. Hence, we can write (5.3) as

$$\sum_{n\geqslant 1} \frac{\Lambda(n)}{n^s} = \sum_{n\leqslant u} \frac{\Lambda(n)}{n^s} + \sum_{\substack{n\geqslant 1\\ m\leqslant u}} \frac{\mu(m)\log(n)}{(nm)^s} - \sum_{\substack{n\geqslant 1\\ m_1\leqslant u\\ m_2\leqslant u}} \frac{\mu(m_1)\Lambda(m_2)}{(m_1m_2n)^s} + \sum_{\substack{n\geqslant 1\\ u<m_1\\ u<m_2}} \frac{\mu(m_1)\Lambda(m_2)}{(m_1m_2n)^s}.$$

If we consider this equality with $1 \leqslant u \leqslant \frac{x}{q}$, by comparison of coefficients and summing over n follows

$$\sum_{\frac{x}{q}<n\leqslant x} \Lambda(n)g(n) = S_1 - S_2 + S_3,$$

where

$$\begin{aligned} S_1 &= \sum_{\substack{m\leqslant u \\ x/q<mn\leqslant x}} \mu(m)\log(n)g(mn), \\ S_2 &= \sum_{\substack{m_1\leqslant u \\ m_2\leqslant u \\ x/q<m_1m_2n\leqslant x}} \mu(m_1)\Lambda(m_2)g(m_1m_2n), \\ S_3 &= \sum_{\substack{u<m\leqslant x \\ u<n_1\leqslant x \\ x/q<mn_1n_2\leqslant x}} \mu(m)\Lambda(n_1)g(mn_1n_2). \end{aligned} \tag{5.4}$$

One can also derive this combinatorial identity without using Dirichlet series. Therefore we follow the presentation in the book of Iwaniec and Kowalski [26, Chapter 13.4]. We start with the relation

$$\Lambda(n) = \sum_{\substack{b,c \\ bc|n}} \Lambda(b)\mu(c),$$

which is a direct consequence of Lemma A.3 (with $z = 1$). In order to obtain the desired decomposition we need the following relation

$$\sum_{d|n} \Lambda(d) = \sum_{p|n} \nu_p(n)\log p = \log\prod_{p|n} p^{\nu_p(n)} = \log n. \tag{5.5}$$

Let $1 \leqslant u < x/q$. We split the sum up according to the size of b and c

$$\Lambda(n) = \sum_{\substack{b\leqslant u,c\leqslant u \\ bc|n}} \Lambda(b)\mu(c) + \sum_{\substack{b\leqslant u,c>u \\ bc|n}} \Lambda(b)\mu(c) + \sum_{\substack{b>,c\leqslant u \\ bc|n}} \Lambda(b)\mu(c) + \sum_{\substack{b>u,c>u \\ bc|n}} \Lambda(b)\mu(c).$$

If $n > u$, we have by Lemma A.3

$$\sum_{\substack{b\leqslant u,c\leqslant u \\ bc|n}} \Lambda(b)\mu(c) + \sum_{\substack{b\leqslant u,c>u \\ bc|n}} \Lambda(b)\mu(c) = \sum_{b\leqslant u} \Lambda(b) \sum_{c\mid \frac{n}{b}} \mu(c) = 0$$

and by (5.5)

$$\sum_{\substack{b\leqslant u,c\leqslant u \\ bc|n}} \Lambda(b)\mu(c) + \sum_{\substack{b>,c\leqslant u \\ bc|n}} \Lambda(b)\mu(c) = \sum_{\substack{c\leqslant u \\ c|n}} \mu(c) \sum_{b\mid \frac{n}{c}} \Lambda(b) = \sum_{\substack{c\leqslant u \\ c|n}} \mu(c)\log\left(\frac{n}{c}\right).$$

Hence, taking these facts into account, we finally obtain ($n > u$)

$$\Lambda(n) = \sum_{\substack{c\leqslant u \\ c|n}} \mu(c)\log\left(\frac{n}{c}\right) - \sum_{\substack{b\leqslant u,c\leqslant u \\ bc|n}} \Lambda(b)\mu(c) + \sum_{\substack{b>u,c>u \\ bc|n}} \Lambda(b)\mu(c).$$

Weighting by $g(n)$ and summing over $x/q < n \leqslant x$ we get the same representation of $\sum_{\frac{x}{q}<n\leqslant x} \Lambda(n)g(n)$ as before. Now we can state the key lemma for Theorem 5.1.

Lemma 5.1 *Let $q \geqslant 2$ be an integer, $0 < \beta_1 < \frac{1}{3}, \frac{1}{2} < \beta_2 < 1$ real numbers and $x \geqslant q^{\frac{1}{\beta_2 - 1/2}}$. Let g be an arithmetic function. Suppose that uniformly for all real numbers $M \leqslant x$ and all complex numbers a_m, b_n with $|a_m|, |b_n| \leqslant 1$, we have*

$$\max_{\frac{x}{qM} < t \leqslant \frac{xq}{M}} \sum_{\frac{M}{q} < m \leqslant M} \left| \sum_{\frac{x}{qm} < n \leqslant t} g(mn) \right| \leqslant U \quad \text{for } M \leqslant x^{\beta_1} \quad \text{(type I)}, \tag{5.6}$$

$$\left| \sum_{\frac{M}{q} < m \leqslant M} \sum_{\frac{x}{qm} < n \leqslant \frac{x}{m}} a_m b_n g(mn) \right| \leqslant U \quad \text{for } x^{\beta_1} \leqslant M \leqslant x^{\beta_2} \quad \text{(type II)}. \tag{5.7}$$

Then

$$\sum_{\frac{x}{q} < n \leqslant x} \Lambda(n) g(n) \ll U (\log x)^2.$$

Proof. As the preceding discussion has shown, we have

$$\sum_{\frac{x}{q} < n \leqslant x} \Lambda(n) g(n) = S_1 - S_2 + S_3,$$

where S_1, S_2 and S_3 are defined in (5.4). We can choose $u = x^{\beta_1}$, since $1 \leqslant u \leqslant \sqrt{x} \leqslant x/q$ (note, that $x \geqslant q^{\frac{1}{\beta_2 - 1/2}} \geqslant q^2$). The sum S_1 is of type I and can be estimated by summation by parts (see Lemma A.5). We have

$$S_1 = \sum_{m \leqslant u} \mu(m) \left(\log\left(\frac{x}{m}\right) \sum_{\frac{x}{qm} < n \leqslant \frac{x}{m}} g(mn) - \int_{\frac{x}{qm}}^{\frac{x}{m}} \sum_{\frac{x}{qm} < n \leqslant t} g(mn) \frac{dt}{t} \right).$$

Thus, taking the absolute value and splitting the sum up according to the powers of q, we obtain

$$\begin{aligned} |S_1| &\leqslant (\log x) \sum_{m \leqslant u} \left| \sum_{\frac{x}{qm} < n \leqslant \frac{x}{m}} g(mn) \right| + \sum_{m \leqslant u} \int_{\frac{x}{qm}}^{\frac{x}{m}} \left| \sum_{\frac{x}{qm} < n \leqslant t} g(mn) \right| \frac{dt}{t} \\ &\ll (\log x) \max_{M \leqslant u} \left((\log x) \sum_{\frac{M}{q} < m \leqslant M} \left| \sum_{\frac{x}{qm} < n \leqslant \frac{x}{m}} g(mn) \right| + \int_{\frac{x}{qm}}^{\frac{x}{m}} \sum_{\frac{M}{q} < m \leqslant M} \left| \sum_{\frac{x}{qm} < n \leqslant t} g(mn) \right| \frac{dt}{t} \right). \end{aligned}$$

Employing (5.6) we derive $S_1 \ll U (\log x)^2$.

To bound S_2 we first observe that (see (5.5))

$$\left| \sum_{\substack{m_1, m_2 \leqslant u \\ m = m_1 m_2}} \mu(m_1) \Lambda(m_2) \right| \leqslant \sum_{d \mid m} \Lambda(d) = \log m.$$

Therefore we get

$$|S_2| \leqslant \sum_{m \leqslant u^2} \left| \sum_{\substack{m_1, m_2 \leqslant u \\ m = m_1 m_2}} \mu(m_1) \Lambda(m_2) \right| \left| \sum_{\frac{x}{qm} < n \leqslant \frac{x}{m}} g(mn) \right| \leqslant \sum_{m \leqslant u^2} (\log m) \left| \sum_{\frac{x}{qm} < n \leqslant \frac{x}{m}} g(mn) \right|.$$

Splitting again the summation up over m according to the powers of q we obtain

$$|S_2| \ll (\log x)^2 \max_{M \leqslant u^2} \sum_{\frac{M}{q} < m \leqslant M} \left| \sum_{\frac{x}{qm} < n \leqslant \frac{x}{m}} g(mn) \right|.$$

Let M_0 be a value of M for which the maximum is attained. If $M_0 \leqslant u$ $(= x^{\beta_1})$ or $u < M_0 \leqslant x^{\frac{1}{2}}$ we can employ (5.6) in the first case or (5.7) in the second case to derive $S_2 \ll U(\log x)^2$. In the case that $x^{\frac{1}{2}} < M_0 \leqslant u^2$ we can choose complex numbers a_m such that

$$\sum_{\frac{M_0}{q} < m \leqslant M_0} \left| \sum_{\frac{x}{qm} < n \leqslant \frac{x}{m}} g(mn) \right| = \sum_{\frac{M_0}{q} < m \leqslant M_0} \sum_{\frac{x}{qm} < n \leqslant \frac{x}{m}} a_m g(mn).$$

Setting $a_m = 0$ if $m > M_0$ or $m \leqslant M_0/q$, we are able to change the order of summation and get

$$\begin{aligned} \sum_{\frac{M_0}{q} < m \leqslant M_0} \left| \sum_{\frac{x}{qm} < n \leqslant \frac{x}{m}} g(mn) \right| &= \sum_{\frac{x}{M_0 q} < n \leqslant \frac{x}{M_0}} \sum_{\frac{x}{qn} < m \leqslant M_0} a_m g(mn) + \sum_{\frac{x}{M_0} < n \leqslant \frac{qx}{M_0}} \sum_{\frac{M_0}{q} < m \leqslant \frac{x}{n}} a_m g(mn) \\ &= \sum_{\frac{x}{M_0 q} < n \leqslant \frac{x}{M_0}} \sum_{\frac{x}{qn} < m \leqslant \frac{x}{n}} a_m g(mn) + \sum_{\frac{x}{M_0} < n \leqslant \frac{qx}{M_0}} \sum_{\frac{x}{qn} < m \leqslant \frac{x}{n}} a_m g(mn). \end{aligned}$$

If we define $M_1 = \frac{x}{M_0}$ and $M_2 = \frac{xq}{M_0}$ and use the fact that $x^{\frac{1}{2}} < M_0 \leqslant u^2 = x^{2\beta_1}$ and $x \geqslant q^{\frac{1}{\beta_2 - 1/2}}$, we derive

$$x^{\beta_1} \leqslant x^{1-2\beta_1} \leqslant M_1 \leqslant x^{\frac{1}{2}} \leqslant x^{\beta_2} \quad \text{and} \quad x^{\beta_1} \leqslant M_2 \leqslant x^{\frac{1}{2}} q \leqslant x^{\beta_2}.$$

Thus we can employ the type II estimation (5.7) to the first sum with $M = M_1$ and to the second with $M = M_2$ and we obtain $S_2 \ll U(\log x)^2$.
To bound S_3 we write

$$S_3 = \log x \sum_{u < m \leqslant \frac{x}{u}} \sum_{\frac{x}{qm} < n \leqslant \frac{x}{m}} a_m b_n g(mn),$$

where $a_m = \mu(m)$ and $b_n = \frac{1}{\log x} \sum_{n = n_1 n_2} \Lambda(n_1)$, satisfying $|a_m| \leqslant 1$ and $0 \leqslant b_n \leqslant \frac{1}{\log x} \sum_{d|n} \Lambda(d) = \frac{\log n}{\log x} \leqslant 1$. Splitting the summation up over m according to the powers of q we obtain

$$|S_3| \ll (\log x)^2 \max_{u \leqslant M \leqslant \frac{x}{u}} \left| \sum_{\frac{x}{M} < m \leqslant M} \sum_{\frac{x}{qm} < n \leqslant \frac{x}{m}} a_m b_n g(mn) \right|.$$

Let M_0 be again a value of M for which the maximum is attained. If $u < M_0 \leqslant x^{\frac{1}{2}}$ we can employ (5.7). In the case that $x^{\frac{1}{2}} < M_0 \leqslant \frac{x}{u}$ we can carry out the same procedure as for S_2 (note, that $x^{\beta_1} \leqslant \frac{x}{M_0} \leqslant x^{\frac{1}{2}} \leqslant x^{\beta_2}$ and $x^{\beta_1} \leqslant \frac{xq}{M_0} \leqslant x^{\frac{1}{2}} q \leqslant x^{\beta_2}$). Thus, we obtain $|S_3| \ll U(\log x)^2$ and therefore finally

$$\sum_{\frac{x}{q} < n \leqslant x} \Lambda(n) g(n) \ll U(\log x)^2.$$

■

5.3 Sums of Type I

Lemma 5.1 shows that the key in proving Theorem 5.1 lies in achieving upper bounds for type I and type II sums. Mauduit and Rivat treated type I sums using a method developed by Fouvry and Mauduit [18, 19]. They could give an upper bound of (5.6) with $\beta_1 = 1/3$ which allowed them to get a better exponent $\sigma_q(\alpha)$ in Theorem 5.1. In this work we want to show a shorter proof of Gelfond's problem and seeing that, we treat type I sums more crudely. If we choose β_1 sufficiently small, we can show a negligible upper bound for type I sums in a much simpler way. In order to compensate this loss, we have to get estimates of type II sums for a bigger domain. This results in a worse exponent $\sigma_q(\alpha)$, but has not a notable effect on proving Gelfond's problem.

Proposition 5.1 *Let $q \geqslant 2$ be an integer and α a real number, such that $(q-1)\alpha \in \mathbb{R} \setminus \mathbb{Z}$. Then we have for $1 \leqslant M \leqslant x^{\frac{c_q\|(q-1)\alpha\|^2}{2}}$*

$$\max_{\frac{x}{qM}<t\leqslant\frac{xq}{M}} \sum_{\frac{M}{q}<m\leqslant M} \left| \sum_{\frac{x}{qm}<n\leqslant t} \mathrm{e}\left(\alpha s_q(mn)\right)\right| \ll_q x^{1-\frac{c_q\|(q-1)\alpha\|^2}{2}},$$

where $c_q = \frac{\pi^2}{12\log q}\left(1-\frac{2}{q+1}\right)$ and $0 < c_q\|(q-1)\alpha\|^2 < 1$.

In order to be able to use results from Chapter 3, we need the following lemma.

Lemma 5.2 *Let f be a completely q-additive function. Then we have for every $q \geqslant 2, \alpha \in \mathbb{R}, N \geqslant 1$*

$$\left|\sum_{0\leqslant l<N} \mathrm{e}\left(f(l)+\frac{kl}{m}\right)\right| \leqslant (q-1) \sum_{\nu\leqslant\frac{\log N}{\log q}} \left|\sum_{0\leqslant l<q^\nu} \mathrm{e}\left(f(l)+\frac{kl}{m}\right)\right|. \tag{5.8}$$

Proof. Writing $i = \left\lfloor \frac{\log N}{\log q} \right\rfloor$, we have $N = yq^i + N'$ with $0 \leqslant y \leqslant q-1$ and $0 \leqslant N' < q^i$. Hence, as f is completely q-additive, the left hand side is bounded by

$$\begin{aligned}&\left|\sum_{0\leqslant l<yq^i} \mathrm{e}\left(f(l)+\frac{kl}{m}\right)\right| + \left|\sum_{0\leqslant l<N'} \mathrm{e}\left(f(yq^i+l)+\frac{k(yq^i+l)}{m}\right)\right| \\ \leqslant & y\left|\sum_{0\leqslant l<q^i} \mathrm{e}\left(f(l)+\frac{kl}{m}\right)\right| + \left|\sum_{0\leqslant l<N'} \mathrm{e}\left(f(l)+\frac{kl}{m}\right)\right|.\end{aligned}$$

Now we apply this procedure to N' and after finite many steps we get our result. ∎

Proof (of Proposition 5.1). Taking the difference, it suffices to prove that

$$\max_{\frac{x}{qM}\leqslant t\leqslant\frac{xq}{M}} \sum_{\frac{M}{q}<m\leqslant M} \left| \sum_{0\leqslant n\leqslant t} \mathrm{e}\left(\alpha s_q(mn)\right)\right| \ll_q x^{1-\frac{c_q\|(q-1)\alpha\|^2}{2}}.$$

According to Lemma 1.2, we can write

$$\begin{aligned}\sum_{\frac{M}{q}<m\leqslant M} \left| \sum_{0\leqslant n\leqslant t} \mathrm{e}\left(\alpha s_q(mn)\right)\right| &= \sum_{\frac{M}{q}<m\leqslant M} \left|\frac{1}{m}\sum_{0\leqslant k<m}\sum_{0\leqslant l\leqslant mt} \mathrm{e}\left(\alpha s_q(l)+\frac{kl}{m}\right)\right| \\ &\leqslant M + \frac{q}{M}\sum_{\frac{M}{q}<m\leqslant M}\sum_{0\leqslant k<m}\left|\sum_{0\leqslant l<mt} \mathrm{e}\left(\alpha s_q(l)+\frac{kl}{m}\right)\right|.\end{aligned}$$

The first term M only exists when mt is an integer. Next, we employ Lemma 5.2

$$\sum_{\frac{M}{q}<m\leqslant M}\left|\sum_{\frac{x}{qm}<n\leqslant t}\mathrm{e}\left(\alpha s_q(mn)\right)\right|\leqslant M+\frac{q(q-1)}{M}\sum_{\lambda\leqslant\frac{\log mt}{\log q}}\sum_{\frac{M}{q}<m\leqslant M}\sum_{0\leqslant k<m}\left|\sum_{0\leqslant l<q^\lambda}\mathrm{e}\left(\alpha s_q(l)+\frac{kl}{m}\right)\right|.$$

By Definition 3.2 (Fourier transform) and Lemma 3.6, we have

$$\left|\sum_{0\leqslant l<q^\lambda}\mathrm{e}\left(\alpha s_q(l)+\frac{kl}{m}\right)\right|=q^\lambda|F(-(k/m)q^\lambda,\alpha)|\leqslant q^{(1-c_q\|(q-1)\alpha\|^2)\lambda},$$

where $0<c_q\|(q-1)\alpha\|^2<1$ since $(q-1)\alpha\notin\mathbb{Z}$ and $c_q<1$. Furthermore we have for $t\leqslant\frac{xq}{M}$ and $m\leqslant M$, that $mt\leqslant xq$. Hence we finally obtain ($M\leqslant x^{\frac{c_q\|(q-1)\alpha\|^2}{2}}$)

$$\begin{aligned}\sum_{\frac{M}{q}<m\leqslant M}\left|\sum_{\frac{x}{qm}<n\leqslant t}\mathrm{e}\left(\alpha s_q(mn)\right)\right|&\ll_q M+\frac{1}{M}\sum_{\lambda\leqslant\frac{\log xq}{\log q}}M^2q^{(1-c_q\|(q-1)\alpha\|^2)\lambda}\\&\ll_q Mx^{1-c_q\|(q-1)\alpha\|^2}\ll_q x^{1-\frac{c_q\|(q-1)\alpha\|^2}{2}}.\end{aligned}$$

■

5.4 Sums of type II

In order to estimate the type II sums we will reduce the problem to a slightly simpler one. We use therefore a version of a classical procedure of separation of variables which allows us to remove the multiplicative constraints.

