

Hybrid results related to Waring's Problem
Martin Jancevskis

Dissertation

Ausgeführt zum Zwecke der Erlangung
des akademischen Grades eines
Doktors der Technischen Wissenschaften
von

Martin Jancevskis,

wohnhafte im Berlinerring 41/14, A-8047 Graz,
geboren am 17.12.1983 in Stuttgart, Deutschland.
Matr-Nr.: 0831606

Betreut von
Ao. Univ.-Prof. Dr. Thuswaldner und
O. Univ.-Prof. Dr. Tichy.

Unterstützt von "FWF Der Wissenschaftsfonds",
Projekte S9610 und S9611.

Eingereicht an der Technischen Universität Graz,
Doktoratsschule für Mathematik und Wissenschaftliches Rechnen.

Graz, den 18. Jänner 2010

Statutory Declaration

I declare that I have authored this thesis independently, that I have not used other than the declared sources / resources, and that I have explicitly marked all material which has been quoted either literally or by content from the used sources.

Martin Jancevskis

January 18, 2010

Dedicated to Lorac.

Acknowledgments

I would like to express my gratitude to my supervisors Jörg Thuswaldner and Robert Tichy. They gave me all the freedom I needed and wanted and always had time whenever I needed help. That what is good for me and what I wanted had always been in their focus.

Financial support by the Austrian Science Foundation FWF (projects S9610 and S9611) is gratefully acknowledged.

Many thanks goes to my friends and colleagues in Graz. In particular, I want to mention Christoph Aistleitner, Bruno Martin, Philipp Mayer, Jochen Resch, Martin Widmer and “Olga”. It was great fun working in the “Beobachtterraum” office in the fourth floor at Steyrergasse 40.

Contents

Part A

Introduction (9)

1. Notation (10)

2. Waring's Problem (11)

2.1. History and developments (11)

2.2. The Hardy–Littlewood method (14)

2.2.1. The treatment of the minor arcs (16)

2.2.2. The treatment of the major arcs (17)

3. Hybrid structures (20)

3.1. Dense sets (21)

Part B

Waring's Problem and convergent sieve sequences (23)

4. Results and context (24)

4.1. Convergent sieve sequences (24)

4.2. Waring's Problem (26)

5. Proofs (30)

5.1. Preliminary considerations (30)

5.2. Asymptotic formula (33)

5.2.1. Minor arcs (33)

5.2.2. Major arcs (36)

5.2.3. Proof of Theorem 4.2.1 (42)

5.3. The singular series (43)

5.3.1. Factorization (45)

5.3.2. Properties of $\kappa(p)$ (50)

5.3.3. Proof of Theorem 4.2.2 (52)

Part C

Waring's Problem, squarefree numbers, and digital restrictions (56)

6. Results and context (57)

6.1. Sum-of-digits function (57)

6.2. Waring's Problem (60)

7. Proofs (63)

7.1. Preliminaries - the circle method (63)

7.2. Weyl's inequality (67)

7.3. Auto-correlation functions (68)

7.4. Iterations (74)

7.5. Conclusion (81)

References (84)

Outline

The topic of this dissertation are developments of Waring's Problem. In Part A, we briefly introduce the history of Waring's Problem. Besides, we give a short non-detailed presentation of the Hardy-Littlewood method. This method is the main tool in order to attack Waring's Problem and related diophantine equations. We also mention the underlining philosophy and motivation of this dissertation that we call "hybrid structures".

Part B is based on a recent paper of the author [50]. Let \mathcal{V} be a set of pairwise coprime positive integers not containing 1 and let $\delta > 0$ such that the series $\sum_{v \in \mathcal{V}} v^{-1+\delta}$ converges. We proof that for given integers with $s > 2^k$ and $k > 0$ and for every sufficiently large N Waring's equation

$$x_1^k + \dots + x_s^k = N$$

has a solution in positive integers x_i such that x_i is not divisible by any $v \in \mathcal{V}$ for all $i = 1, 2, \dots, s$.

Part C generalizes this results. This part is also based on a recent paper of the author [49]. For simplicity, we take \mathcal{V} to be the set of the squares of all primes. Then the condition that an integer n is not divisible by any $v \in \mathcal{V}$ can be read as $\mu^2(n) = 1$, i.e. that n is squarefree. We denote by $s_q(n)$ the sum of digits of the q -ary representation of a non-negative integer n . For example $s_{10}(246) = 2 + 4 + 6 = 12$. The main results of Part C is that for every sufficiently large integer N the equation $x_1^k + \dots + x_s^k = N$ has a solution in positive integers x_i such that $\mu^2(x_i) = 1$ and $s_q(x_i) \equiv h_i \pmod{m_i}$ for all $i = 1, 2, \dots, s$. Here, m_i, h_i are given non-negative integers that fulfill certain minor conditions.

Besides the existence of such solutions, we also give asymptotic formulas of the number of admissible representations. By such asymptotic formulas, we are able to show that certain properties among the integers are in a certain sense independent. That means, that we show some hybrid structures among the integers.

Kurzfassung

Inhalt dieser Dissertation sind neue Resultat im Zusammenhang mit dem Waringschen Problem. In Teil A wird das Waringsche Problem in seinen geschichtlichen Kontext gestellt und eine kurze Einführung in die Hardy-Littlewoodsche Methode gegeben. Es wird zudem die grundlegende Philosophie und Motivation der Arbeit, nämlich hybride Strukturen, vorgestellt.

Teil B basiert auf einem jüngst erschienenen Artikel des Autors [50]. Sei \mathcal{V} eine Menge paarweise teilerfremder natürlicher Zahlen ohne 1 und sei $\delta > 0$, so dass $\sum_{v \in \mathcal{V}} v^{-1+\delta}$ endlich ist. Es wird gezeigt, dass für alle natürlichen Zahlen s, k mit $s > 2^k$ and $k > 0$ und für jedes hinreichend große N die Waringsche Gleichung

$$x_1^k + \dots + x_s^k = N$$

eine Lösung in natürlichen Zahlen x_i hat, so dass x_i von keinem Element aus \mathcal{V} geteilt wird.

Teil C basiert ebenfalls auf einem Artikel des Autors [49]. Sei \mathcal{V} die Menge der Quadrate der Primzahlen. Die Bedingung, dass n von keinem Element aus \mathcal{V} geteilt wird, entspricht nun $\mu^2(n) = 1$, d.h. dass n quadratfrei ist. Sei $s_q(n)$ die Ziffersumme in der q -adischen Darstellung einer natürlichen Zahl n . Es gilt z.B. $s_{10}(246) = 2 + 4 + 6 = 12$. Das Hauptresultat von Teil C ist, dass jedes hinreichend große natürliche N dargestellt werden kann in der Form $x_1^k + \dots + x_s^k = N$ mit positiven Zahlen x_i , so dass $\mu^2(x_i) = 1$ und $s_q(x_i) \equiv h_i \pmod{m_i}$, wobei m_i, h_i gegebene natürliche Zahlen sind, welche gewisse Bedingungen erfüllen.

Neben der Existenz solcher Lösungen werden auch asymptotische Formeln für die Anzahl der zulässigen Darstellungen gegeben. Durch diese Formeln ist ersichtlich, dass die hier untersuchten Eigenschaften der natürlichen Zahlen in einem gewissen Sinne unabhängig sind. Damit werden hybride Strukturen der natürlichen Zahlen aufgezeigt.

Part A:
Introduction

1 Notation

For abbreviation, we implicitly always assume that an integer is non-negative. Hence the symbols \mathbb{N} , \mathbb{R} , and \mathbb{C} denote the set of the integers, the real numbers, and the complex numbers respectively. For $x \in \mathbb{R}$ with $x \geq 0$, we let $\lfloor x \rfloor$ denote the largest integer not exceeding x . We call an integer n squarefree if for every $d \in \mathbb{N}$, the condition $d^2 | n$ implies $d = 1$. The Möbius μ -function is defined by $\mu(n) = 0$ if n is not a squarefree integer, $\mu(n) = 1$ if n is a squarefree positive integer with an even number of distinct prime factors, and $\mu(n) = -1$ elsewhere.

Let $f : \mathbb{N} \rightarrow \mathbb{R}$ and $g : \mathbb{N} \rightarrow \mathbb{R}^+$. We use the expression

- $f(x) = O(g(x))$,
- $f(x) \ll g(x)$, and
- there are $C, c > 0$ such that $|f(x)| \leq cg(x)$ holds for all integer $x > C$

equivalently. Assume that the expression $\lim_{x \rightarrow \infty} f(x)/g(x)$ exists. We write $f(x) \sim g(x)$ if $\lim_{x \rightarrow \infty} f(x)/g(x) = 1$ and $f(x) = o(g(x))$ if $\lim_{x \rightarrow \infty} f(x)/g(x) = 0$.

For abbreviation, for a real number α , we define $e(\alpha) := e^{2\pi i \alpha}$. Here, e denotes the base of the natural logarithm. We will reserve the following special use for the symbol ε : Every expression containing an ε is to be understood as valid if the expression holds for some $\varepsilon > 0$. The constants implied by the use of the symbols O and \ll may depend on ε and on absolute constants only.

2 Waring's Problem

2.1 History and developments

Clearly, not every integer is a square. But one might ask if an integer is a sum of two squares. If $n = x_1^2 + x_2^2$ and $m = y_1^2 + y_2^2$, then an easy calculation shows that $mn = (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2$. Thus, provided that every prime is a sum of two squares, every integer is a sum of two squares. Indeed, every prime p such that $p \equiv 1$ modulo 4 is a sum of two squares. A very short and elegant proof of this fact was found by Don Zagier [84]. However, if p is a prime such that $p \equiv 3$ modulo 4, then p is not a sum of two squares. Let N be an integer and let

$$N = \prod_p p^{e_p(N)}$$

be its unique prime factorization. Then N is a sum of two squares if and only if for all $p \equiv 3$ modulo 4, we have $2|e_p(N)$. This result was stated without proof by Fermat. In 1749, it was proved by Leonhard Euler in a letter to Edward Waring. Notice that not every integer is a sum of three squares. This can be seen from the fact that $x^2 \equiv 0, 1$ or 4 modulo 8 for all $x \in \mathbb{N}$. Thus a sum of three squares is never congruent 7 modulo 8.

However, every integer is a sum of four squares. Let $N \in \mathbb{N}$. In 1770, Lagrange showed that the equation

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = N$$

has a solution in integers x_1, x_2, x_3, x_4 . For an account of this theorem, we refer to [39, Chapter 20]. Actually, an exact expression for the number of representations of an integer N as a sum of four squares is given by

$$8 \sum_{d|N} d$$

if N is odd and by

$$24 \sum_{\substack{d|N \\ d \text{ is odd}}} d$$

if N is even. This result is from 1834 and is due to Jacobi. For a short

proof of this result, see [43] resp. [42].