Lemma 5.3 *Let g be an arithmetic function, $q\geqslant 2, 0<\delta<\beta_1<1/3, 1/2<\beta_2<1$. Suppose that, uniformly for all complex numbers b_n with $|b_n|\leqslant 1$, we have*

$$\sum_{q^{\mu-1}<m\leqslant q^\mu}\left|\sum_{q^{\nu-1}<n\leqslant q^\nu}b_ng(mn)\right|\leqslant V, \tag{5.9}$$

for all positive integers μ and ν with $q^{\mu+\nu}\ll_q x$ and

$$\beta_1-\delta\leqslant\frac{\mu}{\mu+\nu}\leqslant\beta_2+\delta. \tag{5.10}$$

Then for $x>x_0=\max(q^{1/(1-\beta_2)},q^{3/\delta})$ we have uniformly in M such that $x^{\beta_1}\leqslant M\leqslant x^{\beta_2}$ the estimate

$$\left|\sum_{\frac{M}{q}<m\leqslant M}\sum_{\frac{x}{qm}<n\leqslant\frac{x}{m}}a_mb_ng(mn)\right|\ll(\log x)V.$$

Lemma 5.4 *For every sequence of complex numbers $(a_n)_{n\in\mathbb{N}}$ and all integers $N_0\leqslant N_1<N_2\leqslant N_3$, we have*

$$\left|\sum_{N_1<n\leqslant N_2}a_n\right|\leqslant\int_{-\frac12}^{\frac12}\min\left\{N_2-N_1,\frac{1}{|\sin\pi\xi|}\right\}\left|\sum_{N_0<n\leqslant N_3}a_n\mathrm{e}(n\xi)\right|d\xi.$$

Moreover, we have for $x\geqslant\frac{2}{\pi}$

$$\int_{-\frac12}^{\frac12}\min\left\{x,\frac{1}{|\sin\pi\xi|}\right\}d\xi\ll\log x.$$

Proof. As $\int_{-\frac{1}{2}}^{\frac{1}{2}} \mathrm{e}(m\xi)\,d\xi = 1$ for every integer $s \neq 0$ (in the case that $s = 0$ the integral is clearly 1), we have

$$\sum_{N_1<n\leqslant N_2} a_n = \int_{-\frac{1}{2}}^{\frac{1}{2}} \left(\sum_{N_0<n\leqslant N_3} a_n \mathrm{e}(n\xi)\right)\left(\sum_{N_1<n'\leqslant N_2} \mathrm{e}(-n'\xi)\right) d\xi.$$

But for $-\frac{1}{2} \leqslant \xi \leqslant \frac{1}{2}$, $\xi \neq 0$, we can write

$$\left|\sum_{N_1<n'\leqslant N_2} \mathrm{e}(-n'\xi)\right| = \left|\frac{\sin(N_2 - N_1)\pi\xi}{\sin \pi\xi}\right| \leqslant \min\left\{N_2 - N_1, \frac{1}{|\sin \pi\xi|}\right\},$$

which establishes the first inequality. Using the fact that the integrand is an even function and splitting at $\frac{1}{\pi x}$, we obtain

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} \min\left\{x, \frac{1}{|\sin \pi\xi|}\right\} d\xi \leqslant 2\int_0^{\frac{1}{\pi x}} x\,d\xi + 2\int_{\frac{1}{\pi x}}^{\frac{1}{2}} \frac{d\xi}{\sin \pi\xi} = \frac{2}{\pi} + \frac{2}{\pi}\log\cot\left(\frac{1}{2x}\right) \leqslant \frac{2}{\pi} + \frac{2}{\pi}\log 2x \ll \log x.$$

Here we use the fact that $\cot u \leqslant \frac{1}{u}$ on the interval $[0, \pi/2]$. ∎

Proof (of Lemma 5.3). We assume that $x > \max(q^{1/(1-\beta_2)}, q^{3/\delta})$ and $x^{\beta_1} \leqslant M \leqslant x^{\beta_2}$. It follows easily from these assumptions that $M > q$ and $\frac{x}{M} > q$ (note, that $\frac{1}{\beta_1} \leqslant \frac{3}{\delta}$, since $\delta < \beta_1$). Hence, there exist integers $\mu, \nu \geqslant 1$ such that

$$q^{\mu'} < M \leqslant q^{\mu'+1} \quad \text{and} \quad q^{\nu'} < \frac{x}{M} \leqslant q^{\nu'+1}. \tag{5.11}$$

For $\frac{M}{q} < m \leqslant M$ we have $q^{\nu'-1} \leqslant \frac{x}{qm} < \frac{x}{m} \leqslant q^{\nu'+2}$ and hence we can apply Lemma 5.4 with $N_0 = q^{\nu'-1} \leqslant N_1 = \left\lfloor \frac{x}{qm} \right\rfloor < N_2 = \left\lfloor \frac{x}{m} \right\rfloor \leqslant N_3 = q^{\nu'+2}$. Thus we obtain

$$\begin{aligned}\sum_{\frac{M}{q}<m\leqslant M} \left|\sum_{\frac{x}{qm}<n\leqslant \frac{x}{m}} b_n g(mn)\right| &\leqslant \sum_{\frac{M}{q}<m\leqslant M} \int_{-\frac{1}{2}}^{\frac{1}{2}} \min\left\{N_2 - N_1, \frac{1}{|\sin \pi\xi|}\right\} \left|\sum_{q^{\nu'-1}<n\leqslant q^{\nu'+2}} b_n \mathrm{e}(n\xi) g(mn)\right| d\xi \\ &\leqslant \sum_{\mu=\mu'}^{\mu'+1} \sum_{\nu=\nu'}^{\nu'+2} \int_{-\frac{1}{2}}^{\frac{1}{2}} \min\left\{x, \frac{1}{|\sin \pi\xi|}\right\} \sum_{q^{\mu-1}<m\leqslant q^{\mu}} \left|\sum_{q^{\nu-1}<n\leqslant q^{\nu}} b_n \mathrm{e}(n\xi) g(mn)\right| d\xi.\end{aligned}$$

Indeed, after estimating $N_2 - N_1 \leqslant x$, we can interchange the sum and the integral and split the sum up over m, because $q^{\mu'-1} < \frac{M}{q} < M \leqslant q^{\mu'+1}$. Here we possibly add only a few terms. If we now can show condition (5.10) for (μ, ν), we are able to apply inequality (5.9) with b_n replaced by $b_n \mathrm{e}(n\xi)$. Hence we are done since we can bound the last expression by $6V \int_{-\frac{1}{2}}^{\frac{1}{2}} \min\left\{x, \frac{1}{|\sin \pi\xi|}\right\} d\xi \ll (\log x)V$ (Lemma 5.4).

We have for $(\mu, \nu) \in \{\mu', \mu'+1\} \times \{\nu', \nu'+1, \nu'+2\}$

$$\frac{\mu' - 2}{\mu' + \nu'} \leqslant \frac{\mu}{\mu + \nu} \leqslant \frac{\mu' + 3}{\mu' + \nu' + 2},$$

and hence it suffices to show

$$\beta_1 - \delta \leqslant \frac{\mu' - 2}{\mu' + \nu'} \quad \text{and} \quad \frac{\mu' + 3}{\mu' + \nu' + 2} \leqslant \beta_2 + \delta.$$

Using $x^{\beta_1} \leqslant M \leqslant x^{\beta_2}$ and employing (5.11) we get

$$\frac{\log x}{\log q} - 2 \leqslant \mu' + \nu' \leqslant \frac{\log x}{\log q} \quad \text{and} \quad \beta_1 \frac{\log x}{\log q} - 1 \leqslant \mu' \leqslant \beta_2 \frac{\log x}{\log q}.$$

$x > q^{3/\delta}$ implies $\delta > 3\frac{\log q}{\log x}$ and we finally obtain

$$\frac{\mu' - 2}{\mu' + \nu'} \geqslant \frac{\beta_1 \frac{\log x}{\log q} - 3}{\frac{\log x}{\log q}} = \beta_1 - 3\frac{\log q}{\log x} \geqslant 1 - \delta$$

and

$$\frac{\mu' + 3}{\mu' + \nu' + 2} \leqslant \frac{\beta_2 \frac{\log x}{\log q} + 3}{\frac{\log x}{\log q}} = \beta_2 + 3\frac{\log q}{\log x} \leqslant 1 + \delta.$$

■

Proposition 5.2 *Let $q \geqslant 2$ be an integer and α a real number satisfying $(q-1)\alpha \in \mathbb{R} \setminus \mathbb{Z}$. Then there exist β_1, β_2 and δ with $0 < \delta \leqslant \beta_1 < c_q \|(q-1)\alpha\|^2 < 1/3$ and $1/2 < \beta_2 < 1$ and a constant $\xi_q(\alpha)$, such that for every $\varepsilon > 0$*

$$\sum_{q^{\mu-1} < m \leqslant q^{\mu}} \left| \sum_{q^{\nu-1} < n \leqslant q^{\nu}} b_n \mathrm{e}(\alpha s_q(mn)) \right| \ll_{q,\varepsilon} q^{(1 - \frac{1}{2}\xi_q(\alpha) + \varepsilon)(\mu+\nu)}, \tag{5.12}$$

for all positive integers μ and ν such that

$$\beta_1 - \delta \leqslant \frac{\mu}{\mu + \nu} \leqslant \beta_2 + \delta,$$

uniformly for all complex numbers b_n for which $|b_n| \leqslant 1$.

The proof of Proposition 5.2 is the hardest part of proving Theorem 5.1. We will therefore state and prove several lemmas. Let us assume that $\mu \geqslant 1, \nu \geqslant 1$ and ρ be an integers with

$$0 \leqslant \rho \leqslant \nu/2.$$

Recall that we have defined $f(n) = \alpha s_q(n)$. We can assume that $\alpha \in \mathbb{R} \setminus \mathbb{Z}$, since $(q-1)\alpha \in \mathbb{R} \setminus \mathbb{Z}$. For convenience, we use the following abbreviation for the left hand side of (5.12)

$$S = \sum_{q^{\mu-1} < m \leqslant q^{\mu}} \left| \sum_{q^{\nu-1} < n \leqslant q^{\nu}} b_n \mathrm{e}(\alpha s_q(mn)) \right|.$$

First of all, we use the Cauchy-Schwarz inequality and a version of van der Corput's inequality introduced in Chapter 2 to smooth this sums. The Cauchy-Schwarz inequality gives us

$$|S|^2 \leqslant q^{\mu} \sum_{q^{\mu-1} < m \leqslant q^{\mu}} \left| \sum_{q^{\nu-1} < n \leqslant q^{\nu}} b_n \mathrm{e}(\alpha s_q(mn)) \right|^2.$$

Now we employ Lemma 2.7 with $R = q^\rho, N = q^\nu - q^{\nu-1}$, $z_n = b_{q^{\nu-1}+n}\mathrm{e}\left(f(m(q^{\nu-1}+n))\right)$ and $k = 1$. In the next step we split the sum up over $|r|$ in $r = 0$ and $r \neq 0$ and use the fact that $\rho \leqslant \nu - 1$.

$$|S|^2 \leqslant q^\mu \sum_{q^{\mu-1}<m\leqslant q^\mu} \frac{q^\nu - q^{\nu-1} + q^\rho}{q^\rho} \sum_{|r|<q^\rho}\left(1-\frac{|r|}{q^\rho}\right) \sum_{\substack{q^{\nu-1}<n\leqslant q^\nu \\ q^{\nu-1}<n+r\leqslant q^\nu}} b_{n+r}\overline{b_n}\mathrm{e}\left(f(m(n+r)) - f(mn)\right)$$

$$\leqslant q^{\mu+\nu-\rho} \sum_{q^{\mu-1}<m\leqslant q^\mu}\left(q^\nu + \sum_{1\leqslant|r|<q^\rho}\left(1-\frac{|r|}{q^\rho}\right) \sum_{\substack{q^{\nu-1}<n\leqslant q^\nu \\ q^{\nu-1}<n+r\leqslant q^\nu}} b_{n+r}\overline{b_n}\mathrm{e}\left(f(m(n+r)) - f(mn)\right)\right).$$

Since $\sum_{1\leqslant|r|<q^\rho}\left(1-\frac{|r|}{q^\rho}\right) = q^\rho - 1 \leqslant q^\rho$ we get an error term $\sum_{q^{\mu-1}<m\leqslant q^\mu}\sum_{1\leqslant|r|<q^\rho}\left(1-\frac{|r|}{q^\rho}\right)|r| \leqslant q^{\mu+2\rho} \leqslant q^{\mu+\nu}$ when removing the summation condition $q^{\nu-1} < n + r \leqslant q^\nu$. Furthermore we can change the order of summation and consider the maximum over $|r|$ to get

$$|S|^2 \leqslant q^{2(\mu+\nu)-\rho} + q^{\mu+\nu-\rho} \sum_{q^{\mu-1}<m\leqslant q^\mu}\sum_{1\leqslant|r|<q^\rho}\left(1-\frac{|r|}{q^\rho}\right) \sum_{\substack{q^{\nu-1}<n\leqslant q^\nu \\ q^{\nu-1}<n+r\leqslant q^\nu}} b_{n+r}\overline{b_n}\mathrm{e}\left(f(m(n+r)) - f(mn)\right)$$

$$\leqslant 2q^{2(\mu+\nu)-\rho} + q^{\mu+\nu-\rho} \sum_{1\leqslant|r|<q^\rho}\left(1-\frac{|r|}{q^\rho}\right) \sum_{q^{\nu-1}<n\leqslant q^\nu}\left|\sum_{q^{\mu-1}<m\leqslant q^\mu}\mathrm{e}\left(f(m(n+r)) - f(mn)\right)\right|$$

$$\ll q^{2(\mu+\nu)-\rho} + q^{\mu+\nu} \max_{1\leqslant|r|<q^\rho} \sum_{q^{\nu-1}<n\leqslant q^\nu}\left|\sum_{q^{\mu-1}<m\leqslant q^\mu}\mathrm{e}\left(f(m(n+r)) - f(mn)\right)\right|.$$

To continue the proof we are going to show that the digits of high weight in the difference $f(m(n + r)) - f(mn)$ do not contribute significantly and are negligible. Therefore we work with the notion of the truncated sum of digits function which we have already introduced in Chapter 3. Actually, we defined for any integer $\lambda \geqslant 0$

$$f_\lambda(n) = \sum_{k<\lambda} f(n_k q^k) = \alpha \sum_{k<\lambda} n_k,$$

where the integers n_k denote the digits of n in basis q. This function is clearly periodic of period q^λ and arises in a different setting in [14] where Drmota and Rivat studied certain properties of $f_\lambda(n^2)$ when λ is of order $\log n$. The next lemma shows that we can replace the truncated function in the estimation of S, since this yields an negligible error term.

Lemma 5.5 *For all integers μ, ν, ρ with $\mu > 0, \nu > 0, 0 \leqslant \rho \leqslant \nu/2$ and for all $r \in \mathbb{Z}$ with $|r| < q^\rho$, we denote by $E(r, \mu, \nu, \rho)$ the number of pairs $(m, n) \in \mathbb{Z}^2$ such that $q^{\mu-1} < m \leqslant q^\mu, q^{\nu-1} < n \leqslant q^\nu$ and*

$$f(m(n + r)) - f(mn) \neq f_{\mu+2\rho}(m(n + r)) - f_{\mu+2\rho}(mn).$$

Then we have for $\varepsilon > 0$

$$E(r, \mu, \nu, \rho) \ll_\varepsilon q^{(\mu+\nu)(1+\varepsilon)-\rho}.$$

Proof. Suppose $0 \leqslant r < q^\rho$. In this case we have $0 \leqslant mr < q^{\mu+\rho}$. When we compute the sum $mn + mr$, the digits of the product mn of index $\geqslant \mu + \rho$ cannot be modified unless there is a carry propagation.

Hence we must count the number of pairs (m,n) such that the digits a_j in basis q of the product $a=mn$ satisfy $a_j=q-1$ for $\mu+\rho\leqslant j<\mu+2\rho$. Therefore grouping the products mn according to their value a, we obtain

$$E(r,\mu,\nu,\rho)\leqslant\sum_{q^{\mu+\nu-2}<a\leqslant q^{\mu+\nu}}\tau(a)\chi(a),$$

where $\tau(a)$ denotes the number of divisors of a and $\chi(a)=1$ if the digits a_j in basis q of a satisfy $a_j=q-1$ for $\mu+\rho\leqslant j<\mu+2\rho$ and $\chi(a)=0$ in the opposite case. The number of integers a satisfying these conditions is bounded by $q^{\mu+\nu-\rho}$ since $a\leqslant q^{\mu+\nu}$ and ρ digits are fixed. But by Lemma A.2, we have $\tau(a)\ll_\varepsilon a^\varepsilon\ll_\varepsilon q^{(\mu+\nu)\varepsilon}$ and the desired estimation is proved. In the case that $-q^\rho<r<0$, the same reasoning applies. We have to count the pairs (m,n) of integers for which the digits a_j of the product $a=mn$ satisfy $a_j=0$ for $\mu+\rho\leqslant j<\mu+2\rho$, and we obtain the same estimation. ∎

Remark. Drmota, Mauduit and Rivat showed in [13] that $E(r,\mu,\nu,\rho)\leqslant(\mu+\nu)\log q\,q^{\mu+\nu-\rho}$ when $\mu/(\mu+\nu)\geqslant 27/82$. Based on that fact, they obtain a slightly better result in Proposition 5.2.

In order to get a manageable notation we put $\lambda=\mu+2\rho$. Replacing the function f by the truncated function f_λ yields, according to Lemma 5.5, a total error of $O_\varepsilon\left(q^{(2+\varepsilon)(\mu+\nu)-\rho}\right)$. Hence we obtain

$$|S|^2\ll_\varepsilon q^{(2+\varepsilon)(\mu+\nu)-\rho}+q^{\mu+\nu}\max_{1\leqslant|r|<q^\rho}S_2(r,\mu,\nu,\rho),\tag{5.13}$$

where we put

$$S_2(r,\mu,\nu,\rho)=\sum_{q^{\nu-1}<n\leqslant q^\nu}\left|\sum_{q^{\mu-1}<m\leqslant q^\mu}\mathrm{e}\left(f_\lambda(m(n+r))-f_\lambda(mn)\right)\right|.$$

Our next goal is to show that

$$S_2(r,\mu,\nu,\rho)\ll_q(\mu+\nu)^2q^{\mu+\nu-\rho}.\tag{5.14}$$

Therefore we are going to use in a first lemma the important property of f_λ to be periodic of period q^λ. It will allow us to apply the theory of trigonometric products introduced in Chapter 3.

Lemma 5.6 *With the same notation and assumptions as before, we have*

$$\begin{aligned}S_2\ll_q(1+q^{\nu-\lambda})\sum_{d\mid q^\lambda}d\sum_{0\leqslant a<d}\min\left(q^\mu,\frac{1}{\sin\left(\pi\frac{d}{q^\lambda}\left\|\frac{ar}{d}\right\|\right)}\right)\left(\sum_{\substack{0\leqslant h<q^\lambda\\ h\equiv a \bmod d}}|F_\lambda(h,\alpha)|\right)^2\\ +\lambda(1+q^{\nu-\lambda})q^\lambda\left(\sum_{0\leqslant h<q^\lambda}|F_\lambda(h,\alpha)|\right)^2.\end{aligned}\tag{5.15}$$

Proof. Setting $S_2'(n)=\sum_{q^{\mu-1}<m\leqslant q^\mu}\mathrm{e}\left(f_\lambda(m(n+r))-f_\lambda(mn)\right)$, we derive ($f_\lambda$ is periodic of period q^λ)

$$\begin{aligned}S_2'(n)=\frac{1}{q^{2\lambda}}\sum_{0\leqslant u_1<q^\lambda}\sum_{0\leqslant u_2<q^\lambda}\mathrm{e}\left(f_\lambda(u_1)-f_\lambda(u_2)\right)\\ \sum_{0\leqslant h_1<q^\lambda}\sum_{0\leqslant h_2<q^\lambda}\sum_{q^{\mu-1}<m\leqslant q^\mu}\mathrm{e}\left(\frac{h_1(m(n+r)-u_1)+h_2(mn-u_2)}{q^\lambda}\right).\end{aligned}$$

Now we can use the definition of the Fourier transform $|F_\lambda(h,\alpha)|$ (see Chapter 3) to obtain

$$S_2'(n) = \sum_{0\leqslant h_1<q^\lambda} \sum_{0\leqslant h_2<q^\lambda} F_\lambda(h_1,\alpha)\overline{F_\lambda(-h_2,\alpha)} \sum_{q^{\mu-1}<m\leqslant q^\mu} \mathrm{e}\left(\frac{(h_1+h_2)mn+h_1mr}{q^\lambda}\right).$$

The last sum is a geometric series in m and we get

$$|S_2'(n)| \leqslant \sum_{0\leqslant h_1<q^\lambda} \sum_{0\leqslant h_2<q^\lambda} |F_\lambda(h_1,\alpha)F_\lambda(-h_2,\alpha)| \min\left(q^\mu, \frac{1}{\left|\sin\left(\pi\frac{(h_1+h_2)n+h_1r}{q^\lambda}\right)\right|}\right).$$

Since $|S_2| = \sum_{q^{\nu-1}<n\leqslant q^\nu} |S_2'(n)|$, we have to sum the last expression over n. In order to be able to employ Lemma 2.1, we sum in blocks of length q^λ (and add a few terms if $\nu < \lambda$). Arranging the summation over the values of $d = (h_1+h_2, q^\lambda)$ therefore yields

$$\begin{aligned} S_2 \ll (1+q^{\nu-\lambda}) \sum_{d|q^\lambda} \sum_{\substack{0\leqslant h_1,h_2<q^\lambda \\ (h_1+h_2,q^\lambda)=d}} |F_\lambda(h_1,\alpha)F_\lambda(-h_2,\alpha)| d \min\left(q^\mu, \frac{1}{\sin\left(\pi\frac{d}{q^\lambda}\left\|\frac{h_1r}{d}\right\|\right)}\right) \\ + (1+q^{\nu-\lambda})q^\lambda \log(q^\lambda) \sum_{0\leqslant h_1,h_2<q^\lambda} |F_\lambda(h_1,\alpha)F_\lambda(-h_2,\alpha)|. \end{aligned}$$