In the same year, Edward Waring proposed a generalization of Lagrange's Theorem. He asserted without proof that "Every integer is a cube or the sum of two, three, ... nine cubes; every integer is also the square of a square, or the sum of up to nineteen such; and so forth." [78, Page 336] More formally, let $k \in \mathbb{N}$ and denote by $g(k)$ the minimal integer s such that for all integers N , there exists $x_1, \dots, x_s \in \mathbb{N}$ such that

$$x_1^k + \dots + x_s^k = N. \quad (2.1.1)$$

Thus a weak version of Waring's conjecture can be read as

$$g(k) < \infty \quad (2.1.2)$$

for all $k \in \mathbb{N}$. In this language, Lagrange proved $g(2) = 4$. The first proof of (2.1.2) for all k is due to Hilbert [41] in 1909. Roughly speaking, Hilbert made use of polynomial identities of the form

$$\begin{aligned} 6(a^2 + b^2 + c^2 + d^2)^2 = & (a+b)^4 + (a-b)^4 + (c+d)^4 + (c-d)^4 \\ & + (a+c)^4 + (a-c)^4 + (b+d)^4 + (b-d)^4 \\ & + (a+d)^4 + (a-d)^4 + (b+c)^4 + (b-c)^4. \end{aligned}$$

This is a generalization of the fact that the product of a sum of four squares by a sum of four squares equals a sum of four squares, which is an useful tool for the proof of Lagrange's Theorem. However, Hilbert's method gives a very poor bound for $g(k)$. Presently, we know that

$$g(k) = 2^k + \lfloor (3/2)^k \rfloor - 2 \quad (2.1.3)$$

for all $k \leq 471\,600\,000$ (see [53]).

Let $N \in \mathbb{N}$. We denote by $R_{s,k}(N)$ the number of representations of the integer N in the form (2.1.1), where the variables x_i ($i = 1, \dots, s$) are assumed to be integers. However, unlike the case $k = 2, s = 4$, we can not expect to get an exact formula for $R_{s,k}(N)$ for arbitrary k .

Heuristically, one might conjecture that $R_{s,k}(N)$ is of order of magnitude $N^{s/k-1}$. This can be motivated by the observation that the s vari-

ables x_i are supposed to hold $0 \leq x_i \leq N^{1/k}$ ($i = 1, \dots, s$). Having chosen randomly $(x_1, \dots, x_s) \in \{0, 1, \dots, \lfloor N^{1/k} \rfloor\}^s$, the heuristic probability that indeed (2.1.1) holds is N^{-1} .

Suppose that an asymptotic formula of the form

$$R_{s,k}(N) \sim \mathfrak{S}^*(N)N^{s/k-1} \quad (2.1.4)$$

holds, where $1 \ll \mathfrak{S}^*(N) \ll 1$ is some arithmetical function that will be specified later. Then there is an integer N_0 depending on s and k only such that $R_{s,k}(N) > 0$ for all $N > N_0$. Thus if we can show such a formula, we prove that (2.1.1) has a solution for all sufficiently large integers N . Indeed, such an asymptotic formula was obtained by Hardy and Littlewood [35] in 1920. We define $G(k)$ as the least integer value of s such that at most a finite amount of integers N can not be represented in the form (2.1.1). Clearly, $g(k) \geq G(k)$. In [36] and [37], Hardy and Littlewood showed

$$G(k) \leq (k-2)2^{k-1} + 5.$$

There is a large list of improvements of bounds of the function $G(k)$ and we refer the reader to the article [75] that gives a survey of the history on developments of Waring's Problem. We want to mention the sharp estimate

$$G(k) \leq k(\log k + \log \log k + 2 + O(\log \log k / \log k))$$

for large integers k that is due to Wooley [83]. Recall (2.1.3). The number $G(k)$ is thus essential smaller than $g(k)$.

However the present knowledge of the exact value for $G(k)$ is very poor. We only know that $G(2) = 4$ and $G(4) = 16$. The latter result is due to Davenport [20] from 1939, while the former result is Lagrange's Theorem. Besides, Linnik [55] showed in 1943 that $G(3) \leq 7$. This proof has been strongly simplified by Watson [80].

But one can obtain better results if one asks if almost all integers N can be represented in the form (2.1.1) for given integers s and k . Here, we use the expression "almost all" in the following sense. We define $\tilde{G}(k)$ as the smallest number s such that the number of integers $N < X$ such that (2.1.1) has no solution is $o(X)$. Davenport [19] showed that $\tilde{G}(3) = 4$,

Hardy and Littlewood [38] proved that $\tilde{G}(4) = 15$, due to Vaughan [69], we have $\tilde{G}(8) = 32$ and Wooley [82] showed $\tilde{G}(16) = 64$ and $\tilde{G}(32) = 128$.

Having shown a bound or an exact value for $G(k)$ does not imply the existence of an asymptotic formula for the number of solutions of (2.1.1). The first result providing an asymptotic formula is due to Hua [45] from 1938. He showed that an asymptotic formula of the form (2.1.4) holds if $s \geq 2^k + 1$. In 1995, Ford [29] verified the existence of an asymptotic formula provided that

$$s \geq k^2 (\log k + \log \log k + O(1)).$$

Among others, Vaughan and Wooley [71], [72], [73], and [74] improved this bound for smaller values of k

2.2 The Hardy–Littlewood method

The so called Hardy–Littlewood method is a useful tool to prove asymptotic formulas of the form (2.1.4). The basic idea of this method was already presented in a paper by Hardy and Ramanujan [34] in 1918. We only give a short non-detailed introduction to that method and refer the reader to the wonderful books [68] and [21].

Let $M \in \mathbb{N}$. The important observation is the formula

$$\int_0^1 e(\alpha M) d\alpha = \begin{cases} 1 & \text{if } M = 0 \\ 0 & \text{if } M \neq 0. \end{cases} \quad (2.2.1)$$

Substituting

$$M = x_1^k + \dots + x_s^k - N$$

and summing over all integers $x_i \leq N^{1/k}$ ($i = 1, \dots, s$) on the left hand side of (2.2.1) yields the formula

$$\begin{aligned} R_{s,k}(N) &= \sum_{x_1 \leq N^{1/k}} \cdots \sum_{x_s \leq N^{1/k}} \int_0^1 e(x_1^k + \dots + x_s^k - N) d\alpha \\ &= \int_0^1 (f(\alpha))^s e(-\alpha N) d\alpha, \end{aligned}$$

where we define

$$f(\alpha) := \sum_{x \leq N^{1/k}} e(\alpha x^k).$$

Clearly, one can substitute M in (2.2.1) above by a big class of expressions of the form $F(x_1, \dots, x_d) - N$ in order to attack the solubility of the diophantine equation $F(x_1, \dots, x_d) = N$, where F is some function. For instance, the circle method is a useful tool to attack the so-called Goldbach's Problem, where one asks if every large even integer can be expressed as a sum of two primes and if every large odd integer is a sum of three primes.

We want to mention that the formula (2.2.1) can be also deduced in the following way. For a variable X , let

$$F(X) := \sum_{n \geq 1} X^{n^k}.$$

Then

$$(F(X))^s = \sum_{n_1 \geq 1} \dots \sum_{n_s \geq 1} X^{n_1^k + \dots + n_s^k} = \sum_{N \geq 0} R_{s,k}(N) X^N.$$

Cauchy's integral formula enables us to extract a coefficient $R_{s,k}(N)$ of the power series in the last display which again yields (2.2.1).

In order to prove (2.1.4), we need to understand the function $f(\alpha)$. One subdivides the interval $[0, 1)$ into two disjoint sets \mathfrak{M} and \mathfrak{m} , where the former is called the major arcs and the latter is called the minor arcs. For some sufficiently small $\delta > 0$, we define

$$\mathfrak{M} := \bigcup_{\substack{1 \leq q \leq P^\delta \\ 1 \leq a \leq q \\ (a,q)=1}} \left\{ 0 \leq \alpha < 1 \mid \left| \alpha - \frac{a}{q} \right| \leq P^{-k+\delta} \right\}$$

and $\mathfrak{m} := [0, 1) \setminus \mathfrak{M}$. Here, we take $P := N^{1/k}$. Thus

$$R_{s,k}(N) = \int_{\mathfrak{M}} (f(\alpha))^s e(-\alpha N) d\alpha + \int_{\mathfrak{m}} (f(\alpha))^s e(-\alpha N) d\alpha$$

Notice that in the definition of \mathfrak{M} above, the union is a disjoint union of sets. Roughly speaking, if $\alpha \in [0, 1)$ is close to a rational number with a small denominator, then α belongs to the major arcs \mathfrak{M} and $f(\alpha)$ is

well approximable. In the converse situation, we have $\alpha \in \mathfrak{m}$ and $|f(\alpha)|$ is small such that such values of α contribute only to the error term in (2.1.4).

2.2.1 The treatment of the minor arcs

In order to prove (2.1.4), we want to show that

$$\int_{\mathfrak{m}} := \int_{\mathfrak{m}} (f(\alpha))^s e(-\alpha N) d\alpha = o(N^{s/k-1}). \quad (2.2.2)$$

There are two important tools to do so.

First, when $\alpha \in \mathfrak{m}$, we need a non-trivial bound for $|f(\alpha)|$. Let $\alpha \in \mathbb{R}$ and suppose a and q are coprime integers such that $|\alpha - a/q| \leq q^{-2}$. Notice that this approximation is always possible due to Dirichlet's approximation theorem (see e.g. [9, Satz 6.4.2]). In 1916, Hermann Weyl [81] proved that

$$f(\alpha) \ll P^{1+\varepsilon} \left(P^{-1/K} + q^{-1/K} + \left(\frac{P^k}{q} \right)^{-1/K} \right) \quad (2.2.3)$$

holds for every $\varepsilon > 0$. Here we define $K := 2^{k-1}$. Notice that this is better than the the trivial estimate $|f(\alpha)| \leq P$ provided that $P^\delta \leq q \leq P^{k-\delta}$ for some $\delta > 0$. This motivates the definition of major and minor arcs above. Indeed, for all $\alpha \in \mathfrak{m}$, the estimate (2.2.3) is non-trivial. The proof of Weyl's result (2.2.3) makes use of an ingenious application of the Cauchy-Schwarz-Bunyakovsky inequality.

We want to assume that $s > 2^k$. Taking absolute values of the integrand in (2.2.2) we get

$$\int_{\mathfrak{m}} \ll \left(\sup_{\alpha \in \mathfrak{m}} |f(\alpha)| \right)^{s-2^k} \int_0^1 |f(\alpha)|^{2^k} d\alpha.$$

As already mentioned, the supremum can be bounded non trivially by Weyl's Inequality (2.2.3). In order to prove (2.2.2), we have to bound the integral in the last display non-trivial which is the matter of the next paragraph.