Since the condition $(h_1+h_2, q^\lambda) = d$ is not easy to handle, we replace it by the less restrictive condition $h_1 + h_2 \equiv 0 \bmod d$. We can separate this condition into $h_1 \equiv a \bmod d$ and $h_2 \equiv -a \bmod d$, where a covers all residual classes modulo d. Furthermore, it is easy to see from the definition, that $|F_\lambda(h,\alpha)| = |F_\lambda(-h,\alpha)|$. Hence we obtain the desired result

$$\begin{aligned} S_2 \ll_q (1+q^{\nu-\lambda}) \sum_{d|q^\lambda} d \sum_{0\leqslant a<d} \min\left(q^\mu, \frac{1}{\sin\left(\pi\frac{d}{q^\lambda}\left\|\frac{ar}{d}\right\|\right)}\right) \left(\sum_{\substack{0\leqslant h<q^\lambda \\ h\equiv a \bmod d}} |F_\lambda(h,\alpha)|\right)^2 \\ + \lambda(1+q^{\nu-\lambda})q^\lambda \left(\sum_{0\leqslant h<q^\lambda} |F_\lambda(h,\alpha)|\right)^2. \end{aligned}$$

■

If $d \mid q^\lambda$, we have $d = kq^\delta$ where $\delta = \nu_q(d)$ and $k \mid q^{\lambda-\delta}$ but $k \nmid q$. According to Lemma 3.10 for $q \geqslant 3$ and Lemma 3.11 for $q = 2$, we have

$$\sum_{\substack{0\leqslant h<q^\lambda \\ h\equiv a \bmod kq^\delta}} |F_\lambda(h,\alpha)| \ll k^{-\eta_3} q^{\eta_3(\lambda-\delta)} |F_\delta(a,\alpha)|.$$

Here we used the fact, that $k = 1$ if $q = 2$ and that $\eta_2 < 0,4429 < 0,4649 < \eta_3$. For our further studies we define the constant

$$c_q(\alpha) = \frac{\pi^2}{102\log q}\left(1-\frac{2}{q+1}\right)\|(q-1)\alpha\|^2,$$

which depends on q and α. We recall that $(q-1)\alpha \notin \mathbb{Z}$ and hence $0 < \|(q-1)\alpha\| \leqslant 1/2$. Thus we have

$$0 < c_q(\alpha) \leqslant \frac{\pi^2}{102\cdot 4}\frac{1}{\log q} \leqslant \frac{\pi^2}{102\cdot 4\log 2} < 0,0349, \tag{5.16}$$

and consequently

$$\frac{1-c_q(\alpha)}{2} \geqslant \frac{1-0,0349}{2} = 0,48255 \geqslant \eta_3.$$

Hence we can write

$$\sum_{\substack{0\leqslant h<q^\lambda \\ h\equiv a \bmod kq^\delta}} |F_\lambda(h,\alpha)| \ll k^{-\eta_3} q^{\frac{1-c_q(\alpha)}{2}(\lambda-\delta)} |F_\delta(a,\alpha)|. \tag{5.17}$$

Mauduit and Rivat worked in [33] with η_3 when $q \geqslant 3$ and η_2 when $q = 2$. Using the constant $c_q(\alpha)$ yields a little worse result, but it makes it much easier to prove the proposition. Furthermore we can give an exact value of the constant used in (5.12). The key lemma, which makes it so comfortable to work with $c_q(\alpha)$, is Lemma 3.6. It was stated and proved by Mauduit and Rivat in [32]. Note, that $c_q(\alpha) < c_q\|(q-1)\alpha\|^2$, which will allow us to use Lemma 3.6 and Lemma 3.14 with $c_q(\alpha)$ instead of $c_q\|(q-1)\alpha\|^2$. If q is a prime, we could even use the constant η_q instead of η_3. Mauduit and Rivat derived for example a slightly better estimation of S_2 in case $q = 2$. Employing inequality (5.17) to (5.15) (note, that in the second term $\delta = 0$, $k = 1$ and that $|F_0(a,\alpha)| = 1$), we obtain

$$S_2 \ll_q (1+q^{\nu-\lambda}) \sum_{0\leqslant\delta\leqslant\lambda} \sum_{\substack{k|q^{\lambda-\delta} \\ (k,q)<q}} k^{1-2\eta_3} q^{\delta+(1-c_q(\alpha))(\lambda-\delta)} \sum_{0\leqslant a<d} \min\left(q^\mu, \frac{1}{\sin\left(\pi k q^{\delta-\lambda}\left\|\frac{ar}{kq^\delta}\right\|\right)}\right) |F_\delta(a,\alpha|^2$$
$$+ \lambda(1+q^{\nu-\lambda}) q^{(2-c_q(\alpha))\lambda}.$$

Before we study the sum over a, we prove the following lemma in order to eliminate the factor $k^{1-2\eta_3}$. Note that if q is prime, then $k = 1$ and the statement of the lemma is trivial.

Lemma 5.7 *Let η_3, δ and λ be as already defined. For $\omega_q = \left(\frac{1}{2}-\eta_3\right)\frac{\log 2}{\log q}$, we have*

$$q^{\delta+2\eta_3(\lambda-\delta)} \sum_{\substack{k|q^{\lambda-\delta} \\ (k,q)<q}} k^{1-2\eta_3} \ll_q q^{\lambda-\omega_q(\lambda-\delta)}.$$

Proof. First, we note that k can be bounded with respect to q, λ and δ. Indeed, since (k,q) is a proper divisor of q it follows that $(k,q) \leqslant q/2$. But this implies $k = (k, q^{\lambda-\delta}) \leqslant (k,q)^{\lambda-\delta} \leqslant (q/2)^{\lambda-\delta}$. Furthermore, we can also give an upper bound of the number of admissible integers k. It is clearly bounded by the number of divisors of $q^{\lambda-\delta}$. Hence Lemma A.2 shows that the number of considered integers k is bounded by $\tau(q^{\lambda-\delta}) \ll_q q^{\omega_q(\lambda-\delta)}$. Using this facts, we finally have

$$q^{\delta+2\eta_3(\lambda-\delta)} \sum_{\substack{k|q^{\lambda-\delta} \\ (k,q)<q}} k^{1-2\eta_3} \ll_q q^{\delta+2\eta_3(\lambda-\delta)} q^{\omega_q(\lambda-\delta)} \left(\frac{q}{2}\right)^{(1-2\eta_3)(\lambda-\delta)} \ll_q q^{\lambda+\omega_q(\lambda-\delta)-2\omega_q(\lambda-\delta)} \ll_q q^{\lambda-\omega_q(\lambda-\delta)}.$$

■

We obtain from (5.16) and from the fact that $\eta_3 < 0,465$ (see Lemma 3.8) that

$$c_q(\alpha) \leqslant \frac{\pi^2}{102\cdot 4}\frac{1}{\log q} < 0,0242\frac{1}{\log q} < 0,02426\frac{1}{\log q} < \left(\frac{1}{2}-\eta_3\right)\frac{\log 2}{\log q} = \omega_q.$$

Using this fact, we can write

$$S_2 \ll_q (1+q^{\nu-\lambda}) q^\lambda \sum_{0\leqslant\delta\leqslant\lambda} q^{-c_q(\alpha)(\lambda-\delta)} \max_{\substack{k|q^{\lambda-\delta} \\ (k,q)<q}} S_3(k,\delta) + \lambda(1+q^{\nu-\lambda}) q^{(2-c_q(\alpha))\lambda}, \tag{5.18}$$

with

$$S_3(k,\delta) = \sum_{0\leqslant a<kq^\delta} |F_\delta(a,\alpha)|^2 \min\left(q^\mu, \frac{1}{\sin\left(\pi kq^{\delta-\lambda}\left\|\frac{ar}{kq^\delta}\right\|\right)}\right).$$

Our next step is to find an upper bound of $S_3(k,\delta)$. Since the function sin is concave on $[0,\pi]$ and $1 \leqslant k \leqslant q^{\lambda-\delta}$, we have

$$\sin\left(\pi kq^{\delta-\lambda}\left\|\frac{ar}{kq^\delta}\right\|\right) \geqslant kq^{\delta-\lambda}\sin\left(\pi\left\|\frac{ar}{kq^\delta}\right\|\right) = kq^{\delta-\lambda}\left|\sin\frac{\pi ar}{kq^\delta}\right|.$$

Thus, we obtain

$$S_3(k,\delta) \leqslant k^{-1}q^{\lambda-\delta}\sum_{0\leqslant a<kq^\delta} |F_\delta(a,\alpha)|^2 \min\left(kq^{\delta-2\rho}, \frac{1}{\left|\sin\frac{\pi ar}{kq^\delta}\right|}\right).$$

The next lemma provides an upper estimation of $S_3(k,\delta)$, which will be important to prove the proposition in the case that δ is small.

Lemma 5.8 *We have for all $k \mid q^{\lambda-\delta}$ with $k \nmid q$ and for all $0 \leqslant \delta \leqslant \lambda$*

$$S_3(k,\delta) \ll_q \lambda q^\lambda. \tag{5.19}$$

Proof. To prove this lemma we use that $F_\delta(.,\alpha)$ is q^δ-periodic. This puts us in the situation of employing Lemma 2.1 with $m = k$, $n = i$, $a = r$ and $b = (ar)/q^\delta$. But since troubles arise from the common factors of r and q, we only use the crudely estimation $\min(kq^{\delta-2\rho}, (\sin\pi(r,k)/k\|(ar)/((r,k)q^\delta)\|)^{-1}) \leqslant kq^{\delta-2\rho}$,

$$\begin{aligned} S_3(k,\delta) &\leqslant k^{-1}q^{\lambda-\delta}\sum_{0\leqslant a<q^\delta} |F_\delta(a,\alpha)|^2 \sum_{0\leqslant i<k} \min\left(kq^{\delta-2\rho}, \frac{1}{\left|\sin\frac{\pi(a+iq^\delta)r}{kq^\delta}\right|}\right) \\ &\ll k^{-1}q^{\lambda-\delta}\sum_{0\leqslant a<q^\delta} |F_\delta(a,\alpha)|^2 \left((r,k)kq^{\delta-2\rho} + k\log k\right). \end{aligned}$$

Using Lemma 3.13 with $\lambda = \delta$ and $\delta = 0$, the sum above is bounded by 1. Taking into account that $(r,k) \leqslant r \leqslant q^\rho$ and $k \leqslant q^\lambda$, we finally obtain

$$S_3(k,\delta) \ll q^{\lambda-\delta}(q^{\delta-\rho} + \lambda\log q) \ll_q \lambda q^\lambda.$$

■

Now we have the problem, that if we sum (5.19) over δ from 0 to λ (see (5.18)), we do not get a useful upper bound (even if we use the better estimation $S_3(k,\delta) \ll q^{\lambda-\delta}(q^{\delta-\rho} - \lambda\log q)$, which we have actually proved). Hence, we have to find a better bound for large values of δ. If we set

$$\Delta = \left\lfloor \rho\frac{\log q}{\log 2}\right\rfloor,$$

we will see later, that this choice of Δ is already sufficient, that the sum over δ in (5.18) from 0 to Δ yields a negligible upper bound. In fact, we have

$$c_q(\alpha)\Delta \leqslant 0,0242\frac{1}{\log q}\Delta \leqslant 0,0242\frac{1}{\log q}\frac{\log q}{\log 2}\rho \leqslant \rho, \tag{5.20}$$

which will be the crucial condition. Furthermore, the definition of Δ allows as to state the following lemma.

Lemma 5.9 *We have for all $k \mid q^{\lambda-\delta}$ with $k \nmid q$ and for all $\Delta < \delta \leqslant \lambda$*

$$S_3(k,\delta) \ll_q \lambda q^{\lambda - c_q(\alpha)\delta+\rho}. \tag{5.21}$$

Proof. Setting $\delta' = \delta - \Delta$, we can employ the Euclidean algorithm to get

$$S_3(k,\delta) \leqslant k^{-1}q^{\lambda-\delta} \sum_{0\leqslant a<q^{\delta'}} \sum_{0\leqslant i<kq^{\Delta}} |F_\delta(a+iq^{\delta'},\alpha)|^2 \min\left(kq^{\delta-2\rho}, \frac{1}{\left|\sin \pi \frac{(a+iq^{\delta'})r}{kq^{\delta}}\right|}\right).$$

We have $|F_\delta(.,\alpha)| \leqslant |F_{\delta'}(.,\alpha)|$ trivially by (3.2) and Lemma 3.1. Since $F_{\delta'}(.,\alpha)$ is periodic of period $q^{\delta'}$, we get

$$S_3(k,\delta) \leqslant k^{-1}q^{\lambda-\delta} \sum_{0\leqslant a<q^{\delta'}} |F_{\delta'}(a,\alpha)|^2 \sum_{0\leqslant i<kq^{\Delta}} \min\left(kq^{\delta-2\rho}, \frac{1}{\left|\sin \pi \frac{ir+\frac{qr}{q^{\delta'}}}{kq^{\Delta}}\right|}\right).$$

Now we can again employ Lemma 2.1, but this time with $m = kq^{\Delta}$, $n = i$, $a = r$ and $b = (ar)/q^{\delta'}$.

$$S_3(k,\delta) \ll k^{-1}q^{\lambda-\delta} \sum_{0\leqslant a<q^{\delta'}} |F_{\delta'}(a,\alpha)|^2 \left((r,kq^{\Delta}) \min\left(kq^{\delta-2\rho}, \frac{1}{\sin \pi \frac{(r,kq^{\Delta})}{kq^{\Delta}} \left\|\frac{ar}{(r,kq^{\Delta})q^{\delta'}}\right\|}\right) + kq^{\Delta}\log(kq^{\Delta})\right).$$

Taking $r' = \frac{r}{(r,kq^{\Delta})}$ and using that $(r,kq^{\Delta}) \leqslant r < q^{\rho}$, $kq^{\Delta} \leqslant q^{\lambda-\delta+\Delta} \leqslant q^{\lambda}$ and again the concavity of sin on $[0,\pi]$, we obtain

$$\begin{aligned} S_3(k,\delta) &\ll k^{-1}q^{\lambda-\delta} \sum_{0\leqslant a<q^{\delta'}} |F_{\delta'}(a,\alpha)|^2 \left(kq^{\Delta} \min\left((r,kq^{\Delta})q^{\delta-2\rho-\Delta}, \frac{1}{\left|\sin \pi \frac{ar'}{q^{\delta'}}\right|}\right) + kq^{\Delta}\log(q^{\lambda})\right) \\ &\ll_q q^{\lambda-\delta'} \sum_{0\leqslant a<q^{\delta'}} |F_{\delta'}(a,\alpha)|^2 \min\left(q^{\delta'-\rho}, \frac{1}{\left|\sin \pi \frac{ar'}{q^{\delta'}}\right|}\right) + \lambda q^{\lambda-\delta'} \sum_{0\leqslant a<q^{\delta'}} |F_{\delta'}(a,\alpha)|^2. \end{aligned}$$

The sum in the second term is, by Lemma 3.13, equal to 1 (take $\lambda = \delta'$ and $\delta = 0$). If a is 0 in the first term, then the minimum is $q^{\delta'-\rho}$ and by Lemma 3.6, we have $|F_{\delta'}(0,\alpha)| \ll q^{-c_q(\alpha)\delta'}$ (note, that $c_q(\alpha) \leqslant c_q\|(q-1)\alpha\|^2$). Thus we can write

$$\begin{aligned} S_3(k,\delta) &\ll_q q^{\lambda-\delta'} \sum_{1\leqslant a<q^{\delta'}} |F_{\delta'}(a,\alpha)|^2 \min\left(q^{\delta'-\rho}, \frac{1}{\left|\sin \pi \frac{ar'}{q^{\delta'}}\right|}\right) + q^{\lambda-\rho-2c_q(\alpha)\delta'} + \lambda q^{\lambda-\delta'} \\ &\ll_q q^{\lambda-\delta'} \sum_{1\leqslant a<q^{\delta'}} |F_{\delta'}(a,\alpha)|^2 \min\left(q^{\delta'-\rho}, \frac{1}{\left|\sin \pi \frac{ar'}{q^{\delta'}}\right|}\right) + \lambda q^{\lambda-c_q(\alpha)\delta'}. \end{aligned}$$

Next we claim that $(r',q) = 1$. Indeed, if p is a prime with $p^{\nu} \mid r$, then $p^{\nu} = q^{\nu\frac{\log p}{\log q}} \leqslant q^{\rho}$, since $r \leqslant q^{\rho}$. Therefore, we get $\nu \leqslant \rho\frac{\log q}{\log p} \leqslant \rho\frac{\log q}{\log 2}$ and hence $\nu \leqslant \Delta$. Thus, we have $(r',q) = (r(r,kq^{\Delta})^{-1},q) = (r,kq^{\Delta})^{-1}(r,q(r,kq^{\Delta})) = (r,kq^{\Delta})^{-1}(r,qr,kq^{\Delta+1}) = 1$.

This implies that the *sin* term cannot be zero. Organizing the summation on a according to the powers of q by taking $a = q^\theta b$, we can write

$$S_3(k,\delta) \ll_q q^{\lambda-\delta'} \sum_{0\leqslant\theta<\delta'} \sum_{\substack{1\leqslant b\leqslant q^{\delta'-\theta}\\ b\not\equiv 0 \bmod q}} \frac{|F_{\delta'}(q^\theta b,\alpha)|^2}{\left|\sin \pi \frac{br'}{q^{\delta'-\theta}}\right|} + \lambda q^{\lambda - c_q(\alpha)\delta'}.$$

Lemma 3.2 gives us $|F_{\delta'}(q^\theta b,\alpha)| \leqslant |F_{\delta'-\theta}(b,\alpha)|$ and employing Lemma 3.14 yields

$$\sum_{\substack{1\leqslant b\leqslant q^{\delta'-\theta}\\ b\not\equiv 0 \bmod q}} \frac{|F_{\delta'-\theta}(b,\alpha)|^2}{\left|\sin \pi \frac{br'}{q^{\delta'-\theta}}\right|} \ll q^{(1-c_q(\alpha))(\delta'-\theta)}.$$

Thus,

$$\begin{aligned} S_3(k,\delta) &\ll_q q^{\lambda-\delta'} \sum_{0\leqslant\theta<\delta'} q^{(1-c_q(\alpha))(\delta'-\theta)} + \lambda q^{\lambda - c_q(\alpha)\delta'} \\ &\ll_q q^{\lambda-c_q(\alpha)\delta'} + \lambda q^{\lambda-c_q(\alpha)\delta'} \ll_q \lambda q^{\lambda - c_q(\alpha)(\delta-\Delta)}. \end{aligned}$$

Using $c_q(\alpha)\Delta \leqslant \rho$ (see (5.20)), we finally obtain our desired result. ∎

Proof (of Proposition 5.2). Now we can derive the desired upper bound of S_2 (see (5.14)). Using (5.18) and the upper bounds of $S_3(k,\delta)$ (see (5.19) and (5.21)), we have

$$\begin{aligned} S_2 &\ll_q (1+q^{\nu-\lambda})q^\lambda \sum_{0\leqslant\delta\leqslant\lambda} q^{-c_q(\alpha)(\lambda-\delta)} \max_{\substack{k|q^{\lambda-\delta}\\ (k,q)<q}} S_3(k,\delta) + \lambda(1+q^{\nu-\lambda})q^{(2-c_q(\alpha))\lambda} \\ &\ll_q (1+q^{\nu-\lambda})q^\lambda \left(\sum_{0\leqslant\delta\leqslant\Delta} q^{-c_q(\alpha)(\lambda-\delta)}\lambda q^\lambda + \sum_{\Delta<\delta\leqslant\lambda} q^{-c_q(\alpha)(\lambda-\delta)}\lambda q^{\lambda-c_q(\alpha)\delta+\rho}\right) + \lambda(1+q^{\nu-\lambda})q^{(2-c_q(\alpha))\lambda}. \end{aligned}$$

Calculating the geometric series, using again $c_q(\alpha)\Delta \leqslant \rho$ and the definition of λ ($\lambda = \mu + 2\rho \leqslant \mu + \nu$), we obtain

$$\begin{aligned} S_2 &\ll_q \lambda(1+q^{\nu-\lambda})q^{(2-c_q(\alpha))\lambda}\left(q^{c_q(\alpha)\Delta} + \lambda q^\rho\right) \\ &\ll_q \lambda^2(1+q^{\nu-\lambda})q^{(2-c_q(\alpha))\lambda+\rho} \\ &\ll_q (\mu+\nu)^2\left(q^{(2-c_q(\alpha))\mu+(5-2c_q(\alpha))\rho} + q^{(1-c_q(\alpha))\mu+\nu+(3-2c_q(\alpha))\rho}\right) \\ &\ll_q (\mu+\nu)^2\left(q^{(2-c_q(\alpha))\mu+5\rho} + q^{(1-c_q(\alpha))\mu+\nu+3\rho}\right). \end{aligned}$$

To show (5.14) ($S_2 \ll (\mu+\nu)^2 q^{\mu+\nu-\rho}$), the inequalities

$$(2-c_q(\alpha))\mu + 5\rho \leqslant \mu+\nu-\rho \quad \text{and} \quad (1-c_q(\alpha))\mu + \nu + 3\rho \leqslant \mu+\nu-\rho$$

have to be satisfied. It is easy to see that these conditions are true if

$$\frac{4\frac{\rho}{\mu+\nu}}{c_q(\alpha)} \leqslant \frac{\mu}{\mu+\nu} \leqslant \frac{1-6\frac{\rho}{\mu+\nu}}{2-c_q(\alpha)}. \tag{5.22}$$

Now we can fix the still undefined parameters. Set $\xi_q(\alpha) = \frac{c_q(\alpha)^2}{24}$, $\delta = \frac{c_q(\alpha)}{4(2-c_q(\alpha))}$, $\beta_1 = \frac{4\xi_q(\alpha)}{c_q(\alpha)} + \delta$, $\beta_2 = \frac{1-6\xi_q(\alpha)}{2-c_q(\alpha)} - \delta$ and finally $\rho = \lfloor \xi_q(\alpha)(\mu+\nu)\rfloor$.