The second tool is known as Hua's Lemma. Recall that for any complex c , we have $|c|^2 = c\bar{c}$. With this in mind and (2.2.1), one can easily see that

$$\int_0^1 |f(\alpha)|^{2^k} d\alpha$$

equals the number of solutions of

$$x_1^k + \dots + x_{2^{k-1}}^k = x_{2^{k-1}+1}^k + \dots + x_{2^k}^k$$

in integers $x_i \leq P$ for $i = 1, 2, \dots, 2^k$. In 1938, Loo-keng Hua [45] showed by induction on k that for every $\varepsilon > 0$, we have

$$\int_0^1 |f(\alpha)|^{2^k} d\alpha \ll P^{2^k - k + \varepsilon}. \quad (2.2.4)$$

This estimate together with Weyl's result yields (2.2.2). Improvements on the upper bound for $G(k)$ are mostly due to refinements of the result (2.2.4). However, if we have only a poor version of Weyl's Inequality in the form $f(\alpha) = o(P)$ for $\alpha \in \mathfrak{m}$, then we need a strong version of (2.2.4) with $\varepsilon = 0$ which is true due to Vaughan [70]. However, the exponent 2^k in (2.2.4) is essential in Vaughan's strong version of Hua's Lemma. Later, we will pose certain restrictions to the variables x_i in (2.1.1). In this case we only have $f(\alpha) = o(P)$ for $\alpha \in \mathfrak{m}$ and the bound $G(k) \leq 2^k + 1$ can not be improved, since Vaughan's results has not been refined yet.

2.2.2 The treatment of the major arcs

To show an asymptotic formula of the form (2.1.1), we need to prove

$$\int_{\mathfrak{M}} (f(\alpha))^s e(-\alpha N) d\alpha \sim \mathfrak{S}^*(N) N^{s/k-1}.$$

Now, suppose that $\alpha \in \mathfrak{M}$. Then there are coprime integers a, q with $1 \leq a \leq q \leq P^\delta$ such that $|\alpha - a/q| \leq p^{-k+\delta}$. That means that α is well approximable by a/q . Let $\beta := \alpha - a/q$. The first idea of the treatment of the major arcs is to make a transformation of the form $f(a/q + \beta) \sim f_1(a/q)f_2(\beta)$ in order to decouple a/q and β . This can be done due to the condition that q is not too large by using partial summation. For the sake of simplicity, we do not define the function f_1

and f_2 in this introduction. Roughly speaking, we have

$$f_1(a/q) \sim f(a/q) \sim \frac{P}{q} \sum_{x=1}^q e\left(\frac{ax^k}{q}\right).$$

The sum in the last display is called a Gauss–sum and is usually denoted by $S(q, a)$. With this strategy, we raise $f_1(a/q)f_2(\beta)$ to the power of s , multiply by $e(-(a/q + \beta)N)$, integrate over β and sum over a, q according to the definition of the major arcs \mathfrak{M} . Very approximately speaking, this procedure yields

$$\int_{\mathfrak{M}} \sim CN^{s/k-1} \mathfrak{S}(N),$$

for some $C > 0$. Here, $CN^{s/k-1}$ is a result of the integration over β as described above. The arithmetic function $\mathfrak{S}(N)$ results from the contributions of $f(a/q)$. More precisely, the method yields

$$\mathfrak{S}(N) = \sum_{q \geq 1} T(q, N),$$

where we define

$$T(q, N) := \sum_{\substack{a=1 \\ (a,q)=1}}^q \left(\frac{S(a, q)}{q}\right)^s e\left(-\frac{a}{q}N\right).$$

In order to show (2.1.1), we need to show that $\mathfrak{S}(N) > 0$. To do so, one verifies that $T(q, N)$ is multiplicative in q . Thus we obtain

$$\mathfrak{S}(N) = \prod_p T(p, N).$$

Notice

$$\sum_{\substack{a=1 \\ (a,q)=1}}^q e\left(\frac{ab}{q}\right) = \begin{cases} q & \text{if } b \equiv 0 \pmod{q} \\ 0 & \text{else,} \end{cases}$$

the discrete analogue of (2.2.1). With this in mind, we recall the definition of $S(q, a)$. Thus, one can argue that the final task in order to prove an asymptotic formula is to show that for all all prime p , the equation

$$x_1^k + \dots + x_s^k \equiv N \pmod{p^\eta} \tag{2.2.5}$$

has a solution with $p \nmid x_1$. As a consequence, we obtain $\mathfrak{S}(N) > 0$. Here, η is can be defined dependent on p and k . To prove that (2.2.5) has a solution with $p \nmid x_1$, one makes use of generalization of a Theorem of Augustin Cauchy [13] from 1813. He proved that for a given prime p and non-zero integers u, v, w the equation $ux^2 + vy^2 + w \equiv 0 \pmod{p}$ has solution. This theorem was used by Lagrange in order to establish his four squares theorem. Cauchy's result was reproved and extended by Harold Davenport [18] in 1935. He proved that for $A, B \subset \mathbb{Z} \setminus (p\mathbb{Z})$ with $\alpha := \#A$ and $\beta := \#B$, we have

$$\{a + b \pmod{p} \mid a \in A, b \in B\} \geq \min\{p, \alpha + \beta - 1\}.$$

In 1936, Inder Chowla [14] extended this result to composite moduli. This results are interesting for itself and they are an useful tool in order to conclude the proof of the asymptotic formula (2.1.4).

3 Hybrid structures

A central topic in number theory is the question if certain properties among the integers are in some sense independent or not. A first easy example is the following application of the so called Chinese remainder theorem. For coprime integers a, b and $v, w \in \mathbb{N}$, we define

$$A := \{n \in \mathbb{N} : n \equiv v \pmod{a}\},$$

and

$$B := \{n \in \mathbb{N} : n \equiv w \pmod{b}\},$$

Clearly, $\#\{n \leq X : n \in A\}/X \sim 1/a$ and $\#\{n \leq X : n \in B\}/X \sim 1/b$. By the Chinese remainder theorem, we get

$$\frac{\#\{n \leq X : n \in A \cap B\}}{X} \sim \frac{1}{ab}.$$

Abusing the language of probability theory, the probability that a random integer n is an element of A respectively B is $1/a$ respectively $1/b$. The Chinese remainder theorem yields that the probability for $n \in A \cap B$ is $1/(ab)$. Hence, the events $a \in A$ and $b \in B$ are in this sense independent.

An other example of such independent or hybrid structures are square-free integers. Let p be a prime. Notice that

$$\frac{\#\{n \leq X : p^2 \nmid n\}}{X} \sim \left(1 - \frac{1}{p^2}\right).$$

Let p_1, p_2 be two distinct given prime numbers. If we assume that for a random integer n the events $p_1^2 \nmid n$ and $p_2^2 \nmid n$ are independent in the sense suggested above, we conclude for the density of squarefree integers

$$\begin{aligned} \lim_{X \rightarrow \infty} \frac{\#\{n \leq X : n \text{ is squarefree}\}}{X} &= \prod_{\text{all primes } p} \left(1 - \frac{1}{p^2}\right) \\ &= \frac{6}{\pi^2}. \end{aligned}$$

This heuristic statement is indeed true.

As a last famous example of such hybrid results, we want to mention

the Siegel–Walfisz theorem [77] that shows that for a integer n , the events n is prime and n is an element of a given arithmetic progression are in a certain sense independent. More precisely, one has

$$\#\{p \leq X : p \text{ prime and } p \equiv a \pmod{q}\} \sim \frac{1}{\varphi(q)} \frac{X}{\log X},$$

where a, q are given coprime integers.

Here, such results show that certain properties among all integers are independent. The purpose of this work is to generalize this approach of studying such hybrid structures. We want to investigate if among solutions of Waring’s Problem certain properties are independent. Assume that $\mathcal{C} \subset \mathbb{N}$ is a set of positive density c . That is that

$$c := \lim_{X \rightarrow \infty} \frac{\#\{n \leq X : n \in \mathcal{C}\}}{X}$$

exists and is positive. Notice that for instance the set

$$\bigcup_{n \geq 1} \{2^{2n-1}, 2^{2n-1} + 1, 2^{2n-1} + 3, \dots, 2^{2n} - 1\}$$

does not have a density. However, we want to focus on sets that do have a density. Recall the definition of $R_{s,k}(N)$ on page 12. Let $R_{\mathcal{C};s,k}(N)$ be the number of solutions of (2.1.1) with $x_i \in \mathcal{C}$ for $i = 1, 2, \dots, s$. The statement that the events $(x_1, \dots, x_s) \in A^s$ and $(x_1, \dots, x_s) \in \mathbb{N}^s$ is a solution of (2.1.1) are independent can be formulated as

$$R_{\mathcal{C};s,k}(N) \sim c^s R_{s,k}(N).$$

Clearly, this is in general not true. For example the set of even integers has density $1/2$. But if N is odd, than N can not be represented as a sum of powers of even integers. However, one can often show that besides such trivial exceptional cases results of independence indeed hold.

3.1 Dense sets

We want to recall Hilbert’s result mentioned on page 12 that for any given k , one finds some integer s such that for any integer N , the equation

(2.1.1) has at least one solution in integers x_i for $i = 1, 2, \dots, s$. Notice that this result does not imply an asymptotic formula. This result can be generalized in the following way that gives some weak but general insight on hybrid structures as introduced in Section 3. For details we refer the reader to Remark 3.4 of a paper of Thuswaldner and Tichy [65].

Assume that $\mathcal{A} \subset \mathbb{N}$ has positive density. Let $k \in \mathbb{N}$. Under the condition that for all primes p there are integers $a_p, b_p \in \mathcal{A}$ such that $p|a_p$ and $p \nmid b_p$, there is some integer s such that for all $N \in \mathbb{N}$ equation (2.1.1) has a solution with $x_i \in \mathcal{A}$ for $i = 1, 2, \dots, s$.

Notice that this approach does only give a poor bound for the size of s . Besides, no asymptotic formula is obtained.

Our results presented in this work also deal with some dense sets $\mathcal{B} \subset \mathbb{N}$. But the condition that for all primes p there are integers $a_p, b_p \in \mathcal{B}$ such that $p|a_p$ and $p \nmid b_p$ does not hold in the cases of the set \mathcal{B} that we are interested in. We pose some multiplicative conditions to the set \mathcal{B} that imply the existence of primes that do not divide any element of \mathcal{B} .

Part B:
Waring's Problem and convergent sieve sequences

4 Results and context

4.1 Convergent sieve sequences

Many sequences in number theory arise from a sieving process. One of the fundamental invariants associated with a sieve is its dimension, usually denoted by κ . Here, we want to investigate the case $\kappa = 0$, i.e. convergent sieves. With applications in mind, we consider a slightly more general situation.

Let \mathcal{V} be a set of pairwise coprime integers not containing 1. We assume that there is some $0 < \delta < 1$ such that

$$\sum_{v \in \mathcal{V}} \frac{1}{v^{1-\delta}} < \infty. \quad (4.1.1)$$

This generates a sifted sequences whose characteristic function is given by

$$\chi_{\mathcal{V}}(n) := \begin{cases} 1, & \text{if } v \nmid n \text{ for all } v \in \mathcal{V}; \\ 0, & \text{otherwise.} \end{cases} \quad (4.1.2)$$

If \mathcal{V} is a set of primes, we shall also use the letter \mathcal{P} .