All pairs (μ,ν) satisfying $\beta_1-\delta \leqslant \mu/(\mu+\nu) \leqslant \beta_2+\delta$ also satisfy (5.22). Using the upper bound of $c_q(\alpha)$ (see (5.16)) and $\mu \leqslant \nu(\beta_2+\delta)/(1-(\beta_2+\delta))$, it can be readily shown that $\rho \leqslant \nu/2$. Furthermore we have for all pairs (μ,ν) (see (5.13))

$$\begin{aligned}|S|^2 &\ll_\varepsilon q^{(2+\varepsilon)(\mu+\nu)-\rho} + q^{\mu+\nu}\max_{1\leqslant|r|<q^\rho} S_2(r,\mu,\nu,\rho)\\ &\ll_{q,\varepsilon} q^{(2+\varepsilon)(\mu+\nu)-\rho} + q^{\mu+\nu}(\mu+\nu)^2 q^{\mu+\nu-\rho}\\ &\ll_{q,\varepsilon} q^{(2+\varepsilon)(\mu+\nu)-\rho}\\ &\ll_{q,\varepsilon} q^{(2+\xi_q(\alpha)+\varepsilon)(\mu+\nu)}.\end{aligned}$$

Hence, the proof of Proposition 5.2 is finished, since the following inequalities can be easily derived from the definitions of δ,β_1 and β_2

$$0<\delta<\beta_1<\frac{c_q\|(q-1)\alpha\|^2}{2} \quad \text{and } \frac{1}{2}<\beta_2<1.$$

■

Corollary 5.1 *Let $q\geqslant 2$ be an integer, α a real number, such that $(q-1)\alpha\in\mathbb{R}\setminus\mathbb{Z}$ and $c_q(\alpha)=\frac{\pi^2}{102\log q}\left(1-\frac{2}{q+1}\right)\|(q-1)\alpha\|^2$. If $x>q^{3/\delta}$, then we have for $x^{\beta_1}\leqslant M\leqslant x^{\beta_2}$*

$$\left|\sum_{\frac{M}{q}<m\leqslant M}\sum_{\frac{x}{qm}<n\leqslant\frac{x}{m}} a_m b_n g(mn)\right| \ll_{q,\alpha} x^{1-\sigma'_q(\alpha)},$$

where $\sigma'_q(\alpha)=\frac{199}{200}\frac{c_q(\alpha)^2}{48}$, $\beta_1=\frac{4\xi_q(\alpha)}{c_q(\alpha)}+\delta$, $\beta_2=\frac{1-6\xi_q(\alpha)}{2-c_q(\alpha)}-\delta$ and $\delta=\frac{c_q(\alpha)}{4(2-c_q(\alpha))}$. Furthermore, these constants satisfy $0<\beta_1<c_q\|(q-1)\alpha\|^2<1/3$ and $1/2<\beta_2<1$, where $c_q=\frac{\pi^2}{12\log q}\left(1-\frac{2}{q+1}\right)$.

Proof. Define δ, β_1, β_2 and $\xi_q(\alpha)$ as in the proof of the last proposition. We have $\beta_2<1-\delta$ and hence $1/(1-\beta_2)<1/\delta<3/\delta$. Thus, Corollary 5.1 is the direct consequence of Proposition 5.2 and Lemma 5.3. We obtain

$$\left|\sum_{\frac{M}{q}<m\leqslant M}\sum_{\frac{x}{qm}<n\leqslant\frac{x}{m}} a_m b_n g(mn)\right| \ll_{q,\varepsilon} (\log x) q^{(1-\frac{\xi_q(\alpha)}{2}+\varepsilon)(\mu+\nu)} \ll_{q,\varepsilon} (\log x) x^{1-\frac{\xi_q(\alpha)}{2}+\varepsilon},$$

as soon as $x>x_0=q^{3/\delta}$. Here we used that we only need to consider μ and ν satisfying $q^{\mu+\nu}\ll_q x$ (see Lemma 5.3). Setting $\sigma'_q(\alpha)=\frac{199}{200}\frac{\xi_q(\alpha)}{2}$, we finally obtain

$$\left|\sum_{\frac{M}{q}<m\leqslant M}\sum_{\frac{x}{qm}<n\leqslant\frac{x}{m}} a_m b_n g(mn)\right| \ll_{q,\alpha} x^{1-\sigma'_q(\alpha)}.$$

■

5.5 Proof of Theorem 5.1

Let us define $c_q(\alpha)$, δ, β_1 and β_2 as in Corollary 5.1 and set $k_0=\left\lfloor\frac{\log x}{\log q}-\frac{3}{\delta}-1\right\rfloor$. If we assume that $x>q^{3/\delta}$, we can write

$$\sum_{n\leqslant x}\Lambda(n)\mathrm{e}\left(\alpha s_q(n)\right)=\sum_{n\leqslant\frac{x}{q^{k_0+1}}}\Lambda(n)\mathrm{e}\left(\alpha s_q(n)\right)+\sum_{k=0}^{k_0}\sum_{\frac{x}{q^{k+1}}<n\leqslant\frac{x}{q^k}}\Lambda(n)\mathrm{e}\left(\alpha s_q(n)\right).$$

Since we have for $k \leqslant k_0$

$$\frac{x}{q^k} \geqslant \frac{x}{q^{k_0}} > \frac{x}{q^{-\frac{3}{\delta}}x} = q^{\frac{3}{\delta}} = q^{\frac{12(2-c_q(\alpha))}{c_q(\alpha)}} \geqslant q^{\frac{4(2-c_q(\alpha))}{c_q(\alpha)(1-c_q(\alpha))}} = q^{\frac{1}{\beta_2-1/2}},$$

we can use Proposition 5.1 (type I sums) and Corollary 5.1 (type II sums) to employ Lemma 5.1 with β_1 and β_2 as defined and x/q^k instead of x. We finally obtain

$$\begin{aligned}\sum_{n\leqslant x}\Lambda(n)\mathrm{e}\left(\alpha s_q(n)\right) &\ll_{q,\alpha} (\log x)\frac{x}{q^{k_0+1}} + \sum_{k=0}^{k_0}\left(\log\left(\frac{x}{q^k}\right)\right)^2\left(\frac{x}{q^k}\right)^{1-\sigma_q'(\alpha)}\\ &\ll_{q,\alpha} \log x + (\log x)^2\, x^{1-\sigma_q'(\alpha)}\sum_{k=0}^{k_0} q^{-k(1-\sigma_q'(\alpha))}\\ &\ll_{q,\alpha} (\log x)^2\, x^{1-\sigma_q'(\alpha)}\\ &\ll_{q,\alpha} x^{1-\sigma_q(\alpha)},\end{aligned}$$

where $\sigma_q'(\alpha)$ is defined in Corollary 5.1 and $\sigma_q(\alpha) = \frac{198}{199}\sigma_q'(\alpha) = \frac{99}{100}\frac{c_q(\alpha)^2}{48}$. This finally ends the proof of Theorem 5.1. ∎

Remark. It follows from the proof of Theorem 5.1, that we can choose

$$\sigma_q(\alpha) = \frac{99}{100}\frac{1}{48}\left(\frac{\pi^2}{102\log q}\left(1-\frac{2}{q+1}\right)\|(q-1)\alpha\|^2\right)^2.$$

As already mentioned before, we can essentially improve this constant by using a better estimation for type I sums. Actually, using the estimates Mauduit and Rivat derived in their work (and Lemma 3.6), we only have to make β_1 smaller than $1/3$ instead of $c_q\|(q-1)\|^2$. This allows us to choose $\xi_q(\alpha)$ in the proof of Theorem 5.1 as $\xi_q(\alpha) = c_q(\alpha)/25$, which finally yields to $\sigma_q(\alpha) = \frac{99}{100}\frac{1}{50}\frac{\pi^2}{102\log q}\left(1-\frac{2}{q+1}\right)\|(q-1)\alpha\|^2$.

Chapter 6

The Sum of Digits Function of Squares

6.1 Main Theorems

The main contribution of Mauduit's and Rivat's work is the following theorem, which is the analogous statement to Theorem 5.1.

Theorem 6.1 (Mauduit, Rivat) *Let $q \geqslant 2$ be an integer and α a real number with $(q-1)\alpha \in \mathbb{R} \setminus \mathbb{Z}$. Then there exists a constant $\sigma_q(\alpha) > 0$, such that*

$$\sum_{n \leqslant x} \mathrm{e}\left(\alpha s_q\left(n^2\right)\right) = O_{q,\alpha}(x^{1-\sigma_q(\alpha)}). \tag{6.1}$$

The proof of this theorem given in Section 6.2 – Section 6.5 is emulated Mauduit's and Rivat's work [32]. Contrary to them, we do not care about the constant depending on q and α, which yields a more assessable proof. Furthermore we obtain an insignificant worse exponent $\sigma_q(\alpha)$ than Mauduit and Rivat to shorten the proof. In particular, they showed

$$\left|\sum_{n \leqslant x} \mathrm{e}\left(\alpha s_q\left(n^2\right)\right)\right| \leqslant 4q^{7/2}(\log q)^{5/2}\tau(q)^{5/2}\left(1+\frac{x}{q}\right)^{\frac{1}{2}\omega(q)+4} x^{1-\sigma_q(\alpha)},$$

where $\omega(q)$ denotes the number of distinct prime factors of q (see [32]).

The proof is organized as follows. In Section 6.2, we use the Cauchy-Schwarz inequality and a variant of van der Corput's inequality to be able to work with the truncated sum of digits function (similar to the work on the prime numbers - see Chapter 5). But different to the previous chapter, we also have to use the notion of double truncated functions. Well known results on Gauss sums allow us to concentrate on sums of Fourier transforms of these double truncated functions, in order to be able to prove the theorem (Section 6.3 and Section 6.4). Adding the obtained facts together, we finally prove the theorem in Section 5.5.

Before we start the proof, we present the solution of Gelfond's problem concerning the sum of digits function of squares, which is a direct consequence of Theorem 5.1. Furthermore, we show that the sequence $(\alpha s_q(n^2))_{n\in\mathbb{N}}$ is uniformly distributed modulo 1 for any irrational number α.

Theorem 6.2 *Let q and m be integers $\geqslant 2$. Set $d = (q-1, m)$ and $Q(a,d) = \#\{0 \leqslant n < d : n^2 \equiv a \bmod d\}$. Then there exists a constant $\sigma_{q,m} > 0$ such that for all $a \in \mathbb{Z}$*

$$\#\{n \leqslant x : s_q(n^2) \equiv a \bmod m\} = \frac{x}{m}Q(a,d) + O_{q,m}\left(x^{1-\sigma_{q,m}}\right). \tag{6.2}$$

Proof. By Lemma 1.2 we have

$$\#\{n \leqslant x : s_q(n^2) \equiv a \bmod m\} = \sum_{n\leqslant x} \frac{1}{m} \sum_{0\leqslant j<m} \mathrm{e}\left(\frac{j}{m}(s_q(n^2)-a)\right).$$

If we put $d = (m, q-1)$, $m' = \frac{m}{d}$, $J = \{km' : 0 \leqslant k < d\}$, $J' = \{0, \dots, m-1\} \setminus J = \{km' + r : 0 \leqslant k < d, 1 \leqslant r < m'\}$, than we have for $j = km' \in J$

$$\mathrm{e}\left(\frac{j}{m}s_q(n^2)\right) = \mathrm{e}\left(\frac{km'}{dm'}s_q(n^2)\right) = \mathrm{e}\left(\frac{k}{d}s_q(n^2)\right) = \mathrm{e}\left(\frac{k}{d}n^2\right).$$

Indeed, Lemma 1.1 gives us $s_q(n^2) \equiv n^2 \bmod d$, which establishes the last equality. Hence,

$$\begin{aligned}\sum_{n\leqslant x} \frac{1}{m} \sum_{j\in J} \mathrm{e}\left(\frac{j}{m}(s_q(n^2)-a)\right) &= \sum_{n\leqslant x} \frac{1}{m} \sum_{0\leqslant k<d} \mathrm{e}\left(\frac{k}{d}(n^2-a)\right) = \frac{d}{m} \sum_{\substack{n\leqslant x \\ n^2\equiv a \bmod d}} 1 \\ &= \frac{d}{m}\left(\frac{x}{d} + O_{q,m}(1)\right) Q(a,d) = \left(\frac{x}{m} + O_{q,m}(1)\right) Q(a,d).\end{aligned}$$

If we can therefore show that

$$\frac{1}{m} \sum_{j\in J'} \mathrm{e}\left(-\frac{aj}{m}\right) \sum_{n\leqslant x} \mathrm{e}\left(\frac{j}{m}s_q(n^2)\right) = O_{q,m}(x^{1-\sigma_{q,m}}), \tag{6.3}$$

where $\sigma_{q,m} > 0$, we are done. If $J' = \emptyset$, which corresponds to the degenerated case where $m \mid q-1$, then we have an error term equal to zero. Therefore we assume now, that $J' \neq \emptyset$. Putting $q' = \frac{q-1}{d}$, we have $(q', m') = 1$, and hence for $j = km' + r \in J'$

$$\frac{(q-1)j}{m} = \frac{dq'(km'+r)}{dm'} = q'k + \frac{q'r}{m'} \notin \mathbb{Z}.$$

By Theorem 6.1 there exists a constant $\sigma_q(j/m)$ for every $j \in J'$, such that

$$\sum_{n\leqslant x} \mathrm{e}\left(\frac{j}{m}s_q(n^2)\right) = O_{q,m}(x^{1-\sigma_q(j/m)}).$$

Putting $\sigma_{q,m} = \min_{j\in J'} \sigma_q(j/m) > 0$ (recall, that $J' \neq \emptyset$), we get the desired estimation in 6.1. ∎

Theorem 6.3 *For $q \geqslant 2$ the sequence $(\alpha s_q(n^2))_{n\in\mathbb{N}}$ is uniformly distributed modulo 1, if and only if $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.*

Proof. If $\alpha \in \mathbb{Q}$, then the sequence $(\alpha s_q(n^2))_{n\in\mathbb{N}}$ takes modulo 1 only a finite number of values and is therefore not uniformly distributed modulo 1. If in return $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, then for every $h \in \mathbb{Z}$ with $h \neq 0$ we have $(q-1)h\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and according to Theorem 6.1 there exists a constant $\sigma_q(h\alpha) > 0$, such that

$$\left|\sum_{n\leqslant x} \mathrm{e}\left(\alpha s_q\left(n^2\right)\right)\right| = O_{q,h\alpha}(x^{1-\sigma_q(h\alpha)}).$$

This proves that $(\alpha s_q(n^2))_{n\in\mathbb{N}}$ is uniformly distributed modulo 1 (see Theorem A.3). ∎

6.2 Truncated Functions and Gauss Sums

In order to be able to show Theorem 6.1, we need the following proposition which is the hardest part of proving Gelfond's problem on the sum of digits function of squares.

Proposition 6.1 *There exist constants $\nu_0 = \nu_0(q,\alpha) \geqslant 1$ and $\sigma'_q(\alpha) > 0$, such that for all $\nu \geqslant \nu_0$*

$$\sum_{q^{\nu-1}<n\leqslant x} \mathrm{e}(\alpha s_q(n^2)) \ll_q \nu^{3\omega(q)/2} q^{(1-\sigma'_q(\alpha))\nu},$$

uniformly for all x satisfying $q^{\nu-1} < x \leqslant q^\nu$, where $\omega(q)$ denotes the number of distinct prime factors of q.

It needs several steps to prove this proposition. Recall that $f(.)$ is the sum of digits function in base q multiplied by α. In order to get a manageable notation, we set

$$S = \sum_{q^{\nu-1}<n\leqslant x} \mathrm{e}(f(n^2)).$$

First we smooth the sum by using a variant of Van der Corput's inequality. In particular, we employ Lemma 2.8 with $A = 1$, $B = \lfloor x \rfloor - q^{\nu-1}$, $N = q^\nu - q^{\nu-1}$, $z_n = \mathrm{e}(f((q^{\nu-1}+n)^2))$ and $R = q^\rho$, where ρ is an integer satisfying $2 \leqslant q \leqslant \nu/3$. We obtain

$$|S| \leqslant \left(\frac{\lfloor x \rfloor - q^{\nu-1}}{q^\rho} \sum_{|r|<q^\rho} \left(1 - \frac{|r|}{q^\rho}\right) \sum_{\substack{q^{\nu-1}<n\leqslant q^\nu \\ q^{\nu-1}<n+r\leqslant q^\nu}} \mathrm{e}(f((n+r)^2) - f(n^2)) \right)^{1/2} + \frac{q^\rho}{2}.$$

Taking into account that $\lfloor x \rfloor \leqslant q^\nu$ and separating the case $r = 0$ and $r \neq 0$, we get

$$|S| \leqslant q^{(\nu-\rho)/2} \left(q^\nu + \sum_{1\leqslant|r|<q^\rho} \left(1 - \frac{|r|}{q^\rho}\right) \sum_{\substack{q^{\nu-1}<n\leqslant q^\nu \\ q^{\nu-1}<n+r\leqslant q^\nu}} \mathrm{e}(f((n+r)^2) - f(n^2)) \right)^{1/2} + \frac{q^\rho}{2}.$$

We have $\sum_{1\leqslant|r|<q^\rho} \left(1 - \frac{|r|}{q^\rho}\right) = q^\rho - 1 \leqslant q^\rho$. Therefore we get an error term $\sum_{1\leqslant|r|<q^\rho} \left(1 - \frac{|r|}{q^\rho}\right)|r| \leqslant q^{2\rho}$ when removing the summation condition $q^{\nu-1} < n + r \leqslant q^\nu$. Since $\sqrt{a+b} \leqslant \sqrt{a} + \sqrt{b}$ for non-negative real numbers a and b, we obtain

$$\begin{aligned} |S| &\leqslant q^{\nu-\rho/2} + q^{(\nu+\rho)/2} + \frac{q^\rho}{2} + q^{\nu/2} \max_{1\leqslant|r|<q^\rho} \left| \sum_{q^{\nu-1}<n\leqslant q^\nu} \mathrm{e}(f((n+r)^2) - f(n^2)) \right|^{1/2} \\ &\ll q^{\nu-\rho/2} + q^{\nu/2} \max_{1\leqslant|r|<q^\rho} \left| \sum_{q^{\nu-1}<n\leqslant q^\nu} \mathrm{e}(f((n+r)^2) - f(n^2)) \right|^{1/2}. \end{aligned} \tag{6.4}$$

As in the proof of Theorem 5.1, we continue with using the notion of the truncated sum of digits function which was already used in Chapter 3 and Chapter 5. Similar to Lemma 5.5, we show in the following lemma that the digits of high weight in the difference $f((n+r)^2) - f(n^2)$ do not contribute significantly and are negligible.