The notion of the set $\{n \in \mathbb{N} : \chi_{\mathcal{V}}(n) = 1\}$ has been introduced by Erdős [25]. The distribution of this set in residue classes has been studied by Jancevskis [48]. Alkan and Zaharescu [2] investigated the problem of finding integers n in short arithmetic progressions such that $\chi_{\mathcal{V}}(n) = 1$. An integer n satisfying $\chi_{\mathcal{V}}(n) = 1$ is also called a \mathcal{V} -free number (e.g. in [2]).

One of the most prominent examples of such a convergent sieve sequence is the set of k numbers with an integer $k \geq 2$. In this case, $\mathcal{V} = \{p^k : p \text{ prime}\}$, and (4.1.1) holds with $\delta = (k-1)/k + \varepsilon$. Among others, the distribution of squarefree numbers ($k = 2$) in arithmetic progressions has been studied by Prachar [61], Hooley [44], Warlimont [79], and Blomer [8].

For another example, fix an elliptic curve E/\mathbb{Q} without complex mul-

tiplication, and let $f_E(z) = \sum_n a(n)e(nz)$ be the associated modular form. Then the sequence of those squarefree indices n with $a(n) \neq 0$ is again a convergent sieve sequence (see e.g. [1]). Indeed, up to finitely many primes, \mathcal{V} is here the set of primes p such that the reduction of $E \bmod p$ is supersingular, together with the squares of the remaining primes; it is known (see [24]) that in this case (4.1.1) holds with $\delta = 1/4 - \varepsilon$.

For an overview over convergent sieves, in particular with respect to binary additive problems, see Brüdern's work [10]. For example, if \mathcal{P} is a set of primes such that $\sum_{p \in \mathcal{P}} 1/p < \infty$, a special case of [10, Theorem 1.10] states

$$\sum_{n \leq X} \chi_{\mathcal{P}}(n) \sim \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right) X.$$

This formula can be also motivated by an heuristic approach. The so called heuristic probability that a random integer is divisible by a prime p is $(1 - 1/p)$. If for a random integer n and two distinct primes p_1 and p_2 the heuristic events $p_1|n$ and $p_2|n$ are supposed to be independent, the formula in the last display is motivated.

The result in the last display was generalized to residue classes by Jancevskis [48, Theorem 1]. In particular, for a set \mathcal{P} of primes satisfying $\sum_{p \in \mathcal{P}} 1/p < \infty$ and for all $a, q \in \mathbb{N}$ with $(a, q) = 1$ and

$$(\log q)(\log \log q) = o(\log X)$$

one has

$$\sum_{\substack{n \leq X \\ n \equiv a \pmod{q}}} \chi_{\mathcal{P}}(n) \sim \prod_{\substack{p \in \mathcal{P} \\ p \nmid q}} \left(1 - \frac{1}{p}\right) \frac{X}{q}.$$

In this generality we cannot expect to get an explicit error term. However, it is interesting to note that the uniformity in q is much larger than in the classical theorem of Siegel-Walfisz.

It often gives useful information on a sequence a_n if one can understand the correlations of the type $\sum a_n a_{n+h}$ for fixed values of h . Let $\varepsilon > 0$, $0 < \delta < 1$, $q \in \mathbb{N}$ and \mathcal{P} be a set of prime numbers satisfying (4.1.1). Let l_i for $i = 1, 2, \dots, r$ be integers with $l_i \leq L$ and $q|l_i$. For any

prime p we define

$$u(p) := \#\{l_i \pmod p : i = 1, 2, \dots, r\}.$$

and

$$\mathcal{P}(q) := \mathcal{P} \cup \{p \text{ prime} : p|q\}.$$

For

$$S(X) := \sum_{\substack{n \leq X \\ (n, q) = 1}} \chi_{\mathcal{P}}(n + l_1) \cdot \dots \cdot \chi_{\mathcal{P}}(n + l_r)$$

Jancevskis [48, Theorem 3] showed that one has

$$S(X) \leq \prod_{p \in \mathcal{P}(q)} \left(1 - \frac{u(p)}{p}\right) X + O_r((qL)^\varepsilon X^{1-\delta/(2-\delta)+\varepsilon})$$

and

$$S(X) \geq \prod_{p \in \mathcal{P}(q)} \left(1 - \frac{u(p)}{p}\right) X + O_r \left(\min \left\{ \begin{array}{l} (qL)^\varepsilon X^{1-\delta/(3-\delta)+\varepsilon} + LX^{-1/(3-\delta)} \\ (qL)^\varepsilon X^{1-\delta^2+\varepsilon} + LX^{-\delta} \end{array} \right\} \right).$$

The O -constants depend upon r but are independent on L . For every $\delta > 0$ and $L \ll X$ is this result nontrivial. One of the main features here is the uniformity in L . It generalizes once again [10, Theorem 1.10] since our estimates are uniform in the shifts. Tsang [67] proved a similar result in the special case of squarefree numbers.

4.2 Waring's Problem

Waring's Problem with multiplicatively restricted variables has been widely studied. The most famous example is the so called Waring–Goldbach Problem, in which one asks if an integer can be represented as a sum of k -th powers of prime numbers. Among others, this problem has been studied by Hua [46], [47]; Kawada and Wooley [51]; Thanigasalam [63]; and Vinogradov [76]. Among others, Waring's Problem with smooth numbers has been explored by Balog and Sárközy [5] and Harcos [33]; Brüdern and Fouvry [11] showed Lagrange's Four Square Theorem where the variables are almost prime.

In this chapter we want to present results of Waring's Problem where the variables are restricted to a sifted sequences whose characteristic function is defined as in (4.1.2) above for a set \mathcal{V} of coprime integers not containing 1 that such that (4.1.1) holds.

In the case of square-free numbers, Esterman [28] investigated if an integer can be represented as a sum of squares of squarefree integers; Baker and Brüdern [3], [4] proved that almost all integers can be represented as a sum of four cubes of squarefree integers. Our purpose is to generalize this results to our sifted sequences for arbitrary k -th powers.

Let $s, k \in \mathbb{N}$. We denote by $R_{\mathcal{V}}(N)$ the number of solutions of

$$x_1^k + \dots + x_s^k = N \quad (4.2.1)$$

with $\chi_{\mathcal{V}}(x_1) = \dots = \chi_{\mathcal{V}}(x_s) = 1$.

In this chapter, the number of summands is only of secondary interest. Thus we assume for the sake of simplicity that $s > 2^k$. This bound is not best possible and the techniques of the present paper yield also results for smaller s . The range of s depends on the current state of results improving Hua's Lemma (for a survey, see e.g. [75]). Here, we only make use of the original form of Hua's Lemma (see e.g. [68, Lemma 2.5]). Our first result is the following:

Theorem 4.2.1. *Let \mathcal{V} be a set of pairwise coprime integers not containing 1 such that (4.1.1) is finite for some $\delta > 0$. Then there is some $\rho > 0$ such that*

$$R_{\mathcal{V}}(N) = J\mathfrak{S}_{\mathcal{V}}(N)N^{s/k-1} + O(N^{s/k-1-\rho}),$$

where $J > 0$ is defined in (5.2.18) below and only depends on s, k . The arithmetic function $\mathfrak{S}_{\mathcal{V}}(N)$, called the singular series, is defined in Lemma 5.2.6. The implicit O -constant only depends on s, k, δ , and ρ .

Unfortunately, we could not determine whether $\mathfrak{S}_{\mathcal{V}}(N) > 0$ for an arbitrary set \mathcal{V} of pairwise coprime integers. The difficulty lies in the fact that the function D associated with the singular series $\mathfrak{S}_{\mathcal{V}}(N) = \sum_{q \geq 1} D(q)$ might not be multiplicative if \mathcal{V} is not a set of prime powers (see Remark 5.3.2 after Lemma 5.3.1).

However, if we restrict \mathcal{V} to be a set of prime powers, we are able to provide a lower bound for $\mathfrak{S}_{\mathcal{V}}(N)$. In this case we write

$$\mathcal{W} =: \{p^{e_p} \mid p \in \mathcal{P}\}, \quad (4.2.2)$$

instead of \mathcal{V} , where \mathcal{P} is a subset of the prime numbers and (e_p) is a sequence of positive integers. Recall that we assume

$$\sum_{p \in \mathcal{P}} \frac{1}{(p^{e_p})^{1-\delta}} < \infty \quad (4.2.3)$$

for some $\delta > 0$ arbitrarily small. Without loss of generality, we can assume that $e_p \in \{1, 2\}$ for all $p^{e_p} \in \mathcal{W}$, since a solution with the variables not divisible by p^2 implies a solution with the variables not divisible by p^r with $r \geq 2$.

Next, we define a condition that is necessary for $\mathfrak{S}_{\mathcal{W}}(N) > 0$ to hold. We define τ by $p^\tau \parallel k$ and let $\sigma = \tau + 1$ if $p \neq 2$ and $\sigma = \tau + 2$ if $p = 2$. For an integer N , we say that (\mathcal{W}, N) satisfies Condition C if the following two conditions holds:

- For all p prime such that $p \in \mathcal{W}$ (i.e. $e_p = 1$) with $p \leq (k-1)^4 + 8k$ there is a solution of

$$x_1^k + \dots + x_s^k \equiv N \pmod{p^\sigma}$$

with $p \nmid x_1 \cdots x_s$.

- If $k = 2$ and $4 \in \mathcal{W}$, there is a solution of

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv N - 1 \pmod{8}$$

such that $4 \nmid x_i$ for $i = 1, 2, 3, 4$.

Theorem 4.2.2. *Let a set of prime powers \mathcal{W} be defined by (4.2.2). If (4.2.3) and Condition C hold, we have*

$$\mathfrak{S}_{\mathcal{W}}(N) > 0.$$

If we take \mathcal{W} as the set of the squares of all primes, we obtain the following corollary.

Corollary 4.2.3. *Let $s > 2^k$. Assume that $k \geq 3$. Then every sufficiently large integer can be represented as a sum of s k -th powers of squarefree integers. If $k = 2$, the same holds if there is a solution of $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv N - 1 \pmod{8}$ with $4 \nmid x_i$ for $i = 1, 2, 3, 4$.*

If we sieve with primes, we have to be aware that the first part of Condition C does not hold in general. For example, if $k - 1 = p \in \mathcal{W}$, then $x^k \equiv 1 \pmod{p}$ for all $p \nmid x$. Thus $N \equiv s \pmod{p}$ is necessary for Condition C . If $2k + 1 = p \in \mathcal{W}$, then $x^k \equiv \pm 1 \pmod{p}$ for $p \nmid x$ and Condition C cannot hold if s is even and $N \equiv 0 \pmod{p}$. We illustrate this for the case $k = 2$. In this case, we have to check Condition C for $p \leq 17$ by an easy computation.

Corollary 4.2.4. *Let \mathcal{P} be a set of prime numbers and assume that there is some $\delta > 0$ such that*

$$\sum_{p \in \mathcal{P}} \frac{1}{p^{1-\delta}}$$

converges. Let $N \in \mathbb{N}$ and assume $N \equiv 5 \pmod{8}$ if $2 \in \mathcal{P}$ and $N \equiv 2 \pmod{3}$ if $3 \in \mathcal{P}$. If N is sufficiently large, it can be represented as a sum of five squares of integers not being divisible by any prime of \mathcal{P} .