Lemma 6.1 *For all integers ν and ρ with $\nu > 0$ and $2 \leqslant \rho \leqslant \nu/3$ and for all $r \in \mathbb{Z}$ with $|r| < q^\rho$, we denote by $E(r, \nu, \rho)$ the number of integers n such that $q^{\nu-1} < n \leqslant q^\nu$ and*

$$f((n+r)^2) - f(n^2) \neq f_{\nu+2\rho}((n+r)^2) - f_{\nu+2\rho}(n^2).$$

Then we have

$$E(r, \nu, \rho) \ll_q q^{\nu-\rho}.$$

Proof. First, we note that $0 \leqslant |2nr + r^2| < 2q^\nu(q^\rho - 1) + q^{2\rho} < q^{\nu+\rho+1}$. We start with considering the case $0 \leqslant r < q^\rho$. When we compute the sum $n^2 + 2nr + r^2$, the digits of n^2 of index $\geqslant \nu + \rho + 1$ cannot be modified unless there is a carry propagation. Hence we must count the number of integers n such that the digits a_j in basis q of n^2 satisfy $a_j = q - 1$ for $\nu + \rho + 1 \leqslant j < \nu + 2\rho$, or equivalent, that there exists an integer m, such that $\lfloor n^2/q^{\nu+\rho+1} \rfloor = q^{\rho-1}m - 1$. This can be readily verified, and is equivalent to

$$q^{\rho-1}m - 1 \leqslant \frac{n^2}{q^{\nu+\rho+1}} < q^{\rho-1}m. \tag{6.5}$$

Using this inequality, we derive (note, that $n \leqslant q^\nu$)

$$0 < \frac{n^2}{q^{\nu+2\rho}} < m \leqslant \left\lfloor \frac{n^2}{q^{\nu+2\rho}} + q^{-\rho+1} \right\rfloor \leqslant q^{\nu-2\rho}.$$

For each such fixed m, there can only be

$$1 + \sqrt{q^{\nu+2\rho}m}\left(1 - \sqrt{1 - q^{-\rho+1}m^{-1}}\right)$$

integers n satisfying (6.5). Since we have $1 - \sqrt{1-u} = \frac{u}{2} + \frac{1}{4}\int_0^u (u-t)(1-t)^{-3/2}\,dt \leqslant \frac{u}{2} + u^2$ for $0 \leqslant u \leqslant 3/4$ and $q^{-\rho+1}m^{-1} \leqslant 1/2$ ($m \geqslant 1,\ \nu \geqslant 2$), we obtain

$$\begin{aligned} E(r, \nu, \rho) &\leqslant \sum_{0<m\leqslant q^{\nu-2\rho}} \left(1 + \left(\frac{1}{2}q^{-\rho+1}m^{-1} + q^{-2\rho+2}m^{-2}\right)q^{\nu/2+\rho}m^{1/2}\right) \\ &\leqslant q^{\nu-2\rho} + \frac{q}{2}q^{\nu/2} \sum_{0<m\leqslant q^{\nu-2\rho}} \frac{1}{m^{1/2}} + q^2 q^{\nu/2-\rho} \sum_{0<m\leqslant q^{\nu-2\rho}} \frac{1}{m^{3/2}}. \end{aligned}$$

Since $x^{-1/2}$ is convex for positive x, we employ Lemma A.7 to obtain the estimation $\sum_{0<m\leqslant q^{\nu-2\rho}} \frac{1}{m^{1/2}} \leqslant 2q^{\nu/2-\rho}$. Thus, we finally get

$$E(r, \nu, \rho) \leqslant q^{\nu-2\rho} + qq^{\nu-\rho} + q^2 q^{\nu/2-\rho}\zeta(3/2) \ll_q q^{\nu-\rho}.$$

In the case that $-q^\rho < r < 0$, the same reasoning applies and similar calculations have to be done. We have to count the number of integers n such that the digits a_j in basis q of n^2 satisfy $a_j = 0$ for $\nu + \rho + 1 \leqslant j < \nu + 2\rho$. This is equivalent to the existence of an integer m, such that

$$q^{\rho-1}m \leqslant \frac{n^2}{q^{\nu+\rho+1}} < q^{\rho-1}m + 1, \tag{6.6}$$

and we obtain $0 \leqslant m \leqslant q^{\nu-2\rho}$. If $m \neq 0$, there are $1 + \sqrt{q^{\nu+2\rho}m}\left(\sqrt{1 + q^{-\rho+1}m^{-1}} - 1\right)$ integers n satisfying (6.6). Separating the case $m \neq 0$ from the rest of the sum and using the inequality $\sqrt{1+u} - 1 \leqslant$

$\frac{u}{2}$ for positive u, we finally obtain (by assumption, we have $\rho \leqslant \nu/3$)

$$\begin{aligned} E(r,\nu,\rho) &\leqslant q^{(\nu+\rho+1)/2} + \sum_{0<m\leqslant q^{\nu-2\rho}} \left(1 + \frac{q}{2} q^{\nu/2} m^{-1/2}\right) \\ &\leqslant q^{(\nu+\rho+1)/2} + q^{\nu-2\rho} + \frac{q}{2} q^{\nu/2} \sum_{0<m\leqslant q^{\nu-2\rho}} \frac{1}{m^{1/2}} \ll_q q^{\nu-\rho}. \end{aligned}$$

■

In order to get a manageable notation we put $\lambda = \nu + 2\rho$. Replacing the function f by the truncated function f_λ yields, according to Lemma 6.1, an error $\ll_q q^{\nu-\rho}$. By (6.4), we obtain

$$\begin{aligned} |S| &\ll q^{\nu-\rho/2} + q^{\nu/2} \max_{1\leqslant|r|<q^\rho} (|S_1(r,\nu,\rho)| + E(r,\nu,\rho))^{1/2} \\ &\ll_q q^{\nu-\rho/2} + q^{\nu/2} \max_{1\leqslant|r|<q^\rho} |S_1(r,\nu,\rho)|^{1/2}, \end{aligned} \tag{6.7}$$

where

$$S_1(r,\nu,\rho) = \sum_{q^{\nu-1}<n\leqslant q^\nu} \mathrm{e}\left(f_\lambda((n+r)^2) - f_\lambda(n^2)\right).$$

Our next step in proving the proposition is to use the double truncated sum of digits function $f_{\eta,\lambda} = f_\lambda - f_\eta$, which was treated in Chapter 3. In order to be able to work with this function, we employ a generalization of a Van der Corput inequality. Therefore we introduce a parameter η satisfying

$$1 \leqslant \eta \leqslant \nu - 2\rho - 1, \tag{6.8}$$

and set $N = q^\nu - q^{\nu-1}$, $R = q^{2\rho}$, $z_n = \mathrm{e}(f_\lambda((q^{\nu-1}+n+r)^2) - f_\lambda((q^{\nu-1}+n)^2))$ and $k = q^\eta$. Employing Lemma 2.7 yields to

$$\begin{aligned} |S_1(r,\nu,\rho)|^2 &\leqslant \frac{q^\nu - q^{\nu-1} + q^{\eta+2\rho}}{q^{2\rho}} \sum_{|s|<q^{2\rho}} \left(1 - \frac{|s|}{q^{2\rho}}\right) |S_2(r,s,\nu,\rho,\eta)| \\ &\leqslant q^{\nu-2\rho} \sum_{|s|<q^{2\rho}} \left(1 - \frac{|s|}{q^{2\rho}}\right) |S_2(r,s,\nu,\rho,\eta)| \\ &\leqslant q^{2(\nu-\rho)} + q^\nu \max_{1\leqslant|s|<q^{2\rho}} |S_2(r,s,\nu,\rho,\eta)|, \end{aligned} \tag{6.9}$$

where

$$S_2(r,s,\nu,\rho,\eta) = \sum_{\substack{q^{\nu-1}<n\leqslant q^\nu \\ q^{\nu-1}<n+sq^\eta\leqslant q^\nu}} \mathrm{e}\left(f_\lambda((n+r+sq^\eta)^2) - f_\lambda((n+r)^2) - f_\lambda((n+sq^\eta)^2) + f_\lambda(n^2)\right).$$

Here we separated (as in the other cases where we had employed a Van der Corput inequality) the case $s = 0$ and $s \neq 0$ and used the inequality $\sum_{1\leqslant|s|<q^{2\rho}} (1 - |s|/q^{2\rho}) \leqslant q^{2\rho}$. Since f_η is periodic of period q^η, we derive

$$f_\lambda((m+sq^\eta)^2) - f_\lambda(m^2) = f_{\eta,\lambda}((m+sq^\eta)^2) - f_{\eta,\lambda}(m^2).$$

Thus we can write

$$S_2(r,s,\nu,\rho,\eta) = \sum_{\substack{q^{\nu-1}<n\leqslant q^\nu \\ q^{\nu-1}<n+sq^\eta\leqslant q^\nu}} \mathrm{e}\left(f_{\eta,\lambda}((n+r+sq^\eta)^2) - f_{\eta,\lambda}((n+r)^2) - f_{\eta,\lambda}((n+sq^\eta)^2) + f_{\eta,\lambda}(n^2)\right).$$

Since the new function $f_{\eta,\lambda}$ is periodic of period q^λ, we have (by Lemma 1.2)

$$S_2 = \frac{1}{q^{4\lambda}} \sum_{0\leqslant u_1,u_2,u_3,u_4<q^\lambda} \mathrm{e}(f_{\eta,\lambda}(u_1) - f_{\eta,\lambda}(u_2) - f_{\eta,\lambda}(u_3) + f_{\eta,\lambda}(u_4)) \sum_{\substack{q^{\nu-1}<n\leqslant q^\nu \\ q^{\nu-1}<n+sq^\eta\leqslant q^\nu}} \sum_{0\leqslant h_1,h_2,h_3,h_4<q^\lambda} \mathrm{e}\left(\frac{h_1((n+r+sq^\eta)^2-u_1)+h_2((n+r)^2-u_2)+h_3((n+sq^\eta)^2-u_3)+h_4(n^2-u_4)}{q^\lambda}\right).$$

Using the definition $F_{\eta,\lambda}(h,\alpha) = q^{-\lambda}\sum_{0\leqslant u<q^\lambda} \mathrm{e}\left(f_{\eta,\lambda}(u) - huq^{-\lambda}\right)$ (see Chapter 3), we can write

$$S_2 = \sum_{0\leqslant h_1,h_2,h_3,h_4<q^\lambda} F_{\eta,\lambda}(h_1,\alpha)\overline{F_{\eta,\lambda}(-h_2,\alpha)}\,\overline{F_{\eta,\lambda}(-h_3,\alpha)}F_{\eta,\lambda}(h_4,\alpha) \sum_{\substack{q^{\nu-1}<n\leqslant q^\nu \\ q^{\nu-1}<n+sq^\eta\leqslant q^\nu}} \mathrm{e}\left(\frac{h_1(n+r+sq^\eta)^2+h_2(n+r)^2+h_3(n+sq^\eta)^2+h_4n^2}{q^\lambda}\right).$$

The following lemma will allow us to use quadratic Gauss sums, which we have considered in Chapter 2. It is at least known since Vinogradov, and makes it possible to sum over n on a more practicable interval.

Lemma 6.2 *Let m be an integer $\geqslant 2$ and $(z_n)_{n\in\mathbb{Z}}$ complex numbers periodic of period m. Then we have for all $M, N \in \mathbb{Z}$ with $1 \leqslant N \leqslant m$*

$$\sum_{n=M+1}^{M+N} z_n \ll (\log m) \max_{0\leqslant l<m} \left|\sum_{n=0}^{m-1} z_n \,\mathrm{e}\left(\frac{ln}{m}\right)\right|.$$

Proof. Using Lemma 1.2 and the periodicity of the considered complex numbers, we can write

$$\begin{aligned}\sum_{k=M+1}^{M+N} z_k &= \sum_{n=0}^{m-1} z_n \sum_{k=M+1}^{M+N} \frac{1}{m}\sum_{l=0}^{m-1} \mathrm{e}\left(\frac{l(n-k)}{m}\right) \\ &= \sum_{l=0}^{m-1} \frac{1}{m} \sum_{k=M+1}^{M+N} \mathrm{e}\left(\frac{-lk}{m}\right) \sum_{n=0}^{m-1} z_n \,\mathrm{e}\left(\frac{ln}{m}\right).\end{aligned}$$

First we note that the middle sum is a geometric series, and therefore we have

$$\sum_{k=M+1}^{M+N} \mathrm{e}\left(\frac{-lk}{m}\right) \leqslant \min\left(N, \frac{1}{\left|\sin \pi\frac{l}{m}\right|}\right).$$

Furthermore, Lemma A.7 yields (note, that the function $t \mapsto (\sin t)^{-1}$ is convex on $[0,\pi]$)

$$\begin{aligned}\sum_{l=1}^{m-1} \frac{1}{\sin \pi\frac{l}{m}} &\leqslant \int_{1/2}^{m-1/2} \frac{dt}{\sin \pi\frac{t}{m}} = \frac{2m}{\pi}\log\cot\frac{\pi}{4m} \\ &\leqslant \frac{2m}{\pi}\log\frac{4m}{\pi}.\end{aligned}$$

Thus, we have

$$\sum_{l=0}^{m-1}\frac{1}{m}\sum_{k=M+1}^{M+N}\mathrm{e}\left(\frac{-lk}{m}\right)\leqslant\frac{N}{m}+\frac{2}{\pi}\log\frac{4m}{\pi}\ll\log m,$$

and the desired result follows. ∎

If we set $m=q^\lambda$ and $N=\#\{n\in\mathbb{N}:q^{\nu-1}<n\leqslant q^\nu \text{ and } q^{\nu-1}<n+sq^\eta\leqslant q^\nu\}\leqslant q^\nu\leqslant q^\lambda$, applying the previous lemma yields

$$\begin{aligned}S_2&\ll\log q^\lambda\sum_{0\leqslant h_1,h_2,h_3,h_4<q^\lambda}|F_{\eta,\lambda}(h_1,\alpha)F_{\eta,\lambda}(-h_2,\alpha)F_{\eta,\lambda}(-h_3,\alpha)F_{\eta,\lambda}(h_4,\alpha)|\\&\qquad\max_{0\leqslant l<q^\lambda}\left|\sum_{0\leqslant n<q^\lambda}\mathrm{e}\left(\frac{h_1(n+r+sq^\eta)^2+h_2(n+r)^2+h_3(n+sq^\eta)^2+h_4n^2+ln}{q^\lambda}\right)\right|\\&\ll_q\lambda\max_{0\leqslant l<q^\lambda}\sum_{d\mid q^\lambda}\sum_{\substack{0\leqslant h_1,h_2,h_3,h_4<q^\lambda\\(h_1+h_2+h_3+h_4,q^\lambda)=d}}|F_{\eta,\lambda}(h_1,\alpha)F_{\eta,\lambda}(-h_2,\alpha)F_{\eta,\lambda}(-h_3,\alpha)F_{\eta,\lambda}(h_4,\alpha)|\\&\qquad|G(h_1+h_2+h_3+h_4,2r(h_1+h_2)+2sq^\eta(h_1+h_3)+l;q^\lambda)|.\end{aligned}$$

Here we used the notion of the quadratic Gauss sums. Corollary 2.1 yields

$$S_2\ll_q\lambda q^{\lambda/2}\max_{0\leqslant l<q^\lambda}\sum_{d\mid q^\lambda}d^{1/2}\sum_{\substack{0\leqslant h_1,h_2,h_3,h_4<q^\lambda\\(h_1+h_2+h_3+h_4,q^\lambda)=d\\d\mid 2r(h_1+h_2)+2sq^\eta(h_1+h_3)+l}}|F_{\eta,\lambda}(h_1,\alpha)F_{\eta,\lambda}(-h_2,\alpha)F_{\eta,\lambda}(-h_3,\alpha)F_{\eta,\lambda}(h_4,\alpha)|,$$

since the considered Gauss sums are only non-zero (and $\leqslant\sqrt{2dq^\lambda}$) if $d\mid 2r(h_1+h_2)+2sq^\eta(h_1+h_3)+l$. The condition $(h_1+h_2+h_3+h_4,q^\lambda)=d$ is not easy to handle, therefore we replace it by the less restrictive condition $h_1+h_2+h_3+h_4\equiv 0 \bmod d$. Furthermore, there arise some problems with the greatest common divisor of $2r$ and d, respectively with handling the summation conditions, if $\nu_q(d)$ is small. Thus, we consider the last sum over d separately for $\nu_q(d)<\Delta$ and $\nu_q(d)\geqslant\Delta$, where Δ is an integer satisfying $1\leqslant\Delta<\eta$. We write

$$S_2\ll_q\lambda q^{\lambda/2}\max_{0\leqslant l<q^\lambda}(S_3+S_4),\tag{6.10}$$

where

$$S_3=\sum_{\substack{d\mid q^\lambda\\ \nu_q(d)<\Delta}}d^{1/2}\sum_{\substack{0\leqslant h_1,h_2,h_3,h_4<q^\lambda\\ h_1+h_2+h_3+h_4\equiv 0 \bmod d\\ 2r(h_1+h_2)+2sq^\eta(h_1+h_3)+l\equiv 0 \bmod d}}|F_{\eta,\lambda}(h_1,\alpha)F_{\eta,\lambda}(-h_2,\alpha)F_{\eta,\lambda}(-h_3,\alpha)F_{\eta,\lambda}(h_4,\alpha)|,$$

and

$$S_4=\sum_{\substack{d\mid q^\lambda\\ \nu_q(d)\geqslant\Delta}}d^{1/2}\sum_{\substack{0\leqslant h_1,h_2,h_3,h_4<q^\lambda\\ h_1+h_2+h_3+h_4\equiv 0 \bmod d\\ 2r(h_1+h_2)+2sq^\eta(h_1+h_3)+l\equiv 0 \bmod d}}|F_{\eta,\lambda}(h_1,\alpha)F_{\eta,\lambda}(-h_2,\alpha)F_{\eta,\lambda}(-h_3,\alpha)F_{\eta,\lambda}(h_4,\alpha)|.$$

In order to derive an upper estimate of S_3 and S_4, we need the following lemma, which deals with the square root expressions in these sums.

Lemma 6.3 *Let $0 < \delta_1 \leqslant \lambda$ be integers and $\theta \in [-\log 2/(2\log q) + 1/(100\log q), 0]$ a real number. Then we have*

$$\sum_{\substack{d|q^\lambda \\ \nu_q(d)\leqslant\delta_1}} d^{\frac{1}{2}} q^{\theta\nu_q(d)} \ll_q \tau(q^\lambda) q^{\frac{\lambda}{2}+\delta_1\theta-\frac{\log 2}{2\log q}(\lambda-\delta_1)}.$$

Proof. We can write d in the form kq^δ, where $0 \leqslant \delta \leqslant \delta_1$, $k \mid q^{\lambda-\delta}$ and $(k,q) < q$. Thus we have

$$\sum_{\substack{d|q^\lambda \\ \nu_q(d)\leqslant\delta_1}} d^{\frac{1}{2}} q^{\theta\nu_q(d)} = \sum_{0\leqslant\delta\leqslant\delta_1} q^{(\frac{1}{2}+\theta)\delta} \sum_{\substack{k<q^{\lambda-\delta} \\ (k,q)<q}} k^{\frac{1}{2}}.$$

Since (k,q) is strict smaller then q, we have $(k,q) < q/2$ and hence $k = (k, q^{\lambda-\delta}) \leqslant (k,q)^{\lambda-\delta} \leqslant (q/2)^{\lambda-\delta}$. Furthermore the number of admissible integers k is trivially bounded by the numbers of divisors of $q^{\lambda-\delta}$. Thus we finally obtain

$$\begin{aligned}\sum_{\substack{d|q^\lambda \\ \nu_q(d)\leqslant\delta_1}} d^{\frac{1}{2}} q^{\theta\nu_q(d)} &\leqslant \sum_{0\leqslant\delta\leqslant\delta_1} q^{(\frac{1}{2}+\theta)\delta} \tau\left(q^{\lambda-\delta}\right)\left(\frac{q}{2}\right)^{\frac{\lambda-\delta}{2}} \\ &\leqslant \tau(q^\lambda) q^{\frac{\lambda}{2}-\lambda\frac{\log 2}{2\log q}} \sum_{0\leqslant\delta\leqslant\delta_1} q^{\delta\left(\theta+\frac{\log 2}{2\log q}\right)} \ll_q \tau(q^\lambda) q^{\frac{\lambda}{2}+\delta_1\theta-\frac{\log 2}{2\log q}(\lambda-\delta_1)}.\end{aligned}$$

■

6.3 Estimate of S_3

In order to find an upper bound of S_3, we ignore the additional conditions for the indices $h_1, \dots, h_4$. Using Lemma 3.15, we derive

$$\begin{aligned}S_3 &\leqslant \sum_{\substack{d|q^\lambda \\ \nu_q(d)<\Delta}} d^{1/2} \sum_{0\leqslant h_1,h_2,h_3,h_4<q^\lambda} |F_{\eta,\lambda}(h_1,\alpha)F_{\eta,\lambda}(-h_2,\alpha)F_{\eta,\lambda}(-h_3,\alpha)F_{\eta,\lambda}(h_4,\alpha)| \\ &\leqslant \sum_{\substack{d|q^\lambda \\ \nu_q(d)<\Delta}} d^{1/2}\eta^4 q^{4(\lambda-\eta)}.\end{aligned}$$

Employing Lemma 6.3 with $\delta_1 = \Delta$ and $\theta = 0$, we get

$$S_3 \ll_q \tau(q^\lambda)\eta^4 q^{\frac{\lambda}{2}-\frac{\log 2}{2\log q}(\lambda-\Delta)+4(\lambda-\eta)}.$$