To prove Theorem 4.2.1, we make use of the classical circle method. The main part of this paper is the proof of Theorem 4.2.2 which is motivated by a work of Baker and Brüdern [3].

5 Proofs

5.1 Preliminary considerations

Let $P := N^{1/k}$ and let \mathcal{V} be a set of pairwise coprime positive integers not containing 1. Throughout this section, we define

$$f(\alpha) = \sum_{\substack{x \leq P \\ \chi_{\mathcal{V}}(x)=1}} e(\alpha x^k).$$

Recall that $e(\theta)$ stands for $e^{2\pi i\theta}$. Remember that $R_{\mathcal{V}}(N)$ is the number of solutions of (4.2.1) with $\chi_{\mathcal{V}}(x_1) = \dots = \chi_{\mathcal{V}}(x_s) = 1$. Applying the fundamental formula (2.2.1) as described in Section 2.2 yields

$$R_{\mathcal{V}}(N) = \int_0^1 f(\alpha)^s e(-\alpha N) d\alpha. \quad (5.1.1)$$

We define

$$\Pi(\mathcal{V}) := \left\{ n = \prod_{v \in \mathcal{V}'} v : \mathcal{V}' \text{ is a finite subset of } \mathcal{V} \right\}$$

and

$$\mu_{\mathcal{V}}(n) := \begin{cases} (-1)^{\#\mathcal{V}'}, & \text{if } n \in \Pi(\mathcal{V}) \text{ with } n = \prod_{v \in \mathcal{V}'} v, \\ 0, & \text{otherwise,} \end{cases}$$

a variant of the well known Möbius μ -function. Notice that $1 \in \Pi(\mathcal{V})$, since we define the empty product as 1.

Lemma 5.1.1. *For an integer n , we have*

$$\chi_{\mathcal{V}}(n) = \sum_{\substack{m \in \Pi(\mathcal{V}) \\ m|n}} \mu_{\mathcal{V}}(m).$$

Proof. The proof of this convolution formula is very similarly to the well know identity $\mu^2(n) = \sum_{d^2|n} \mu(n)$. We first assume that $\chi_{\mathcal{V}}(n) = 1$ for $n \in \mathbb{N}$. In this case, the right hand side of the last display simplifies to

$\mu_{\mathcal{V}}(1) = 1$, since for all $1 \neq v \in \Pi(\mathcal{V})$, we have $v \nmid n$. Now, we assume that $\chi_{\mathcal{V}}(n) = 0$. Let $\tilde{\mathcal{V}} \subset \mathcal{V}$ be defined via $m \in \tilde{\mathcal{V}} \Leftrightarrow m|n$. Thus

$$\sum_{\substack{m \in \Pi(\mathcal{V}) \\ m|n}} \mu_{\mathcal{V}}(m) = \sum_{m \in \Pi(\tilde{\mathcal{V}})} \mu_{\mathcal{V}}(m) = \sum_{j=1}^{\#\tilde{\mathcal{V}}} (-1)^j \binom{\#\tilde{\mathcal{V}}}{j} = 0,$$

and the statement is proved. \square

Lemma 5.1.2. *Let $0 \leq \delta < 1$. If*

$$\sum_{v \in \mathcal{V}} \frac{1}{v^{1-\delta}}$$

is finite, then

$$\sum_{\substack{d \geq 1 \\ d\xi \in \Pi(\mathcal{V})}} \frac{1}{d^{1-\delta}} \ll 1$$

holds uniformly for all $\xi \in \mathbb{N}$.

Proof. For arbitrary $\xi \in \mathbb{N}$ we define

$$\xi_0 := \prod_{\substack{v \in \mathcal{V} \\ (v, \xi) > 1}} \frac{v}{(v, \xi)}$$

and

$$\mathcal{V}_{\xi} := \{v \in \mathcal{V} | (v, \xi) = 1\} \cup \{\xi_0\}.$$

Let $d \geq 1$. If $d\xi \in \Pi(\mathcal{V})$, there is a finite subset \mathcal{V}' of \mathcal{V} such that

$$d\xi = \prod_{\substack{v \in \mathcal{V}' \\ (v, \xi) = 1}} v \prod_{\substack{v \in \mathcal{V}' \\ (v, \xi) > 1}} v. \quad (5.1.2)$$

Since \mathcal{V} is a set of pairwise coprime integers, one has

$$\prod_{\substack{v \in \mathcal{V}' \\ (v, \xi) > 1}} v = \prod_{\substack{v \in \mathcal{V} \\ (v, \xi) > 1}} v = \xi \prod_{\substack{v \in \mathcal{V} \\ (v, \xi) > 1}} \frac{v}{(v, \xi)} = \xi \xi_0.$$

Hence we get by (5.1.2) that

$$d = \xi_0 \prod_{\substack{v \in \mathcal{V}' \\ (v, \xi) = 1}} v.$$

Thus $d\xi \in \Pi(\mathcal{V})$ implies $d \in \Pi(\mathcal{V}_\xi)$ and consequently

$$\sum_{\substack{d \geq 1 \\ d\xi \in \Pi(\mathcal{V})}} \frac{1}{d^{1-\delta}} \leq \sum_{\substack{d \geq 1 \\ d \in \Pi(\mathcal{V}_\xi)}} \frac{1}{d^{1-\delta}}. \quad (5.1.3)$$

One has

$$\sum_{v \in \mathcal{V}_\xi} \log \left(1 + \frac{1}{v^{1-\delta}} \right) \leq \sum_{v \in \mathcal{V}_\xi} \frac{1}{v^{1-\delta}} \leq \sum_{v \in \mathcal{V}} \frac{1}{v^{1-\delta}} + 1. \quad (5.1.4)$$

By our assumption, the right hand side of (5.1.4) is finite. Thus

$$\exp \left(\sum_{v \in \mathcal{V}_\xi} \log \left(1 + \frac{1}{v^{1-\delta}} \right) \right) = \prod_{v \in \mathcal{V}_\xi} \left(1 + \frac{1}{v^{1-\delta}} \right) = \sum_{d \in \Pi(\mathcal{V}_\xi)} \frac{1}{d^{1-\delta}}$$

is finite and the lemma follows from (5.1.3). \square

Lemma 5.1.3. *Let $0 \leq \delta < 1$. If*

$$\sum_{v \in \mathcal{V}} 1/v^{1-\delta}$$

is finite, then

$$\sum_{\substack{d < Y \\ d \in \Pi(\mathcal{V})}} 1 \ll Y^{1-\delta}, \quad \sum_{\substack{d > Y \\ d \in \Pi(\mathcal{V})}} \frac{1}{d} \ll Y^{-\delta}, \quad (5.1.5)$$

and

$$\sum_{d \in \Pi(\mathcal{V})} \frac{\mu_{\mathcal{V}}(d)}{d} = \prod_{v \in \mathcal{V}} \left(1 - \frac{1}{v} \right) \quad (5.1.6)$$

holds.

Proof. The first statement of (5.1.5) follows from

$$\sum_{\substack{d \leq Y \\ d \in \Pi(\mathcal{V})}} 1 \leq \sum_{\substack{d \geq 1 \\ d \in \Pi(\mathcal{V})}} \frac{Y^{1-\delta}}{d^{1-\delta}}$$

and Lemma 5.1.2 with $\xi = 1$. The proof of the second statement of (5.1.5) is similar. Formula 5.1.6 is due to Euler's Product Formula (see [40, § 17.2]). \square

5.2 Asymptotic formula

Let $\eta > 0$ be sufficiently small and be specified later. As in the classical case of Waring's Problem (see e.g. [21, page 15 ff.] and Chapter 2.2), let the major arcs \mathfrak{M} be the union of the major arcs

$$\mathfrak{M}(q, a) := \left\{ \alpha \in [0, 1] : \left| \alpha - \frac{a}{q} \right| \leq P^{-k+\eta} \right\}$$

with $1 \leq a \leq q \leq P^\eta$ and $(a, q) = 1$, and let $\mathfrak{m} := [0, 1] \setminus \mathfrak{M}$ be the minor arcs.

5.2.1 Minor arcs

Our next aim is to show that the integral in (5.1.1) restricted to the minor arcs \mathfrak{m} is $O(N^{s/k-1-\rho})$. To do so, we need a variant of Weyl's inequality.

Lemma 5.2.1. *Let $X, Y, \alpha \in \mathbb{R}$ such that $X \geq 1$, $Y \geq 1$, $\alpha > 0$ and $|\alpha - a/q| \leq q^{-2}$, where a and q are positive coprime integers. Then we have*

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

Proof. See e.g. [68, Lemma 2.2]. \square

For coprime integers a, q let $\alpha \in \mathbb{R}$ satisfy $|\alpha - a/q| \leq q^{-2}$. Let

$K = 2^{k-1}$. By Weyl's classical inequality (see e.g. [68, p. 12]), we get

$$\left| \sum_{x \leq P/d} e(\alpha d^k x^k) \right|^K \ll (P/d)^{K-k+\varepsilon} \left((P/d)^{k-1} + \sum_{h \leq k!(P/d)^{k-1}} \min \left\{ (P/d)^k h^{-1}, \|\alpha d^k h\|^{-1} \right\} \right).$$

We substitute $y := d^k h$ in the h -sum above and extend the summation. Thus, the h -sum is less than

$$\sum_{y \leq k!P^k} \min \{ P^k y^{-1}, \|\alpha y\|^{-1} \} \ll P^{k+\varepsilon} \left(\frac{1}{q} + \frac{q}{P^k} \right),$$

where we made use of Lemma 5.2.1 with $Y = 1$ and $X = k!p^k$. Thus we showed

$$\begin{aligned} \sum_{x \leq P/d} e(\alpha d^k x^k) &\ll \left(P^{K-k+\varepsilon} \left(P^{k-1} d^{-K} + P^{k+\varepsilon} \left(\frac{1}{q} + \frac{q}{P^k} \right) \right) \right)^{1/K} \\ &\ll P^{1+\varepsilon} \left(\frac{1}{P} + \frac{1}{q} + \frac{q}{P^k} \right)^{1/K} \end{aligned} \quad (5.2.1)$$

Notice that the implicit O -constant does not depend on d . Now, we are able to prove the next lemma by following [3, Lemma 1].

Lemma 5.2.2. *Suppose that $s > 2^k$. Then there is some $\rho > 0$ only dependent on η, s and k such that*

$$\int_{\mathfrak{m}} f(\alpha)^s e(-\alpha N) d\alpha \ll N^{s/k-1-\rho}.$$

Proof. Notice that Lemma 5.1.1 yields

$$f(\alpha) = \sum_{\substack{d \leq P \\ d \in \Pi(\mathcal{V})}} \mu_{\mathcal{V}}(d) \sum_{x \leq P/d} e(\alpha d^k x^k). \quad (5.2.2)$$

Since $s > 2^k$, one has

$$\int_{\mathfrak{m}} f(\alpha)^s e(-\alpha N) d\alpha \leq \left(\sup_{\alpha \in \mathfrak{m}} \{|f(\alpha)|\} \right)^{s-2^k} \int_0^1 |f(\alpha)|^{2^k} d\alpha. \quad (5.2.3)$$

We have further

$$\begin{aligned} & \int_0^1 |f(\alpha)|^s d\alpha \\ & \leq \#\{x_1, y_1, \dots, x_{2^k-1}, y_{2^k-1} \mid x_1 + \dots + x_{2^k-1} = y_1 + \dots + y_{2^k-1}\} \\ & \ll P^{2^k-k} \end{aligned} \quad (5.2.4)$$

by [70, Theorem 2]. Recall formula (5.2.2).

Let $\alpha \in \mathfrak{m}$. By Dirichlet's Approximation Theorem, there exists co-prime integers a, q with $q \leq P^{k-\eta}$ and $|\alpha - a/q| \leq 1/qP^{k-\eta}$. Since $q \leq P^\eta$ implies $\alpha \in \mathfrak{M}(a, q)$, we have $P^\eta < q \leq P^{k-\eta}$.

Let $\beta > 0$ such that $\beta\delta < \eta/K$. By (5.2.1), we have

$$\begin{aligned} \sum_{\substack{d \leq P^\beta \\ d \in \Pi(\mathcal{V})}} \sum_{x \leq P/d} e(\alpha d^k x^k) & \ll \sum_{\substack{d \leq P^\beta \\ d \in \Pi(\mathcal{V})}} P^{1-\eta/K+\varepsilon} \\ & \ll P^{1-\eta/K+\beta\delta+\varepsilon}. \end{aligned} \quad (5.2.5)$$

For the last estimation, we made use of Lemma 5.1.3. On the other hand

$$\sum_{\substack{d > P^\beta \\ d \in \Pi(\mathcal{V})}} \sum_{x \leq P/d} e(\alpha d^k x^k) \ll P^{1-\delta\beta} \quad (5.2.6)$$

by trivial estimates and again Lemma 5.1.3. Recall $\beta\delta < \eta/K$. Thus the estimates (5.2.5), and (5.2.6) together with (5.2.2) yields

$$f(\alpha) \ll P^{1-\rho'}$$

for some $\rho' > 0$. By this and (5.2.4), and (5.2.3) the lemma follows. \square

5.2.2 Major arcs

By applying (5.2.2), we verify that the integral in (5.1.1) restricted to the major arcs \mathfrak{M} equals

$$\sum_{\substack{d_1, \dots, d_s \leq P \\ d_1, \dots, d_s \in \Pi(\mathcal{V})}} \mu_{\mathcal{V}}(d_1) \cdots \mu_{\mathcal{V}}(d_s) \int_{\mathfrak{M}} f_{d_1}(\alpha) \cdots f_{d_s}(\alpha) e(-\alpha N) d\alpha \quad (5.2.7)$$

with

$$f_d(\alpha) := \sum_{x \leq P/d} e(\alpha d^k x^k).$$

Let $\gamma > 0$ sufficiently small. We defer the choice of y . We split (5.2.7) into a part where $d_1, \dots, d_s \leq P^\gamma$ and a remaining part U where there is at least one $1 \leq i \leq s$ such that $d_i > P^\gamma$. Now, we want to bound $|U|$. We have

$$U \ll P^{s-2k-1} \sum_{\substack{d > P^\gamma \\ d \in \Pi(\mathcal{V})}} \frac{P}{d} \int_0^1 \left| \sum_{\substack{d \leq P \\ d \in \Pi(\mathcal{V})}} \sum_{x \leq P/d} e(\alpha d^k x^k) \right|^{2k} d\alpha.$$

The integral is bounded by the number of solutions of

$$(d_1 x_1)^k + \dots + (d_{2^{k-1}} x_{2^{k-1}})^k = (d_{2^{k-1}+1} x_{2^{k-1}+1})^k + \dots + (d_{2^k} x_{2^k})^k \quad (5.2.8)$$

with $d_i x_i \leq P$. Notice that there are $O(P^\varepsilon)$ possibilities to write an integer $y \leq P$ as a produkt of two integers. Hence the number of solutions of (5.2.8) is bounded by $O(P^\varepsilon)$ times the number of solutions of

$$y^k + \dots + y_{2^{k-1}}^k = y_{2^{k-1}+1}^k + \dots + y_{2^k}^k$$

Applying Hua's Lemma, the number of solutions of (5.2.8) is thus at most of order $P^{2^k - k + \varepsilon}$. Recall that by Lemma 5.1.3, we have

$$\sum_{\substack{d > P^\gamma \\ d \in \Pi(\mathcal{V})}} \frac{1}{d} \ll P^{\delta\gamma}.$$

Thus we have $U \ll N^{s/k-1-\rho}$ for some $\rho > 0$. Now, by this and Lemma 5.2.2, we obtain the following lemma.

Lemma 5.2.3. *Let $\gamma > 0$. Then there is some $\rho > 0$ such that*

$$R_{\mathcal{V}}(N) = \sum_{\substack{d_1, \dots, d_s \leq P^\gamma \\ d_1, \dots, d_s \in \Pi(\mathcal{V})}} \mu_{\mathcal{V}}(d_1) \cdots \mu_{\mathcal{V}}(d_s) \int_{\mathfrak{M}} f_{d_1}(\alpha) \cdots f_{d_s}(\alpha) e(-\alpha N) d\alpha \\ + O(N^{s/k-1-\rho}).$$

Let $1 \leq a \leq q \leq P^\eta$ with $(a, q) = 1$ and $\alpha \in \mathfrak{M}(a, q)$. Define $\beta := \alpha - a/q$,

$$S(q, b) := \sum_{m=1}^q e\left(\frac{bm^k}{q}\right),$$

and

$$I(\beta) := \int_0^P e(\beta u^k) du.$$

Lemma 5.2.4. *With the definitions above, we have*

$$f_d(\alpha) = \frac{S(q, ad^k)}{qd} I(\beta) + O(P^{2\eta}) \quad (5.2.9)$$

uniformly in all integers d .

Proof. We want to generalize formula

$$\sum_{x \leq P} e(\alpha x^k) = \frac{S(q, a)}{q} I(\beta) + O(P^{2\eta})$$

which is well known (see e.g [21, Lemma 4.2]).

First, we assume that $\beta = 0$ and collect those values of the summations variable in $f(a/q)$ which are in the same residue class modulo p .

Hence

$$f_d(a/q) = \sum_{z=1}^q e\left(\frac{a}{q}d^k z^k\right) \sum_{\substack{\ell \leq P/d \\ \ell \equiv z(q)}} 1.$$

The inner sum is $P/(qd) + O(1)$. Recall that $q \leq P^\eta$ and the definition of $S(q, ad^k)$. Thus

$$f_d(a/q) = \frac{S(q, ad^k)}{qd}P + O(P^\eta). \quad (5.2.10)$$

Now, we assume that $\beta \neq 0$. We have

$$f_d(a/q + \beta) = \sum_{x \leq P/d} e\left(\frac{a}{q}d^k x^k\right) e(\beta d^k x^k).$$

Summation by parts yields

$$\begin{aligned} f_d(\alpha) &= e(\beta P^k) f_d(a/q) \\ &\quad - 2\pi i \beta d^k k \int_0^{P/d} \xi^{k-1} e(\beta d^k \xi^k) \sum_{x \leq \xi} e\left(\frac{a}{q}d^k x^k\right) d\xi. \end{aligned} \quad (5.2.11)$$

The sum in the integral is

$$S(q, ad^k) \frac{\xi}{q} + O(q).$$

The error term $O(q) = O(P^\eta)$ in the last display causes an error term in (5.2.11) of the form

$$O\left(|\beta| d^k P^\eta \int_0^{P/d} \xi^{k-1} d\xi\right) = O(P^{2\eta}),$$

as $|\beta| \leq P^{-k+\eta}$, since $\alpha \in \mathfrak{M}(a, q)$. Note, that the error term does not

depend on d . By this and (5.2.10), we obtain

$$f_d(\alpha) = \frac{S(q, ad^k)}{qd} \left(e(\beta P^k) P - 2\pi i \beta d^{k-1} k \int_0^{P/d} \xi^k e(\beta d^k \xi^k) d\xi \right) + O(P^{2\eta}).$$

Notice, that by a simple substitution $\xi \mapsto \xi/d$, the integral in last display simplifies to

$$d^{k-1} \int_0^P \xi^k e(\beta \xi^k) d\xi.$$

Hence, the lemma follows if we can show

$$I(\beta) = e(\beta P^k) P - 2\pi i \beta k \int_0^P \xi^k e(\beta \xi^k) d\xi.$$

But this can be verified via integration by substitution. \square

Now introduce

$$\mathfrak{S}_{d_1, \dots, d_s}(P^\eta, N) := \sum_{q \leq P^\eta} \sum_{\substack{a=1 \\ (a, q)=1}}^q \frac{S(q, ad_1^k)}{qd_1} \dots \frac{S(q, ad_s^k)}{qd_s} e\left(-\frac{a}{q} N\right),$$

and

$$J(P^\eta) := \int_{|\beta| < P^\eta} \left(\int_0^1 e(\beta u^k) du \right)^s e(-\beta) d\beta. \quad (5.2.12)$$

Our next lemma is generalization of [21, Lemma 4.3]

Lemma 5.2.5. *With the definition above, we have*

$$\int_{\mathfrak{M}} f_{d_1}(\alpha) \dots f_{d_s}(\alpha) e(-\alpha N) d\alpha = \mathfrak{S}_{d_1, \dots, d_s}(P^\eta, N) J(P^\eta) N^{s/k-1} + O(P^{s-k-(1-5\eta)}) \quad (5.2.13)$$

uniformly in all integers d_1, \dots, d_s .

Proof. Let $\alpha \in \mathfrak{M}(a, q)$ for $1 \leq a \leq q \leq P^\eta$ with $(a, q) = 1$. Let $\beta := \alpha - a/q$. For s integers $d_1, \dots, d_s \leq P$, we multiply the right hand side of (5.2.9) together and obtain

$$f_{d_1}(\alpha) \cdots f_{d_s}(\alpha) = \left(\frac{S(q, ad_1^k)}{qd_1} \cdots \frac{S(q, ad_s^k)}{qd_s} \right) I(\beta)^s + O(P^{s-1+2\eta}),$$

as $S(q, ad_i^k)/(qd_i) \leq 1$ for all $i = 1, 2, \dots, s$ and $I(\beta) \leq P$. Recall that we have $|\beta| \leq P^{-k+\eta}$. Hence

$$\begin{aligned} & \int_{\alpha \in \mathfrak{M}(a, q)} f_{d_1}(\alpha) \cdots f_{d_s}(\alpha) e(\alpha N) d\alpha \\ &= \left(\frac{S(q, ad_1^k)}{qd_1} \cdots \frac{S(q, ad_s^k)}{qd_s} e\left(-\frac{a}{q}N\right) \right) \int_{|\beta| \leq P^{-k+\eta}} I(\beta)^s e(-\beta N) d\beta \\ & \quad + O(P^{s-k-1+3\eta}). \end{aligned}$$

Now, we can argue as in [21, p. 19 ff]. In particular, we sum over all coprime integers a, q with $1 \leq a \leq q \leq P^\eta$ and replace in the integrand N by P^k at the cost of a negligible error term. Finally, we substitute $\xi \mapsto P\xi$ and $\beta \mapsto P^{-k}\beta$ in order to obtain the stated formula. \square

Lemma 5.2.6. *The singular series*

$$\mathfrak{S}_\nu(N) := \sum_{q \geq 1} \sum_{\substack{a=1 \\ (a, q)=1}}^q \left(\sum_{d \in \Pi(\nu)} \mu_\nu(d) \frac{S(q, ad^k)}{dq} \right)^s e\left(-\frac{a}{q}N\right)$$

is absolutely convergent.