In order to find a feasible upper bound, we have to choose Δ not to large and η not to small. We set

$$\Delta = \lambda - \eta + \rho_q \quad \text{with} \quad \rho_q = \left\lfloor 3\rho\frac{\log q}{\log 2}\right\rfloor,$$

where we have to impose the following condition (note that we assumed $\Delta < \eta$)

$$\rho_q < 2\eta - \lambda = 2\eta - \nu - 2\rho. \tag{6.11}$$

Moreover, we choose

$$\eta \geqslant \frac{\nu + \frac{27}{8}\rho}{1 + \frac{\log 2}{8\log q}}. \tag{6.12}$$

We will show later, that these choices are reasonable and eligible. Using $\lambda = \nu + 2\rho$ therefore yields

$$\begin{aligned} S_3 &\ll_q \tau(q^\lambda)\eta^4 q^{\frac{\lambda}{2}-\frac{\log 2}{2\log q}(\eta-\rho_q)+4(\nu+2\rho-\eta)} \\ &\ll_q \tau(q^\lambda)\eta^4 q^{\frac{\lambda}{2}-4\rho+4\nu-\left(4+\frac{\log 2}{2\log q}\right)\eta+\frac{27}{2}\rho} \\ &\ll_q \tau(q^\lambda)\eta^4 q^{\frac{\lambda}{2}-4\rho}. \end{aligned} \tag{6.13}$$

6.4 Estimate of S_4

To find an upper bound of S_4, we transform the summation conditions regarding $h_1, \dots, h_4$ in such a way, that we can employ the results about the discrete Fourier transformation of $\mathrm{e}(f_{\eta,\lambda})$ proved in Chapter 3. We set $\tilde{d} = (d, 2|r|)$. If p is a prime factor of $\tilde{d}$ (and therefore also of q, since $\tilde{d} \mid d \mid q^\lambda$), we have $p^{\nu_p(\tilde{d})} \leqslant 2|r| \leqslant 2q^\rho$. Thus we get $\nu_p(\tilde{d}) \leqslant \lfloor(\rho \log q + \log 2)/\log p\rfloor \leqslant \rho_q$. This yields

$$\tilde{d} = \prod_{p|\tilde{d}} p^{\nu_p(\tilde{d})} \mid \prod_{p|\tilde{d}} p^{\rho_q} \mid q^{\rho_q}.$$

By the imposed condition (6.11), we have $\tilde{d} \mid q^\eta$ and hence

$$2r(h_1 + h_2) + 2sq^\eta(h_1 + h_3) + l \equiv 0 \bmod d$$

implies $\tilde{d} \mid l$. Thus, the above equation is equivalent to

$$r'(h_1 + h_2) + s'q^{\eta-\rho_q}(h_1 + h_3) + l' \equiv 0 \bmod d',$$

where $r' = 2r/\tilde{d}$, $s = 2sq^{\rho_q}/\tilde{d}$, $l' = l/\tilde{d}$ and $d' = d/\tilde{d}$. The integer r' has an inverse element modulo d' since $(r', d') = 1$. If we call it r'' and set $l'' = r''l'$ and $s'' = r''s'$, we can write the last equation as

$$h_1 + h_2 + s''q^{\eta-\rho_q}(h_1 + h_3) + l'' \equiv 0 \bmod d'.$$

Furthermore, we have $\nu_q(d') = \nu_q(d) - \nu_q(\tilde{d}) \geqslant \nu_q(d) - \rho_q$, which implies $q^{\nu_q(d)-\rho_q} \mid d'$. If we replace d' and d by $q^{\nu_q(d)-\rho_q}$, we have a less restrictive but much easier to handle condition. We will see that this proceeding is justified. For the purpose of finding an upper bound of S_4, we split the sum up over d into three different sums.

$$S_4 \leqslant S_5 + S_6 + S_7, \tag{6.14}$$

where

$$S_5 = \sum_{\substack{d|q^\lambda \\ \Delta\leqslant\delta=\nu_q(d)<\eta}} d^{1/2} \sum_{\substack{0\leqslant h_1,h_2,h_3,h_4<q^\lambda \\ h_1+h_2+h_3+h_4\equiv 0 \bmod q^{\delta-\rho q} \\ h_1+h_2+s''q^{\eta-\rho q}(h_1+h_3)+l''\equiv 0 \bmod q^{\delta-\rho q}}} |F_{\eta,\lambda}(h_1,\alpha)F_{\eta,\lambda}(-h_2,\alpha)F_{\eta,\lambda}(-h_3,\alpha)F_{\eta,\lambda}(h_4,\alpha)|,$$

$$S_6 = \sum_{\substack{d|q^\lambda \\ \delta=\nu_q(d)\geqslant\eta}} d^{1/2} \sum_{\substack{0\leqslant h_1,h_2,h_3,h_4<q^\lambda \\ h_1+h_2+h_3+h_4\equiv 0 \bmod q^{\delta-\rho q} \\ h_1+h_2+s''q^{\eta-\rho q}(h_1+h_3)+l''\equiv 0 \bmod q^{\delta-\rho q} \\ \left\|\frac{h_1+s''q^{\eta-\rho q}(h_1+h_3)+l''}{q^{\delta-\rho q}}\right\|\geqslant q^{-\eta+\lambda-\delta+\rho q+4\rho}}} |F_{\eta,\lambda}(h_1,\alpha)F_{\eta,\lambda}(-h_2,\alpha)F_{\eta,\lambda}(-h_3,\alpha)F_{\eta,\lambda}(h_4,\alpha)|,$$

$$S_7 = \sum_{\substack{d|q^\lambda \\ \delta=\nu_q(d)\geqslant\eta}} d^{1/2} \sum_{\substack{0\leqslant h_1,h_2,h_3,h_4<q^\lambda \\ h_1+h_2+h_3+h_4\equiv 0 \bmod q^{\delta-\rho q} \\ h_1+h_2+s''q^{\eta-\rho q}(h_1+h_3)+l''\equiv 0 \bmod q^{\delta-\rho q} \\ \left\|\frac{h_1+s''q^{\eta-\rho q}(h_1+h_3)+l''}{q^{\delta-\rho q}}\right\|<q^{-\eta+\lambda-\delta+\rho q+4\rho}}} |F_{\eta,\lambda}(h_1,\alpha)F_{\eta,\lambda}(-h_2,\alpha)F_{\eta,\lambda}(-h_3,\alpha)F_{\eta,\lambda}(h_4,\alpha)|.$$

Estimate of S_5

At first we consider S_5. Since $\delta = \nu_q(d) < \eta$, we can conclude that the conditions $h_1 + h_2 + s''q^{\eta-\rho_q}(h_1 + h_3) + l'' \equiv 0 \bmod q^{\delta-\rho_q}$ and $h_1 + h_2 + h_3 + h_4 \equiv 0 \bmod q^{\delta-\rho_q}$ are equivalent to $h_1 + h_2 \equiv -l'' \bmod q^{\delta-\rho_q}$ and $h_3 + h_4 \equiv l'' \bmod q^{\delta-\rho_q}$. Hence, we have (using Lemma 3.18)

$$S_5 = \sum_{\substack{d|q^\lambda \\ \Delta\leqslant\delta=\nu_q(d)<\eta}} d^{1/2} \left(\sum_{\substack{0\leqslant h_1,h_2<q^\lambda \\ h_1+h_2\equiv -l'' \bmod q^{\delta-\rho_q}}} |F_{\eta,\lambda}(h_1,\alpha)F_{\eta,\lambda}(-h_2,\alpha)| \right)^2 \ll_q \eta^4 \sum_{\substack{d|q^\lambda \\ \Delta\leqslant\delta=\nu_q(d)<\eta}} d^{1/2}.$$

Now we can employ Lemma 6.3 and obtain

$$S_5 \ll_q \eta^4 \tau(q^\lambda) q^{\frac{\lambda}{2} - \frac{\log 2}{2\log q}(\lambda-\eta)}. \tag{6.15}$$

Estimate of S_6

To estimate S_6, we note that the conditions $h_1 + h_2 + h_3 + h_4 \equiv 0 \bmod q^{\delta-\rho_q}$ and $h_1 + h_2 + s''q^{\eta-\rho_q}(h_1 + h_3) + l'' \equiv 0 \bmod q^{\delta-\rho_q}$ are equivalent to $h_1 + h_2 + s''q^{\eta-\rho_q}(h_1 + h_3) + l'' \equiv 0 \bmod q^{\delta-\rho_q}$ and $h_3 + h_4 - s''q^{\eta-\rho_q}(h_1 + h_3) - l'' \equiv 0 \bmod q^{\delta-\rho_q}$. Let $\mathcal{H}^+$ be the pairs of integers (h_1, h_3) satisfying

$$\left\| \frac{h_1 + s''q^{\eta-\rho_q}(h_1 + h_3) + l''}{q^{\delta-\rho_q}} \right\| \geqslant q^{-\eta+\lambda-\delta+\rho_q+4\rho}. \tag{6.16}$$

Since $\delta = \nu_q(d) \geqslant \eta$ and by (6.11) we have $\delta - \rho_q \geqslant \eta - \rho_q \geqslant \lambda - \eta$. Thus the assumptions of Lemma 3.16 are satisfied and we obtain (using (3.19))

$$\sum_{\substack{0\leqslant h_2<q^\lambda \\ h_1+h_2+s''q^{\eta-\rho_q}(h_1+h_3)+l''\equiv 0 \bmod q^{\delta-\rho_q}}} |F_{\eta,\lambda}(-h_2,\alpha)| \ll_q \eta |F_{\lambda-\eta}(h_1 + s''q^{\eta-\rho_q}(h_1 + h_3) + l'', \alpha)|$$
$$q^{-\eta+\lambda-\delta+\rho_q} \varphi_{q^{\eta-\lambda+\delta-\rho_q}} \left(\frac{h_1 + s''q^{\eta-\rho_q}(h_1 + h_3) + l''}{q^{\delta-\rho_q}} \right).$$

Since $\eta - \rho_q \geqslant \lambda - \eta$, we have that $F_{\lambda-\eta}$ is also periodic of period $q^{\eta-\rho_q}$. Using the fact that $\varphi_k(t) \leqslant (\sin \pi\|t\|)^{-1} \leqslant (2\|t\|)^{-1}$ for all $k \geqslant 2$ and $t \in \mathbb{R} \setminus \mathbb{Z}$ and (6.16), we obtain

$$\sum_{\substack{0\leqslant h_2<q^\lambda \\ h_1+h_2+s''q^{\eta-\rho_q}(h_1+h_3)+l''\equiv 0 \bmod q^{\delta-\rho_q}}} |F_{\eta,\lambda}(-h_2,\alpha)| \ll_q \eta |F_{\lambda-\eta}(h_1 + l'', \alpha)| q^{-4\rho}.$$

In a similar way (employing (3.20) instead of (3.19)) we get

$$\sum_{\substack{0\leqslant h_4<q^\lambda \\ h_3+h_4-s''q^{\eta-\rho_q}(h_1+h_3)-l''\equiv 0 \bmod q^{\delta-\rho_q}}} |F_{\eta,\lambda}(h_4,\alpha)| \ll_q \eta |F_{\lambda-\eta}(-h_3 + l'', \alpha)|.$$

Thus we have

$$\begin{aligned} S_6 &\ll_q \eta^2 q^{-4\rho} \sum_{\substack{d|q^\lambda \\ \delta=\nu_q(d)\geqslant\eta}} d^{1/2} \sum_{(h_1,h_3)\in\mathcal{H}^+} |F_{\eta,\lambda}(h_1,\alpha)F_{\lambda-\eta}(h_1 + l'',\alpha)F_{\eta,\lambda}(-h_3,\alpha)F_{\lambda-\eta}(-h_3 + l'',\alpha)| \\ &\ll_q \eta^2 q^{-4\rho} \sum_{\substack{d|q^\lambda \\ \delta=\nu_q(d)\geqslant\eta}} d^{1/2} \left(\sum_{0\leqslant h<q^\lambda} |F_{\eta,\lambda}(h,\alpha)F_{\lambda-\eta}(h + l'',\alpha)| \right)^2 \\ &\ll_q \eta^4 q^{-4\rho} \sum_{\substack{d|q^\lambda \\ \delta=\nu_q(d)\geqslant\eta}} d^{1/2}, \end{aligned}$$

where we used Lemma 3.17 to obtain the last inequality. Lemma 6.3 with $\delta_1 = \lambda$ and $\theta = 0$ finally yields

$$S_6 \ll_q \eta^4 \tau(q^\lambda) q^{\frac{\lambda}{2}-4\rho}. \tag{6.17}$$

Estimate of S_7

The last crucial step in proving Proposition 6.1 is the estimation of S_7. To be in line with the previous studies, let $\mathcal{H}^-$ be the pairs of integers (h_1, h_3) satisfying

$$\left\| \frac{h_1 + s'' q^{\eta-\rho_q}(h_1+h_3) + l''}{q^{\delta-\rho_q}} \right\| < q^{-\eta+\lambda-\delta+\rho_q+4\rho}. \tag{6.18}$$

Similar calculations as for S_6 show, that

$$S_7 \ll_q \eta^2 \sum_{\substack{d|q^\lambda \\ \delta=\nu_q(d)\geqslant\eta}} d^{1/2} \sum_{(h_1,h_3)\in\mathcal{H}^+} |F_{\eta,\lambda}(h_1,\alpha)F_{\lambda-\eta}(h_1+l'',\alpha)F_{\eta,\lambda}(-h_3,\alpha)F_{\lambda-\eta}(-h_3+l'',\alpha)|. \tag{6.19}$$

The only difference exists therein, that we employ (3.20) for the sum over h_2 instead of (3.19). We impose the condition

$$\eta + 2\rho_q \leqslant \lambda. \tag{6.20}$$

We distinguish two cases. If $\nu_q(d) = \delta \leqslant \eta + 2\rho_q$, we remove the additional summation conditions to sum over all $0 \leqslant h_1, h_3 < q^\lambda$, employ Lemma 3.17 and subsequently Lemma 6.3.

$$\begin{aligned} &\eta^2 \sum_{\substack{d|q^\lambda \\ \eta\leqslant\delta=\nu_q(d)\leqslant\eta+2\rho_q}} d^{1/2} \left(\sum_{0\leqslant h<q^\lambda} |F_{\eta,\lambda}(h,\alpha)F_{\lambda-\eta}(h+l'',\alpha)| \right)^2 \\ &\ll_q \eta^4 \sum_{\substack{d|q^\lambda \\ \eta\leqslant\delta=\nu_q(d)\leqslant\eta+2\rho_q}} d^{1/2} \ll_q \eta^4 \tau(q^\lambda) q^{\frac{\lambda}{2}-\frac{\log 2}{2\log q}(\lambda-\eta-2\rho_q)}. \end{aligned} \tag{6.21}$$

In the converse case ($\nu_q(d) = \delta < \eta+2\rho_q$), we have to be more careful, since the trivial estimates arranged before do not yield the desired result. We impose the condition

$$2\eta > \lambda + \rho_q + 4\rho + 1 = \nu + \rho_q + 6\rho + 1, \tag{6.22}$$

which allows us to obtain a better upper bound. In particular, we can show the following lemma.

Lemma 6.4 *With the same notation as before, let $\nu_q(d) = \delta \geqslant \eta + 2\rho_q$ and $2\eta < \lambda + \rho_q + 4\rho + 1$ (condition* (6.22)*). Furthermore, let h_1 be a fixed integer and $(h_1, h_3) \in \mathcal{H}^-$. Then there exists an integer $a(h_1)$, satisfying $0 \leqslant a(h_1) < q^{\delta-\eta-2\rho_q}$ and*

$$h_3 \equiv a(h_1) \bmod q^{\delta-\eta-2\rho_q}.$$

Proof. Clearly, we only have to prove that two integers h_3 and h_3', satisfying $(h_1, h_3) \in \mathcal{H}^-$ and $(h_1, h_3') \in \mathcal{H}^-$ are congruent 0 modulo $q^{\delta-\eta-2\rho_q}$. Indeed, we have

$$\begin{aligned} \left\| \frac{s''(h_3-h_3')}{q^{\delta-\eta}} \right\| &= \left\| \frac{h_1 + s'' q^{\eta-\rho_q}(h_1+h_3) + l''}{q^{\delta-\rho_q}} - \frac{h_1 + s'' q^{\eta-\rho_q}(h_1+h_3') + l''}{q^{\delta-\rho_q}} \right\| \\ &\leqslant \left\| \frac{h_1 + s'' q^{\eta-\rho_q}(h_1+h_3) + l''}{q^{\delta-\rho_q}} \right\| + \left| \frac{h_1 + s'' q^{\eta-\rho_q}(h_1+h_3') + l''}{q^{\delta-\rho_q}} \right\| \\ &< 2q^{-\eta+\lambda-\delta+\rho_q+4\rho} < q^{\eta-\delta}. \end{aligned}$$

The last inequality is a result of (6.22) and implies $\left\| \frac{s''(h_3-h_3')}{q^{\delta-\eta}} \right\| = 0$. Taking into account the definition of s'', this is equivalent to

$$r''2s\frac{q^{\rho_q}}{(d,2|r|)}(h_3-h_3') \equiv 0 \bmod q^{\delta-\eta}.$$

By definition, r'' is relatively prime to d'. Recall that $\nu_q(d') \geqslant \delta - \rho_q > 0$ which implies that $q \mid d'$. Hence, r'' is also relatively prime to $q^{\delta-\eta}$ and therefore invertible modulo $q^{\delta-\eta}$. Furthermore, we have for all prime factors p of q which also divide $2s$, that $p^{\nu_p(2|s|)} \leqslant 2|s| < 2q^{2\rho}$. But since $\nu_p(2|s|) \leqslant \lfloor (2\rho\log q + \log 2)/(\log p) \rfloor \leqslant \rho_q$, we finally can conclude

$$h_3 - h_3' \equiv 0 \bmod q^{\delta-\eta-2\rho_q}.$$

■

After (6.19) and the previous lemma, we have

$$\begin{aligned} S_7 &\ll_q \eta^2 \sum_{\substack{d\mid q^\lambda \\ \eta+2\rho_q<\delta=\nu_q(d)\leqslant\lambda}} d^{1/2} \sum_{(h_1,h_3)\in\mathcal{H}^+} |F_{\eta,\lambda}(h_1,\alpha)F_{\lambda-\eta}(h_1+l'',\alpha)F_{\eta,\lambda}(-h_3,\alpha)F_{\lambda-\eta}(-h_3+l'',\alpha)| \\ &\quad + \eta^4\tau(q^\lambda)q^{\frac{\lambda}{2}-\frac{\log 2}{2\log q}(\lambda-\eta-2\rho_q)} \\ &\ll_q \eta^2 \sum_{\substack{d\mid q^\lambda \\ \eta+2\rho_q<\delta=\nu_q(d)\leqslant\lambda}} d^{1/2} \sum_{0\leqslant h_1<q^\lambda} |F_{\eta,\lambda}(h_1,\alpha)F_{\lambda-\eta}(h_1+l'',\alpha)| \\ &\qquad \sum_{\substack{0\leqslant h_3<q^\lambda \\ h_3\equiv a(h_1) \bmod q^{\delta-\eta-2\rho_q}}} |F_{\eta,\lambda}(-h_3,\alpha)F_{\lambda-\eta}(-h_3+l'',\alpha)| + \eta^4\tau(q^\lambda)q^{\frac{\lambda}{2}-\frac{\log 2}{2\log q}(\lambda-\eta-2\rho_q)}. \end{aligned}$$

Now we can employ Lemma 3.17 to the last sum.

$$\begin{aligned} S_7 &\ll_q \eta^3 \sum_{\substack{d\mid q^\lambda \\ \eta+2\rho_q<\delta=\nu_q(d)\leqslant\lambda}} d^{1/2}|F_{\delta-\mu-2\rho_q}(-a(h_1),\alpha)F_{\delta-\eta-2\rho_q}(-a(h_1)+l'',\alpha)| \\ &\qquad \sum_{0\leqslant h_1<q^\lambda} |F_{\eta,\lambda}(h_1,\alpha)F_{\lambda-\eta}(h_1+l'',\alpha)| + \eta^4\tau(q^\lambda)q^{\frac{\lambda}{2}-\frac{\log 2}{2\log q}(\lambda-\eta-2\rho_q)}. \end{aligned}$$

Using Lemma 3.6 and again Lemma 3.17 to the remaining sum yields

$$\begin{aligned} S_7 &\ll_q \eta^3 \sum_{\substack{d\mid q^\lambda \\ \eta+2\rho_q<\delta=\nu_q(d)\leqslant\lambda}} d^{1/2}q^{-2c_q\|(q-1)\alpha\|^2(\delta-\eta-2\rho_q)} \sum_{0\leqslant h_1<q^\lambda} |F_{\eta,\lambda}(h_1,\alpha)F_{\lambda-\eta}(h_1+l'',\alpha)| \\ &\quad + \eta^4\tau(q^\lambda)q^{\frac{\lambda}{2}-\frac{\log 2}{2\log q}(\lambda-\eta-2\rho_q)} \\ &\ll_q \eta^4 \sum_{\substack{d\mid q^\lambda \\ \eta+2\rho_q<\delta=\nu_q(d)\leqslant\lambda}} d^{1/2}q^{-2c_q\|(q-1)\alpha\|^2(\delta-\eta-2\rho_q)} + \eta^4\tau(q^\lambda)q^{\frac{\lambda}{2}-\frac{\log 2}{2\log q}(\lambda-\eta-2\rho_q)}. \end{aligned}$$

We introduce the following constant

$$c_q'(\alpha) := 2\frac{\pi^2}{15\log q}\left(1-\frac{2}{q+1}\right)\|(q-1)\alpha\|^2 \leqslant 2\frac{\pi^2}{15\cdot 4\log q} < \frac{0,329}{\log q} < \frac{0,346}{\log q} < \frac{\log 2}{2\log q}. \tag{6.23}$$

In particular, we have $c'_q(\alpha) = 12/15 \cdot 2c_q\|(q-1)\alpha\|^2$. Since $\delta - \eta - 2\rho_q \geqslant 0$, we can replace $2c_q\|(q-1)\alpha\|^2$ by $c'_q(\alpha)$ and apply Lemma 6.3 with $\delta_1 = \lambda$ and $\theta = -c'_q(\alpha)$. Thus, we get

$$S_7 \ll_q \eta^4\tau(q^\lambda)q^{\frac{\lambda}{2}-c'_q(\alpha)(\lambda-\eta-2\rho_q)} + \eta^4\tau(q^\lambda)q^{\frac{\lambda}{2}-\frac{\log 2}{2\log q}(\lambda-\eta-2\rho_q)}.$$

Because $c'_q(\alpha)$ satisfies $c'_q(\alpha) \leqslant \log 2/(2\log q)$, we finally obtain

$$S_7 \ll_q \eta^4\tau(q^\lambda)q^{\frac{\lambda}{2}-c'_q(\alpha)(\lambda-\eta-2\rho_q)}. \tag{6.24}$$

Conclusion

According to (6.14), we have to sum up the derived upper bounds of S_5, (see (6.15)), S_6 (see (6.17)) and S_7 (see (6.24))

$$S_4 \ll_q \eta^4\tau(q^\lambda)q^{\frac{\lambda}{2}-\frac{\log 2}{2\log q}(\lambda-\eta)} + \eta^4\tau(q^\lambda)q^{\frac{\lambda}{2}-4\rho} + \eta^4\tau(q^\lambda)q^{\frac{\lambda}{2}-c'_q(\alpha)(\lambda-\eta-2\rho_q)}.$$

The first sum is negligible since $c'_q(\alpha) \leqslant \log 2/(2\log q)$. Furthermore we have by the definitions of λ and ρ_q that $\lambda - \eta - 2\rho_q \geqslant \nu - \eta - 6\log q/\log 2$. Hence, we get

$$S_4 \ll_q \eta^4\tau(q^\lambda)q^{\frac{\lambda}{2}-4\rho}\left(1 + q^{-c'_q(\alpha)(\nu-\eta)+\left(4+6c'_q(\alpha)\frac{\log q}{\log 2}\right)\rho}\right).$$

To eliminate the last term in the brackets, we impose

$$\eta \leqslant \nu - \left(\frac{4}{c'_q(\alpha)} + 6\frac{\log q}{\log 2}\right)\rho. \tag{6.25}$$

We will see in the next chapter, that we really can choose η satisfying this inequality. Thus, we finally obtain

$$S_4 \ll_q \eta^4\tau(q^\lambda)q^{\frac{\lambda}{2}-4\rho}. \tag{6.26}$$

6.5 Proof of Proposition 6.1 and Theorem 6.1

After estimating the crucial sums S_3 and S_4, we are in the situation of proving Proposition 6.1. After (6.10), (6.13) and (6.24), we have

$$S_2 \ll_q \lambda\eta^4\tau(q^\lambda)q^{\lambda-4\rho}.$$

Since $\tau(.)$ is multiplicative (see Appendix A), we have

$$\tau(q^\lambda) = \prod_{p|q}\tau(p^{\lambda\nu_p(q)}) = \prod_{p|q}(\lambda\nu_p(q)+1) \leqslant \prod_{p|q}(\lambda\nu_p(q)+\lambda) = \lambda^{\omega(q)}\tau(q).$$

We assumed $\rho \leqslant \nu/3$, which implies $\eta \leqslant \lambda = \nu + 2\rho \ll \nu$. Thus we have

$$S_2 \ll_q \nu^{5+\omega(q)}q^{\nu-\rho} \ll_q \nu^{6\omega(q)}q^{\nu-2\rho},$$

because $\omega(q) \geqslant 1$. Inserting this estimate in (6.9) and combining with (6.7) yields

$$S \ll_q \nu^{3\omega(q)/2}q^{\nu-\rho/2}.$$

In order to finish the proof, we have to choose $2 \leqslant \rho \leqslant \nu/3$ and η in such a way, that all imposed conditions from the last sections are satisfied and $\nu - \rho/2 = \nu(1 - \sigma_q'(\alpha))$, with $\sigma_q'(\alpha) > 0$. By (6.12) and (6.25), η has to fulfill

$$\frac{\nu + \frac{27}{8}\rho}{1 + \frac{\log 2}{8 \log q}} \leqslant \eta \leqslant \nu - \left(\frac{4}{c_q'(\alpha)} + 6\frac{\log q}{\log 2}\right)\rho.$$

If we choose

$$\rho < \gamma(q,\alpha)\nu \coloneqq \frac{\log 2}{27 \log q + (8 \log q + \log 2)\left(\frac{4}{c_q'(\alpha)} + 6\frac{\log q}{\log 2}\right)}\,\nu,$$

we have $\rho \leqslant \nu/3$. If ν is big enough, we have $2 \leqslant \rho$ in addition. Since η has to be an integer, the considered interval has to be strictly greater than zero. Indeed, one can readily show that the above choice of ρ is sufficient. The nearer ρ is by the given bound, the greater ν has to be. If we fix ρ (say $\rho = \lfloor (199/200)\gamma(q,\alpha)\nu \rfloor$) we have to restrict ν to be greater than a suitable $\nu_0(q,\alpha)$, such that we can really choose η as an integer and such that $\rho \geqslant 2$. It remains to show, that the following conditions are fulfilled:

$$\begin{aligned}
(6.8) &: 1 \leqslant \eta \leqslant \nu - 2\rho - 1,\\
(6.11) &: \rho_q < 2\eta - \nu - 2\rho,\\
(6.20) &: \eta + 2\rho_q \leqslant \nu + 2\rho,\\
(6.22) &: 2\eta > \nu + \rho_q + 6\rho + 1.
\end{aligned}$$

By our choice, (6.8) is trivially satisfied. To show (6.20), we only have to note that

$$\eta + 2\rho_q \leqslant \nu - 14\frac{\log q}{\log 2}\rho + 6\frac{\log q}{\log 2}\rho,$$

since $\frac{4}{c_q'(\alpha)} + 6\frac{\log q}{\log 2} \geqslant 14\frac{\log q}{\log 2}$ by (6.23). If $\nu \geqslant 27$, we have (using the given bounds of η and ρ very crude)

$$\nu + \rho_q + 6\rho + 1 \leqslant \nu + 3\frac{\log q}{\log 2}\rho + 6\rho + 1 \leqslant \nu\left(1 + 3\frac{\log q}{\log 2}\frac{\log 2}{27 \log q} + \frac{6}{27} + \frac{1}{27}\right) = \nu\frac{37}{27} \leqslant 2\frac{\nu}{1 + \frac{1}{8}} < 2\eta,$$

which proves (6.22) and (6.11). Hence we have shown Proposition 6.1. ∎

Proof of Theorem 6.1

The proof of Theorem 6.1 is a direct consequence of Proposition 6.1. Let λ be that integer, such that $q^{\lambda-1} < x \leqslant q^{\lambda}$. Moreover, consider only numbers x, such that $\lambda \geqslant \nu_0$, where ν_0 is defined in Proposition 6.1. Then we can write

$$\begin{aligned}
\sum_{1 \leqslant n \leqslant x} \mathrm{e}\left(f(n^2)\right) &= \sum_{1 \leqslant n \leqslant q^{\nu_0 - 1}} \mathrm{e}\left(f(n^2)\right) + \sum_{\nu_0 \leqslant \nu < \lambda} \sum_{q^{\nu-1} < n \leqslant q^{\nu}} \mathrm{e}\left(f(n^2)\right) + \sum_{q^{\lambda-1} < n < x} \mathrm{e}\left(f(n^2)\right)\\
&\ll_q \sum_{\nu_0 \leqslant \nu \leqslant \lambda} \nu^{3\omega(q)/2} q^{(1-\sigma_q'(\alpha))\nu} \ll_q \lambda^{3\omega(q)/2} q^{(1-\sigma_q'(\alpha))\lambda}.
\end{aligned}$$

Since $\lambda \leqslant \lfloor \log x/\log q + 1 \rfloor$, we finally obtain

$$\sum_{1\leqslant n\leqslant x} \mathrm{e}\left(f(n^2)\right) \ll_q (\log x)^{3\omega(q)/2} x^{(1-\sigma_q'(\alpha))} \ll_{q,\alpha} x^{(1-\sigma_q(\alpha))},$$

where $\sigma_q(\alpha) = 198/199\sigma_q'(\alpha)$. Thus, the proof of Theorem 6.1 is finished. ■

Remark. It follows from the proof of Theorem 6.1, that we can choose

$$\sigma_q(\alpha) = \frac{99}{100}\frac{\log 2}{2\left(27\log q + (8\log q + \log 2)\left(\frac{4}{c_q'(\alpha)} + 6\frac{\log q}{\log 2}\right)\right)},$$

where $c_q'(\alpha) = \frac{2\pi^2}{15\log q}\left(1 - \frac{2}{q+1}\right)\|(q-1)\alpha\|^2$. In comparison to this result, Mauduit and Rivat obtained

$$\sigma_q(\alpha) = \frac{99}{100}\frac{\log 2}{2\left(25\log q + (8\log q + \log 2)\left(\frac{4}{c_q''(\alpha)} + 3\frac{\log q}{\log 2}\right)\right)},$$

where $c_q''(\alpha) = \min\left(\frac{\pi^2}{6\log q}\left(1 - \frac{2}{q+1}\right)\|(q-1)\alpha\|^2, \frac{\log 2}{2\log q}\right)$. Note, that $\frac{2\pi^2}{12\log q}\left(1 - \frac{2}{q+1}\right)\|(q-1)\alpha\|^2 \geqslant \frac{\log 2}{2\log q}$ only in the case that $\|(q-1)\alpha\|$ is near $1/2$.

Appendix A

Number Theoretical Fundamentals

In this chapter we want to introduce the notion of arithmetic functions. We define a couple of important representatives and state some fundamental results. For further information and definitions see for example [26, 23].

Definition A.1 (Arithmetic function) *A complex valued function a defined on $\mathbb{N}$ is called an arithmetic function.*

Arithmetic functions play an important role in analytic number theory and can be also understood as sequences of complex numbers. To every function corresponds a (formal) generating series

$$A(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}.$$

It is called a *Dirichlet series* and one of the most famous representatives is *Riemann's zeta-function*

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

It is absolutely convergent for $Re(s) > 1$ and the corresponding arithmetic function is $J(n) = 1$ for $n \geqslant 1$. It was Euler, who first considered this series. He showed that

$$\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}}$$

for some real $s > 1$ and deduced from that, that there have to be infinitely many primes. Riemann was the first who studied the zeta-function also for complex values. His ideas brought a fulminant development in analytic number theory.

The arithmetic functions form an integral domain. Therefore we define the following operations.

Definition A.2 *Let a and b two arithmetic functions. Then we define the sum*

$$c(n) = (a + b)(n) := a(n) + b(n),$$

and the Dirichlet convolution

$$c'(n) = (a * b)(n) := \sum_{d|n} a(d) b\left(\frac{n}{d}\right).$$

The corresponding (formal) Dirichlet series are $C(n) = A(n) + B(n)$ and $C'(n) = A(n) \cdot B(n)$.

Now we can state the following lemma, which can be readily verified.

Lemma A.1 *The arithmetic functions, equipped with these operations, form an integral domain. The additive identity is the function H such that $H(n) = 0$ for any integer $n \geqslant 1$. The multiplicative identity is the function I with $I(1) = 1$ and $I(n) = 0$ for any $n > 1$. The units are those arithmetic functions f, such that $f(1) \neq 0$.*

From particular interest are such functions, that satisfy multiplicative properties.

Definition A.3 *An arithmetic function a is multiplicative, if*

$$a(mn) = a(m)a(n) \quad \text{for } m \text{ and } n \text{ relatively prime.} \tag{A.1}$$

It is completely multiplicative, if (A.1) holds for all m and n.

Some important arithmetic functions. Now we introduce some arithmetic functions, which are essential in the theory of numbers.

Euler's ϕ - function. It occurs in different fields of number theory, is multiplicative and is defined in the following way:

$$\varphi(n) = \#\{k | 1 \leqslant k \leqslant n, (k, n) = 1\}.$$

The number of divisors of n. $\tau(n) = \sum_{d|n} 1$ is the number of divisors of n. If we write $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, then the divisors of n are of the form $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ where $0 \leqslant b_1 \leqslant a_1, \ldots 0 \leqslant b_k \leqslant a_k$. Hence, we can also write

$$\tau(n) = \prod_{p|n} (\nu_p(n) + 1), \tag{A.2}$$

where $\nu_p(n)$ is the integer r, such that $p^r \mid n$ but $p^{r+1} \nmid n$. This calculation also shows, that $\tau(.)$ is multiplicative. Furthermore, we can bound the number of divisors in the following way.

Lemma A.2 *Let $\delta > 0$. Then we have*

$$\tau(n) = O_\delta(n^\delta).$$

Proof. By (A.2) we can write

$$\frac{\tau(n)}{n^\delta} = \prod_{p|n} \left(\frac{\nu_p(n) + 1}{p^{\nu_p(n)\delta}} \right).$$

If $p \geqslant 2^{1/\delta}$, we have $\frac{\nu_p(n)+1}{p^{\nu_p(n)\delta}} \leqslant \frac{\nu_p(n)+1}{2^{\nu_p(n)}} \leqslant 1$. Contrary, if $p \leqslant 2^{1/\delta}$, we have to look a little bit more carefully. Since $\nu_p(n)\delta \log 2 \leqslant \exp(\nu_p(n)\delta \log 2) = 2^{\nu_p(n)\delta} \leqslant p^{\nu_p(n)\delta}$, we obtain

$$\frac{\nu_p(n) + 1}{p^{\nu_p(n)\delta}} \leqslant 1 + \frac{\nu_p(n)}{p^{\nu_p(n)\delta}} \leqslant 1 + \frac{1}{\delta \log 2} \leqslant \exp\left(\frac{1}{\delta \log 2} \right).$$

Thus, we get

$$\frac{\tau(n)}{n^\delta} \leqslant \prod_{p \leqslant 2^{1/\delta}} \exp\left(\frac{1}{\delta \log 2}\right) < \exp\left(\frac{2^{1/\delta}}{\delta \log 2}\right) = O_\delta(1).$$

■

von Mangoldt function $\Lambda(n)$**.** Especially for questions concerning primes and sums over primes, the von Mangoldt function is very helpful. It is defined as follows:

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and integer } k \\ 0 & \text{otherwise.} \end{cases}$$

The Möbius function $\mu(n)$**.** Following function is named after the German mathematician August Ferdinand Möbius,

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

Lemma A.3 *The Möbius function has the property that for* $z \in \mathbb{N}$

$$\sum_{d^z \mid n} \mu(d) = \begin{cases} 1 & \textit{if } n \textit{ is not divisible by a } z\textit{-th power of a prime} \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. This identity is trivial if n is not divisible by a z-th power of a prime. In this case, there is only one summand ($d = 1$). If $n > 1$, we can write $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}} \cdots p_m^{\alpha_m}$ where $p_1, \ldots, p_m$ are pairwise distinct primes in such an order, that $\alpha_1 \cdots \alpha_k \geqslant z$ and $\alpha_{k+1} \cdots \alpha_m < z$. If n is divisible by a z-th power of a prime, then $k \geqslant 1$. Then

$$\begin{aligned} \sum_{d^z \mid n} \mu(d) &= 1 + \sum_{1 \leqslant i \leqslant k} \mu(p_i) + \sum_{1 \leqslant i < j \leqslant k} \mu(p_i p_j) + \cdots + \mu(p_1 \cdots p_k) \\ &= 1 - k + \binom{k}{2} + \cdots + (-1)^k = (1-1)^k = 0, \end{aligned}$$

and hence, we have the stated result. ■

Remark. If $z = 1$, then we have the more common assertion $\sum_{d \mid n} \mu(d) = 1$ if $n = 1$ and $\sum_{d^z \mid n} \mu(d) = 0$ otherwise. Using the notion of the Dirichlet convolution, this is equivalent to $\mu * J = I$, where J is the arithmetic function corresponding to the zeta-function ($J(1) = 1$ for all $n \geqslant 1$) and I denotes the multiplicative inverse in the ring of arithmetic functions. Hence we have for the corresponding Dirichlet series

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

where $Re(s) > 1$. In addition, we can show the following lemma.

Lemma A.4 *If $s = \sigma + it$ is a complex number with real part $\sigma > 1$ and imaginary part t, we have*

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

Proof. Since $\zeta(s) = \prod_{p\in\mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}$ (the infinite product is absolutely convergent for $\sigma > 1$), we get

$$\frac{1}{\zeta(s)} = \prod_{p\in\mathbb{P}} \left(1 - \frac{1}{p^s}\right).$$

Carrying out the multiplication (first only for all primes $p \leqslant P$ and then going with $P \to \infty$), we exactly get the desired Dirichlet series for $1/\zeta(s)$. We also see from Euler's representation of $\zeta(s)$, that

$$\log \zeta(s) = \sum_{p\in\mathbb{P}} \log\left(\frac{1}{1-p^{-s}}\right).$$

Differentiating with respect to s, we obtain

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p\in\mathbb{P}} \frac{d}{ds} \log\left(\frac{1}{1-p^{-s}}\right) = \sum_{p\in\mathbb{P}} \frac{\log p}{p^s - 1}.$$

The differentiation is legitimate because the derived series is uniformly convergent for $\sigma \geqslant 1 + \delta > 1$. Moreover, we can write

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p\in\mathbb{P}} \log p \sum_{m=1}^{\infty} p^{-ms} = \sum_{p,m} p^{-ms} \log p = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},$$

where the last equality follows from the definition of $\Lambda(n)$. ∎

Prime counting function. $\pi(x) = \sum_{p\leqslant x} 1$ counts all primes, which are less or equal to x. The function $\pi(x; k, a) = \sum_{\substack{p\leqslant x \\ p\equiv a \bmod k}} 1$ counts all primes, which are less or equal to x and are congruent a modulo k.

Now we state without proof two very important and famous theorems. The first one is the *Prime Number Theorem* and the second one is the *Prime Number Theorem for Arithmetic Progressions*. For proofs of the theorems, see [26].

Theorem A.1 (Prime Number Theorem) *There exists a positive constant C, such that for $x \geqslant 3$*

$$\pi(x) = \int_2^x \frac{du}{\log u} + O\left(x \exp\left(-C(\log x)^{3/5}(\log\log x)^{-1/5}\right)\right).$$

Theorem A.2 (Page-Siegel-Walfisz) *Let a and k be integers satisfying $(a, k) = 1$ and $A > 0$. Then we have for $x \geqslant 2$*

$$\pi(x; k, a) = \frac{1}{\varphi(k)} \int_2^x \frac{du}{\log u} + O_A\left(\frac{x}{(\log x)^A}\right).$$

Remark. Since $\int_2^x (\log u)^{-1}\, du = x/\log x + o(x/\log x)$, one can derive from the previous Theorems

$$\pi(x) = \frac{x}{\log x} + o(\frac{x}{\log x}), \quad \text{and} \quad \pi(x; k, a) = \frac{1}{\varphi(k)} \frac{x}{\log x} + o(\frac{x}{\log x}).$$

Next, we state and prove some fundamental summation formulas.