Proof. We go along the lines of [3, p. 5]. First, we need a bound for $|S(q, b)|$, where b, q are not necessarily coprime. One has

$$S(q, b) = (a, q) S\left(\frac{q}{(a, q)}, \frac{b}{(a, q)}\right).$$

Since $(q/(b, q), b/(b, q)) = 1$, we have

$$S\left(\frac{q}{(b, q)}, \frac{b}{(b, q)}\right) \ll \left(\frac{q}{(a, q)}\right)^{1-1/k}$$

by [21, Lemma 6.4] and consequently

$$S(q, b) \ll q^{1-1/k} (b, q)^{1/k}. \quad (5.2.14)$$

Let

$$\mathcal{S}_{q,a} := \sum_{d \in \Pi(\mathcal{V})} \mu_{\mathcal{V}}(n) \frac{S(q, ad^k)}{qd}.$$

One has

$$\begin{aligned} \mathcal{S}_{q,a} &\leq \sum_{d \in \Pi(\mathcal{V})} \frac{|S(q, ad^k)|}{qd} = \sum_{\xi|q} \sum_{\substack{d \in \Pi(\mathcal{V}) \\ (d,q)=\xi}} \frac{|S(q, ad^k)|}{qd} \\ &= \sum_{\xi|q} \sum_{\substack{\hat{d} \geq 1 \\ \hat{d}\xi \in \Pi(\mathcal{V}) \\ (\hat{d}, q/\xi)=1}} \frac{|S(q, a\hat{d}^k \xi^k)|}{q\hat{d}\xi}. \end{aligned} \quad (5.2.15)$$

Let $j \in \mathbb{N}$. Notice that

$$\left\{ j \frac{q\hat{d}}{\xi} + x\hat{d} \mid x = 1, 2, \dots, \frac{q}{\xi} \right\}$$

is a complete set of residues modulo (q/ξ) if $\xi|q$ and $(\hat{d}, q/\xi) = 1$. Thus

$$\begin{aligned} S(q, a\hat{d}^k \xi^k) &= \sum_{j=0}^{\xi-1} \sum_{x=1}^{q/\xi} e \left(\left(j \frac{q\hat{d}}{\xi} + x\hat{d} \right)^k \frac{a\xi^{k-1}}{q/\xi} \right) \\ &= \xi S(q/\xi, a\xi^{k-1}) \\ &= S(q, a\xi^k). \end{aligned}$$

Hence by (5.2.15),

$$\mathcal{S}_{q,a} \leq \sum_{\xi|q} \frac{|S(q, a\xi^k)|}{\xi q} \sum_{\substack{\hat{d} \geq 1 \\ \hat{d}\xi \in \Pi(\mathcal{V}) \\ (\hat{d}, q/\xi)=1}} \frac{1}{\hat{d}}.$$

Applying (5.2.14) and Lemma 5.1.2, we get

$$\mathcal{S}_{q,a} \ll q^{-1/k} \sum_{\xi|q} \frac{(q, \xi^k)^{1/k}}{\xi} \ll q^{-1/k+\varepsilon}. \quad (5.2.16)$$

Now, the lemma follows. In particular, we have

$$\begin{aligned} & \sum_{q \geq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^q \left(\sum_{d \in \Pi(\mathcal{V})} \mu_{\mathcal{V}}(d) \frac{S(q, ad^k)}{dq} \right)^s e\left(-\frac{a}{q}N\right) \\ & \ll Q^{2-s/k+\varepsilon} \end{aligned} \quad (5.2.17)$$

for any $Q > 0$, which will be useful later. \square

5.2.3 Proof of Theorem 4.2.1

Recall (5.2.12). We define the singular J like $J(P^\eta)$, but with outer integration over the whole real line, i.e. $J := J(\infty)$. This object has been well studied. One has

$$J = \frac{\Gamma(1 + 1/k)^s}{\Gamma(s/k)} > 0 \quad (5.2.18)$$

and

$$J - J(P^\eta) \ll P^{-(s/k-1)\eta} \quad (5.2.19)$$

by [21, p. 21].

We multiply both sides of (5.2.13) by $\mu_{\mathcal{V}}(d_1) \cdots \mu_{\mathcal{V}}(d_s)$ and sum over $d_1, \dots, d_s \leq P^\gamma$, $d_1, \dots, d_s \in \Pi(\mathcal{V})$, and obtain by Lemma 5.2.3 that $R(N)$ equals a main term

$$J(P^\eta) \sum_{q \leq P^\eta} \sum_{\substack{a=1 \\ (a,q)=1}}^q \left(\sum_{\substack{d \leq P^\gamma \\ d \in \Pi(\mathcal{V})}} \mu_{\mathcal{V}}(d) \frac{S(q, ad^k)}{qd} \right)^s e\left(-\frac{a}{q}N\right) N^{s/k-1} \quad (5.2.20)$$

and an error term $O(P^{s-k-(1-5\eta-s\gamma)})$. The error term is of the form stated

in the lemma if

$$5\eta + s\gamma < 1. \quad (5.2.21)$$

Next, we want to complete the d -sum in (5.2.20). Recall the estimates (5.1.5). Since $|S(q, ad^k)| \leq q$, we have

$$\sum_{\substack{d > N^\gamma \\ d \in \Pi(\mathcal{V})}} \frac{|S(a, qd^k)|}{qd} \ll P^{-\gamma\delta}.$$

Hence the completion of the d -sum engenders an additional error term $O(P^{s-k-(\gamma\delta-2\eta)})$ which is of the form stated in the lemma if

$$2\eta < \gamma\delta \quad (5.2.22)$$

holds. Thus we choose η and γ small enough so that both (5.2.21) and (5.2.22) are fulfilled, and deduce from (5.2.20) that there is some $\rho > 0$ such that

$$\begin{aligned} & R_{\mathcal{V}}(N) \\ &= J(P^\eta) \sum_{q \leq P^\eta} \sum_{\substack{a=1 \\ (a,q)=1}}^q \left(\sum_{\substack{d \geq 1 \\ d \in \Pi(\mathcal{V})}} \mu_{\mathcal{V}}(d) \frac{S(q, ad^k)}{qd} \right)^s e\left(-\frac{a}{q}N\right) N^{s/k-1} \\ &+ O(N^{s-k-\rho}). \end{aligned}$$

By (5.2.17), the completion of the singular series, e.g. the completion of the q -sum, creates an additional error which is negligible. Finally, by (5.2.19), replacing $J(P^\eta)$ by J yields a negligible error term, too.

5.3 The singular series

In this section, we restrict \mathcal{V} to be a set of prime powers and use the symbol \mathcal{W} instead.

We consider a more general singular series and generalize the procedure presented in [3] and [60]. We go along the lines of [3, Section 5]. For shortness, bold symbols are reserved to denote an element in \mathbb{N}^s , e.g. we

write $\mathbf{n} = (n_1, \dots, n_s)$ for an s -tuple of integers. Let $\varphi \in \mathbb{Z}[\mathbf{x}]$. We write

$$\begin{aligned}\varphi_{\mathbf{h}}(\mathbf{x}) &:= \varphi(h_1x_1, \dots, h_sx_s), \\ \mathbf{h}\mathbf{x} &:= (h_1x_1, \dots, h_sx_s),\end{aligned}$$

and further

$$\mu_{\mathcal{W}}(\mathbf{h}) := \mu_{\mathcal{W}}(h_1) \cdots \mu_{\mathcal{W}}(h_s)$$

for $\mathbf{x} = (x_1, \dots, x_s)$ and $\mathbf{h} = (h_1, \dots, h_s)$. For the sake of a short notation, if we use the index j in an expression, it is understood that j ranges over $1, \dots, s$. For instance $x_j \in A$ means $x_1 \in A, \dots, x_s \in A$ for $A \subset \mathbb{N}$. The symbol j is reserved for this usage only.

Besides, introduce

$$T(\varphi, q) := \sum_{x_j=1}^q e\left(\frac{\varphi(\mathbf{x})}{q}\right) = \sum_{x_j=1}^q \cdots \sum_{x_s=1}^q e\left(\frac{\varphi(x_1, \dots, x_s)}{q}\right)$$

and

$$A(\mathbf{d}, q) := \sum_{\substack{a=1 \\ (a,q)=1}}^q T(a\varphi_{\mathbf{d}}, q).$$

We fix $\varphi \in \mathbb{Z}[\mathbf{x}]$ to be the polynomial

$$\varphi(x_1, \dots, x_s) := x_1^k + \dots + x_s^k - N.$$

With this definitions, it is easy to see that we have

$$\mathfrak{S}_P(N) = \sum_{q \geq 1} \frac{1}{q^s} \sum_{d_j \in \Pi(\mathcal{W})} \frac{\mu_{\mathcal{W}}(\mathbf{d})}{d_1 \cdots d_s} A(\mathbf{d}, q), \quad (5.3.1)$$

where the singular series has been defined in Lemma 5.2.6.

5.3.1 Factorization

For every $q \in \mathbb{N}$, we subdivide \mathcal{W} into two disjoint sets

$$\mathcal{W}_q^+ := \{ v \mid v \in \mathcal{W} \text{ and } (v, q) > 1 \}$$

and

$$\mathcal{W}_q^- := \{ v \mid v \in \mathcal{W} \text{ and } (v, q) = 1 \}.$$

We omit the proof of the following lemma, which is trivial.

Lemma 5.3.1. *Let $q, q_1, q_2 \in \mathbb{N}$ with $(q_1, q_2) = 1$.*

- *Every integer $g \in \Pi(\mathcal{W})$ can be factorized uniquely in the form $g = dt$ with $d \in \Pi(\mathcal{W}_q^+)$ and $t \in \Pi(\mathcal{W}_q^-)$. In particular, we have $(d, t) = 1$ and $(t, q) = 1$.*
- *Every integer $g \in \Pi(\mathcal{W}_{q_1 q_2}^+)$ can be factorized uniquely in the form $g = dt$ with $d \in \Pi(\mathcal{W}_{q_1}^+)$ and $t \in \Pi(\mathcal{W}_{q_2}^+)$. One further has $(d, t) = 1$, $(d, q_2) = 1$ and $(t, q_1) = 1$.*

Remark 5.3.2. Note that the second part of this lemma is not valid if \mathcal{W} is replaced by a set \mathcal{V} of arbitrary coprime integers. For instance, let $\mathcal{V} = \{6\}$, then $6 \in \Pi(\mathcal{V}_6^+)$ does not factorize over $\Pi(\mathcal{V}_2^+) \cup \Pi(\mathcal{V}_3^+)$. This is the reason why we restrict ourselves to \mathcal{W} .