Lemma A.5 (Summation by parts) *Let $(a_n)_{n\in\mathbb{N}}$ be a sequence of complex numbers and $\lambda_1 < \lambda_2 < \cdots < \lambda_n \to \infty$ be real numbers. Suppose that the complex-valued function g is continuous and piecewise continuously differentiable on the interval $[\lambda_1, x]$. Then we have*

$$\sum_{\lambda_n \leqslant x} a_n g(\lambda_n) = g(x) \sum_{\lambda_n \leqslant x} a_n - \int_{\lambda_1}^{x} \left(\sum_{\lambda_n < u} a_n \right) g'(u)\, du.$$

Proof. Let j be the appropriate index, such that $\lambda_j \leqslant x < \lambda_{j+1}$. Then

$$\begin{aligned} -\int_{\lambda_1}^{x} \sum_{\lambda_n \leqslant u} a_n g'(u)\, du &= -\sum_{i=1}^{j-1} \int_{\lambda_i}^{\lambda_{i+1}} \sum_{\lambda_n \leqslant u} a_n g'(u)\, du - \int_{\lambda_j}^{x} \sum_{\lambda_n \leqslant u} a_n g'(u)\, du \\ &= \sum_{i=1}^{j-1} \left(\sum_{\lambda_\nu \leqslant \lambda_i} a_\nu \right) (g(\lambda_i) - g(\lambda_{i+1})) + \left(\sum_{\lambda_\nu \leqslant \lambda_j} a_\nu \right) (g(\lambda_j) - g(x)) \\ &= -g(x) \sum_{\lambda_n \leqslant x} a_n + \sum_{i=2}^{j} \left\{ \sum_{\lambda_\nu \leqslant \lambda_i} a_\nu - \sum_{\lambda_\nu \leqslant \lambda_{i-1}} a_\nu \right\} g(\lambda_i) + a_1 g(\lambda_1), \end{aligned}$$

and the assertion follows. ∎

Lemma A.6 *Let a and b be integers. If g is a monotone not increasing function from the interval $[a, b]$ into the real numbers, then we have*

$$\int_a^b g(u)\, du \leqslant \sum_{a \leqslant n < b} g(n) \quad \text{and} \quad \sum_{a < n \leqslant b} g(n) \leqslant \int_a^b g(u)\, du.$$

Proof. Because of the additivity of the integral and the monotony of g, we have

$$\int_a^b g(u)\, du = \sum_{n=a}^{b-1} \int_n^{n+1} g(u)\, du \leqslant \sum_{n=a}^{b-1} \int_n^{n+1} g(n)\, du = \sum_{a \leqslant n < b} g(n).$$

Analogously, one can prove the second statement. ∎

Lemma A.7 *Let a and b be integers and f a continuous, continuous differentiable and convex function on $[a - 1/2, b + 1/2]$. Then we have*

$$\sum_{n=a}^{b} f(n) \leqslant \int_{a-\frac{1}{2}}^{b+\frac{1}{2}} f(t)\, dt.$$

Proof. Using the trapezoid method and the convexity of f, we have

$$f(n) = \int_{n-\frac{1}{2}}^{n+\frac{1}{2}} f(n) + f'(n)(n - t)\, dt \leqslant \int_{n-\frac{1}{2}}^{n+\frac{1}{2}} f(t)\, dt.$$

Summing over n, we obtain

$$\sum_{n=a}^{b} f(n) \leqslant \sum_{n=a}^{b} \int_{n-\frac{1}{2}}^{n+\frac{1}{2}} f(t)\, dt = \int_{a-\frac{1}{2}}^{b+\frac{1}{2}} f(t)\, dt.$$

∎

Next we state a generalization of Poisson's summation formula. A proof can be found for example in [46].

Lemma A.8 *Let $f(x)$ be of bounded variation for $|x| \leqslant M$ and let $f(x)$ be twice differentiable for $|x| \geqslant M$. Assume that $\int_{-\infty}^{\infty} f(x)\,dx$, $\int_{M}^{\infty} |f''(x)|\,dx$ and $\int_{-\infty}^{-M} |f''(x)|\,dx$ exist. If we put $f^*(x) = \frac{1}{2}(f(x+0)+f(x-0))$, then $\sum_{n=-\infty}^{\infty} f^*(n)$ is convergent and*

$$\sum_{n=-\infty}^{\infty} f^*(n) = \sum_{k=-\infty}^{\infty} \int_{-\infty}^{\infty} f(x)\mathrm{e}(-kx)\,dx.$$

A lot of problems in analytic number theory dealing with prime numbers, need estimates of sums of the form $\sum_{p\leqslant x} f(p)$. In many cases (for example the prime number theorem, where $f(n) = 1$), it is cleverer to study the sum $\sum_{n\leqslant x} \Lambda(n)f(n)$ since one can transmit results from this sum to the other one by summation by parts. This emphasizes the importance of von Mangoldt's Λ-function. In particular, we can show the following lemma as a consequence of the prime number theorem.

Lemma A.9 ([33]) *Let g be an arithmetic function such that $|g(n)| \leqslant 1$ for any integer n. Then*

$$\left|\sum_{p\leqslant x} g(p)\right| \leqslant \frac{2}{\log x} \max_{t\leqslant x} \left|\sum_{n\leqslant t} \Lambda(n)g(n)\right| + O(\sqrt{x}).$$

Proof. Using Lemma A.5, we can write

$$\sum_{p\leqslant x} g(p) = \frac{1}{\log x} \sum_{p\leqslant x} (\log p)g(p) + \int_2^x \left(\sum_{p\leqslant t} (\log p)g(p)\right) \frac{dt}{t\log^2 t}.$$

Note, that by the Prime Number Theorem, $\sum_{p\leqslant t} \log p \leqslant \sum_{p\leqslant t} \log t = O(t)$. Hence, slicing the integral at $\sqrt{x}$, we get

$$\begin{aligned}\left|\sum_{p\leqslant x} g(p)\right| &\leqslant \left(\frac{1}{\log x} + \int_{\sqrt{x}}^x \frac{dt}{t\log^2 t}\right) \max_{\sqrt{x}<t\leqslant x} \left|\sum_{p\leqslant t} (\log p)g(p)\right| + O(\sqrt{x}) \\ &= \frac{2}{\log x} \max_{\sqrt{x}<t\leqslant x} \left|\sum_{p\leqslant t} (\log p)g(p)\right| + O(\sqrt{x}).\end{aligned}$$

But, using the Prime Number Theorem again, we obtain

$$\left|\sum_{n\leqslant t} \Lambda(n)g(n) - \sum_{p\leqslant t} (\log p)g(p)\right| \leqslant \sum_{p\leqslant \sqrt{x}} \log p \sum_{2\leqslant a\leqslant \left\lfloor \frac{\log x}{\log p}\right\rfloor} 1 \leqslant \pi(\sqrt{x}) \log x = O(\sqrt{x}).$$

This proves the desired result. ∎

Next we state and prove Weyl's criterion (see [54]). Therefore we recall, that a sequence $(x_n)_{n\in\mathbb{N}}$ of real numbers is uniformly distributed modulo 1, if for every pair a, b of real numbers with $0 \leqslant a < b \leqslant 1$ we have

$$\lim_{N\to\infty} \frac{\#\{x_n : 1 \leqslant n \leqslant N, x_n \in [a,b)\}}{N} = b - a.$$

Theorem A.3 (Weyl Criterion) *The sequence $(x_n)_{n\in\mathbb{N}}$ is uniformly distributed modulo* 1*, if and only if for all integers $h \neq 0$*

$$\sum_{n=1}^{N} \mathrm{e}(hx_n) = o(N). \tag{A.3}$$

Proof. We use the following common notation for the fractional part of a real number x: $\{x\} = x - \lfloor x \rfloor$. Let us first note, that if $\mathbb{1}_{[a,b)}$ is the characteristic function of the interval $[a, b)$, we can write (1.1) in the form

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathbb{1}_{[a,b)}(\{x_n\}) = \int_0^1 \mathbb{1}_{[a,b)}(x)\, dx. \tag{A.4}$$

The first step to prove the theorem is to show that $(x_n)_{n\in\mathbb{N}}$ is uniformly distributed modulo 1 if and only if for every real-valued continuous function f defined on the unit interval $[0, 1]$ we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(\{x_n\}) = \int_0^1 f(x)\, dx. \tag{A.5}$$

Let $(x_n)_{n\in\mathbb{N}}$ be uniformly distributed modulo 1, and let $f(x) = \sum_{i=0}^{k-1} d_i \mathbb{1}_{[a_i,a_{i+1})}(x)$ be a step function on the unit interval, where $0 = a_0 < a_1 < \cdots < a_k = 1$. It follows directly from (A.4) that for such a function the desired equality holds. Since the step functions are dense in the continuous functions, (A.5) holds also for all real-valued continuous functions. Conversely, let a sequence $(x_n)_{n\in\mathbb{N}}$ be given, and suppose that (A.5) holds for every continuous function f. We have to show that (A.5) holds also for a characteristic function of a half-open interval. But this is by density of step functions again clear.
We can now easily extend our claim to a complex-valued continuous function f on $\mathbb{R}$ with period 1. The same argumentation as above for the real and imaginary part of f yields (A.5), but where the fractional part of x is replaced by x (periodicity of f). Hence, the following claim is true: The sequence $(x_n)_{n\in\mathbb{N}}$ is uniformly distributed modulo 1, if and only if for every complex-valued continuous function f on $\mathbb{R}$ with period 1 we have

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(x_n) = \int_0^1 f(x)\, dx. \tag{A.6}$$

Now we are in the situation to prove the theorem. If $(x_n)_{n\in\mathbb{N}}$ is uniformly distributed modulo 1, we get (A.3) using (A.6) and the fact, that $\int_0^1 \mathrm{e}(hx)\, dx = 0$ if $h \neq 0$. Vice versa, if (A.3) holds for all integers $h \neq 0$, we have to show that (A.6) is true for all complex-valued continuous functions with period 1. But since the functions $x \mapsto \mathrm{e}(xh)$, $h \in \mathbb{Z}$ are dense in the complex-valued continuous functions on $\mathbb{R}$ with period 1, there exists a trigonometric polynomial $g(x)$ such that for every $\varepsilon > 0$

$$\sup_{0\leqslant x\leqslant 1} |f(x) - g(x)| \leqslant \varepsilon.$$

Hence we have

$$\left| \int_0^1 f(x)\, dx - \frac{1}{N} \sum_{n=1}^{N} f(x_n) \right| \leqslant \left| \int_0^1 (f(x) - g(x))\, dx \right| + \left| \int_0^1 g(x)\, dx - \frac{1}{N} \sum_{n=1}^{N} g(x_n) \right| + \left| \frac{1}{N} \sum_{n=1}^{N} (g(x_n) - f(x_n)) \right|.$$

Using again $\int_0^1 \mathrm{e}(hx)\, dx = 0$ if $h \neq 0$ and $\int_0^1 \mathrm{e}(hx)\, dx = 1$ if $h = 0$, we readily derive the desired result. ∎

Finally, we prove the Chinese remainder theorem (see for example [48, Theorem 5.4.3]).

Theorem A.4 (Chinese remainder theorem) *Let $m_1, \dots, m_l$ and $a_1, \dots, a_l$ be integers. The system of simultaneous congruences*
$n \equiv a_i \bmod m_i$, $1 \leqslant i \leqslant l$ has an integer solution, if and only if

$$a_i \equiv a_j \bmod (d_i, d_j) \quad \text{for } 1 \leqslant i, j \leqslant l. \tag{A.7}$$

All solutions n are then congruent $\operatorname{lcm}(d_1, \dots, d_l)$.

Proof. First we observe that there cannot be a solution if (A.7) is not satisfied. Indeed, if $n \equiv a_i \bmod m_i$ and $n \equiv a_j \bmod m_j$, than it follows that $a_i \equiv n \equiv a_j \bmod (d_i, d_j)$.

Let us assume now, that the integers m_i, $1 \leqslant i \leqslant l$ are pairwise coprime and (A.7) is satisfied. If we set $M_j := \frac{1}{m_j} \prod_{i=1}^{l} m_i$, then we have $(M_j, m_j) = 1$. But this implies that there exists an integer b_j, such that $b_j M_j \equiv 1 \bmod m_j$. Thus, we obtain

$$n := \sum_{i=1}^{l} a_i b_i M_i \equiv a_i b_i M_i \equiv a_i \bmod m_i$$

for each i.

If n_1 and n_2 are two solutions, then we have $n_1 - n_2 \equiv 0 \bmod m_j$ for $1 \leqslant j \leqslant l$. Since the integers m_j are pairwise coprime, we obtain $n_1 \equiv n_2 \bmod m_1 \cdots m_l$.

Now we consider the general case. If $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then the previous result shows, that the congruence $n \equiv a \bmod m$ is equivalent to the system of congruences $n \equiv a \bmod p_i^{\alpha_i}$. Using this observation, we split the system of congruences $n \equiv a_i \bmod m_i$, $1 \leqslant i \leqslant l$ up into a bigger system. If $(d_i, d_j) \neq 1$, then there are some congruences trivially satisfied (by (A.7)). Deleting these congruences yields a new system of congruences where the moduli are pairwise coprime. The previous result assures that there exists a solution which is unique modulo $\operatorname{lcm}(d_1, \dots, d_l)$. ∎

Index

Bibliography

[1] J.-P. Allouche and J. Shallit. *Automatic sequences*. Cambridge University Press, 2003.

[2] R. Bellman and H. N. Shapiro. On a problem in additive number theory. *Annals of Mathematics*, 49(2):333–340, 1948.

[3] J. Bésineau. Indépendence statistique d'ensembles liés à la fonction "sommes des chiffres". *Acta Arithmetica*, 20:401–416, 1972.

[4] E. Borel. Les probabilités dénombrables et leurs applications arithmétiques. *Rend. Circ. Mat. Palermo*, 27:247–271, 1909.

[5] D. G. Champernowne. The construction of decimals normal in the scale of ten. *J. London Math. Soc.*, 8:254–260, 1933.

[6] J.-R. Chen. On the representation of a large even integer as the sum of a prime and a product of at most two primes. *Scientia Sinica*, 16:157–176, 1973.

[7] A. H. Copeland and P. Erdős. Note on normal numbers. *Bull. Amer. Math. Soc.*, 52:857–860, 1946.

[8] J. Coquet. Sur certaines suites uniformément équiréparties modulo 1. *Acta Arithmetica*, 36:157–162, 1980.

[9] C. Dartyge and G. Tennenbaum. Congruences de sommes de chiffres de valeurs polynomiales. *Bulletin of the London Mathematical Society*, 38:61–69, 2006.

[10] H. Davenport and P. Erdős. Note on normal decimals. *Canadian J. Math.*, 4:58–63, 1952.

[11] H. Delange. Sur la fonction sommatoire de la fonction "somme des chiffres". *Enseign. Math.*, 21:31–47, 1975.

[12] G. L. Dirichlet. *Mathematische Werke. Bände I,II, Herausgegeben auf Veranlassung der Königlich Preussischen Akademie der Wissenschaften von L. Kronecker*. Chelsea Publishing Co., Bronx, N.Y., 1969.

[13] M. Drmota, C. Mauduit, and J. Rivat. Primes with an average sum of digits. preprint.

[14] M. Drmota and J. Rivat. The sum of digits function of squares. *J. London Math. Soc.*, 72,2:273–292, 2005.

[15] M. Drmota, J. Rivat, and T. Stoll. The sum of digits of primes in $\mathbb{Z}[i]$. Monatshefte für Mathematik, to appear.

[16] M. Euwe. Mengentheoretische Betrachtungen über das Schachspiel. *Proc. Konin. Acad. Wetenschappen Amsterdam*, 32:633–642, 1929.

[17] N. J. Fine. The distribution of the sum of digits (mod p). *Bull. Amer. Math. Soc*, 71:651–652, 1965.

[18] E. Fouvry and C. Mauduit. Méthodes de crible et fonctions sommes des chiffres. *Acta Arithmetica*, 77,4:339–351, 1996.

[19] E. Fouvry and C. Mauduit. Sommes des chiffres et nombres presques premiers. *Mathematische Annalen*, 305:571–599, 1996.

[20] J. B. Friedlander, D. R. Heath-Brown, H. Iwaniec, and J. Kaczorowski. *Analytic Number Theory, Lecture Notes in Mathematics vol. 1891*. Springer-Verlang, 2006.

[21] A. O. Gelfond. Sur les nombres qui ont des propriétés additives et multiplicatives données. *Acta Arithmetica*, 13:259–265, 1968.

[22] S. Graham and G. Kolesnik. *Van der Corput's Method of Exponential Sums*. London Mathematical Society Lecture Note Series vol. 126, Campridge University Press, 1991.

[23] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers - Fifth Edition*. Oxford University Press, 2005.

[24] G. Harman and J. Rivat. Primes of the form $[p^c]$ and related questions. *Glasgow Mathematical Journal*, 37:131–141, 1995.

[25] E. Heppner. Über die Summe der Ziffern natürlicher Zahlen. *Annales Uiv. Sci. Budapest, Sectio Math.*, 19:41–43, 1976.

[26] H. Iwaniec and E. Kowalski. *Analytic Number Theory, American Mathematical Society Colloquium Publications vol. 53*. American Mathematical Society Providence. Rhode Island, 2004.

[27] I. Kátai. On the sum of digits of prime numbers. *Annales Uiv. Sci. Budapest, Sectio Math.*, 10:89–93, 1967.

[28] D.-H. Kim. On the joint distribution of q-additive functions in residue classes. *Journal of Number Theory*, 74:307–336, 1999.

[29] L. Kuipers and H. Niederreiter. *Uniform Distribution of Sequences*. Wiley-Interscience Publication, 1974.

[30] K. Mahler. The spectrum of an array and its application to the study of the translation porperties of a simple class of arithmetical functions II. On the translation properties of a simple class of arithmetical functions. *J. Math. and Physics*, 6:158–163, 1927.

[31] C. Mauduit. Multiplicative properties of the Thue-Morse sequence. *Periodica Mathematica Hungarica*, 43,1-2:137–153, 2001.

[32] C. Mauduit and J. Rivat. La somme des chiffres des carrés. Acta Mathematica, to appear.

[33] C. Mauduit and J. Rivat. Sur un problème de Gelfond: la somme des chiffres des nombres premiers. Annals of Mathematics, to appear.

[34] C. Mauduit and J. Rivat. Répartition des fonctions q-multiplicatives dans la suite $([n^c])$, $c > 1$. *Acta Arithmetica*, 71,2:171–179, 1995.

[35] C. Mauduit and J. Rivat. Propriétés q-multiplicatives de la suite $([n^c])$, $c > 1$. *Acta Arithmetica*, 118,2:187–203, 2005.

[36] M. Mendès-France. Nombres normaux applications aux fonctions pseudo-aléatoires. *Journal d'Analyse Mathématique*, 20:1–56, 1967.

[37] H. L. Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis, CBMS Regional Conference Series in Mathematics, Number 84*. American Mathematical Society, 1994.

[38] M. Morse. Recurrent geodesics on a surface of negative curvature. *Trans. Amer. Math. Soc.*, 22:84–100, 1921.

[39] H. Niederreiter and I. E. Shparlinski. On the distribution of inversive congruential pseudorandom numbers in parts of the period. *Math. Comput.*, 70(236):1569–1574, 2001.

[40] M. Olivier. Répartition des valeurs de la fonction "somme des chiffres". Séminaire de Théorie des Nombres 1970-1971, Exp. No. 16 p.7.

[41] M. Olivier. Sur le développement en base g des nombres premiers. *C. R. Acad. Sci. Paris Sér. A-B*, 272:A937–A939, 1971.

[42] M. Peter. The summatroy function of the sum-of-digits function on polynomial sequences. *Acta Arithmetica*, 104,1:85–96, 2002.

[43] I. I. Piatetski-Shapiro. On the distribution of prime numbers in sequences of the form $[f(n)]$. *Mat. Sbornik N.S.*, 33(75):559–566, 1953.

[44] E. Prouhet. Mémoire sur quelques relations entre les puissances des nombres. *C. R. Acad Sc. Paris*, 33:31, 1851.

[45] M. Queffélec. *Substitution Dynamical Systems - Spectral Analysis, Lecture Notes in Mathematics vol. 1294*. Springer-Verlag, 1987.

[46] H. Rademacher. *Topics in Analytic Number Theory*. Springer-Verlag Berlin Heidelberg New York, 1973.

[47] P. Ribenboim. *The little book of bigger primes, Second Edition*. Springer-Verlag New York, 2004.

[48] H. N. Shapiro. *Introduction to the Theory of Numbers*. Wiley, New York, 1983.

[49] I. Shiokawa. On the sum of digits of prime numbers. *Proc. Japan Acad.*, 50:551–554, 1974.

[50] S. C. Tang. An improvement and generalization of Bellman - Shapiro's theorem on a problem in additive number theory. *Proc. Amer. Math. Soc.*, 14:199–204, 1963.

[51] A. Thue. Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen (1912). Reprinted: Selected mathematical papers of Axel Thue Universitetsforlaget, 1977 413–478.

[52] A. Thue. Über unendliche Zeichenreihen (1906). Reprinted: Selected mathematical papers of Axel Thue Universitetsforlaget, 1977 139–158.

[53] I. M. Vinogradov. *The method of trigonometrical sums in the theory of numbers*. translated from the Russian, revised and annotated by K. F. Roth and A. Davenport, Interscience Publisher, 1954.

[54] H. Weyl. Über die Gleichverteilung von Zahlen mod. Eins. *Math. Ann.*, 77:313–352, 1916.

[55] N. Wiener. The spectrum of an array and its application to the study of the translation porperties of a simple class of arithmetical functions I. The spectrum of an array. *J. Math. and Physics*, 6:145–157, 1927.