Lemma 5.3.3. *Let $q \in \mathbb{N}$. One has*

$$\sum_{d_j \in \Pi(\mathcal{W})} \frac{\mu_{\mathcal{W}}(\mathbf{d})}{d_1 \cdots d_s} A(\mathbf{d}, q) = C \prod_{v \in \mathcal{W}_q^+} \left(1 - \frac{1}{v}\right)^{-s} B(q), \quad (5.3.2)$$

where

$$B(q) := \sum_{d_j \in \Pi(\mathcal{W}_q^+)} \mu_{\mathcal{W}}(\mathbf{d}) \frac{A(\mathbf{d}, q)}{d_1 \cdots d_s},$$

and $C > 0$ is a constant only depending on the set \mathcal{W} .

Proof. This lemma is a generalization of [3, Lemma 7]. By the first part

of Lemma 5.3.1, the left hand side of (5.3.2) equals

$$\sum_{d_j \in \Pi(\mathcal{W}_q^+)} \sum_{t_j \in \Pi(\mathcal{W}_q^-)} \frac{\mu_{\mathcal{W}}(\mathbf{dt})}{d_1 \cdots d_s t_1 \cdots t_s} A(\mathbf{dt}, q). \quad (5.3.3)$$

Since $(d_{j_1}, t_{j_2}) = 1$ for all $j_1, j_2 \in \{0, 1, \dots, s\}$, we have $\mu_{\mathcal{W}}(\mathbf{dt}) = \mu_{\mathcal{W}}(\mathbf{d})\mu_{\mathcal{W}}(\mathbf{t})$ and $A(\mathbf{dt}, q) = A(\mathbf{d}, q)$ by the definition of $A(\mathbf{d}, q)$ and since $(t_j, q) = 1$ by the first part of Lemma 5.3.1. Hence (5.3.3) simplifies to

$$\sum_{d_j \in \Pi(\mathcal{W}_q^+)} \mu_{\mathcal{W}}(\mathbf{d}) \frac{A(\mathbf{d}, q)}{d_1 \cdots d_s} \sum_{t_j \in \Pi(\mathcal{W}_q^-)} \frac{\mu_{\mathcal{W}}(\mathbf{t})}{t_1 \cdots t_s}.$$

The inner multiple sum is the s -th power of

$$\sum_{t \in \Pi(\mathcal{W}_q^-)} \frac{\mu_{\mathcal{W}}(t)}{t} = \prod_{\substack{v \in \mathcal{W} \\ (v, q) = 1}} \left(1 - \frac{1}{v}\right) = C^{1/s} \prod_{\substack{v \in \mathcal{W} \\ (v, q) > 1}} \left(1 - \frac{1}{v}\right)^{-1}$$

with

$$C^{1/s} = \prod_{v \in \mathcal{W}} \left(1 - \frac{1}{v}\right) > 0.$$

□

Lemma 5.3.4. *The function $B(q)$ defined in Lemma 5.3.3 is multiplicative.*

Proof. Let

$$H(q, a) := \sum_{d_j \in \Pi(\mathcal{W}_q^+)} \frac{\mu_{\mathcal{W}}(\mathbf{d})}{d_1 \cdots d_s} T(a\varphi_{\mathbf{d}}, q).$$

Suppose we can show that

$$H(q_1 q_2, a_1 q_2 + a_2 q_1) = H(q_1, a_1) H(q_2, a_2) \quad (5.3.4)$$

holds for coprime integers q_1, q_2 and $(a_1, q_1) = (a_2, q_2) = 1$; then it follows

from the definition of $B(q)$ that

$$B(q_1, q_2) = \sum_{\substack{a_1=1 \\ (a_1, q_1)=1}}^{q_1} \sum_{\substack{a_1=1 \\ (a_1, q_1)=1}}^{q_1} H(q_1 q_2, a_1 q_2 + a_2 q_1) = B(q_1) B(q_2).$$

Thus it suffices to prove (5.3.4). By the second part of Lemma 5.3.1, we have

$$\begin{aligned} & H(q_1 q_2, a_1 q_2 + a_2 q_1) \\ = & \sum_{d_j \in \Pi(\mathcal{W}_{q_1}^+)} \frac{\mu_{\mathcal{W}}(\mathbf{d})}{d_1 \cdots d_s} \sum_{t_j \in \Pi(\mathcal{W}_{q_2}^+)} \frac{\mu_{\mathcal{W}}(\mathbf{t})}{t_1 \cdots t_s} T((a_1 q_2 + a_2 q_1) \varphi_{\mathbf{d}\mathbf{t}}, q_1 q_2). \end{aligned}$$

Notice $(d_{j_1}, t_{j_2}) = 1$ for all $j_1, j_2 \in \{0, 1, \dots, s\}$. Hence to prove (5.3.4) it suffices to show

$$T((a_1 q_2 + a_2 q_1) \varphi_{\mathbf{d}\mathbf{t}}, q_1 q_2) = T(a_1 \varphi_{\mathbf{d}}, q_1) T(a_2 \varphi_{\mathbf{t}}, q_2).$$

By the definition of T , the left hand side equals

$$\begin{aligned} & \sum_{x_j=1}^{q_1 q_2} e \left(\frac{a_1 q_2 + a_2 q_1}{q_1 q_2} ((d_1 t_1 x_1)^k + \dots + (d_s t_s x_s)^k - N) \right) \\ = & e \left(-\frac{a_1}{q_1} N \right) e \left(-\frac{a_2}{q_2} N \right) \prod_{i=1}^s \left(\sum_{x=1}^{q_1 q_2} e \left(\left(\frac{a_1}{q_1} + \frac{a_2}{q_2} \right) (d_i t_i x)^k \right) \right). \end{aligned}$$

By a standard trick, we replace $x \leq q_1 q_2$ by $z q_1 + y q_2$ with $1 \leq z \leq q_2$, $1 \leq y \leq q_1$. Thus it is straightforward to verify that the x -sum simplifies to

$$\begin{aligned} & \sum_{y=1}^{q_1} e \left(\frac{a_1}{q_1} (d_i t_i y)^k \right) \sum_{z=1}^{q_2} e \left(\frac{a_2}{q_2} (d_i t_i z)^k \right) \\ = & \sum_{y=1}^{q_1} e \left(\frac{a_1}{q_1} (d_i y)^k \right) \sum_{z=1}^{q_2} e \left(\frac{a_2}{q_2} (t_i z)^k \right) \end{aligned}$$

since $(t_i, q_1) = 1$, $(d_i, q_2) = 1$. Now the lemma follows easily. \square

Recall that by Lemma 5.2.6 the singular series $\mathfrak{S}_{\mathcal{W}}(N)$ is absolutely

convergent. By (5.3.1) we get

$$\mathfrak{S}_{\mathcal{W}}(N) = C \sum_{q \geq 1} D(q)$$

with

$$D(q) = \frac{1}{q^s} \prod_{v \in \mathcal{W}_q^+} \left(1 - \frac{1}{v}\right)^{-s} B(q). \quad (5.3.5)$$

On account of the second part of Lemma 5.3.1 and Lemma 5.3.4, the function $D(q)$ is multiplicative and we can apply the well known product formula due to Euler to obtain

$$\mathfrak{S}_{\mathcal{W}}(N) = C \prod_{p \text{ prime}} \left(\sum_{n \geq 0} D(p^n) \right). \quad (5.3.6)$$

We have to distinguish two cases in order to determine the value of the factor $\sum_{n \geq 0} D(p^n)$. If $p \nmid v$ for all $v \in \mathcal{W}$, then $\mathcal{P}_{p^n}^+ = \emptyset$ and $\Pi(\mathcal{P}_{p^n}^+) = \{1\}$. Consequently

$$D(p^n) = \sum_{\substack{a=1 \\ (a,p)=1}}^{p^n} \left(\frac{S(a, p^n)}{p^n} \right)^s e \left(-\frac{a}{p^n} N \right),$$

and $\sum_{n \geq 0} D(p^n)$ equals the factor usually denoted by $\chi(p)$ associated with the singular series $\mathfrak{S} = \prod_p \chi(p)$ of the classical Waring's Problem (for a definition of $\chi(p)$, see e.g. [21, p. 26]). Thus we rewrite the formula (5.3.6) as

$$\mathfrak{S}_{\mathcal{W}}(N) = C \prod_{\substack{p \text{ prime} \\ p \nmid v \forall v \in \mathcal{W}}} \chi(p) \prod_{\substack{p \text{ prime} \\ \exists v \in \mathcal{W} : p \mid v}} \sum_{n \geq 0} D(p^n).$$

It is well known that $0 < \prod_p \chi(p) \ll 1$ (see e.g. [21, Lemma 5.2 and Lemma 5.6]) and it is easy to see that

$$0 < \prod_{\substack{p \text{ prime} \\ \forall v \in \mathcal{V} : p \nmid v}} \chi(p) \ll 1.$$

We define

$$\kappa(p) := \sum_{n \geq 0} D(p^n).$$

For an integer p , we use the abbreviation $p \sim \mathcal{W}$ if p divides some $v \in \mathcal{W}$. We have proved the following lemma.

Lemma 5.3.5. *If*

$$\prod_{p \sim \mathcal{W}} \kappa(p) > 0,$$

then

$$\mathfrak{S}_{\mathcal{W}}(N) > 0.$$

Let $p \sim \mathcal{W}$ and let $v_p \in \mathcal{W}$ denote the unique prime power in \mathcal{W} such that $p|v_p$. Recall (5.3.5). Notice that for $n \geq 1$, we have

$$\prod_{v \in \mathcal{W}_{p^n}^+} \left(1 - \frac{1}{v}\right)^{-s} = \left(1 - \frac{1}{v_p}\right)^{-s}.$$

Hence

$$\begin{aligned} \kappa(p) &= 1 + \sum_{n \geq 1} D(p^n) \\ &= 1 + \left(1 - \frac{1}{v_p}\right)^s \sum_{n \geq 1} p^{-sn} B(p^n). \end{aligned}$$

Let $n \geq 1$. By the definition of $B(p^n)$ and (5.2.16) we have

$$p^{-sn} B(p^n) \ll p^{-n(s/k-1-\varepsilon)}.$$

Hence

$$\kappa(p) = 1 + O\left(p^{-s/k+1+\varepsilon}\right),$$

and consequently (see e.g. [21, Corollary to Lemma 5.2]) there is a p_0

depending only on s, k such that

$$\frac{1}{2} \leq \prod_{p > p_0} \kappa(p) \leq \frac{3}{2}.$$

Therefore, Lemma 5.3.5 yields the following lemma.

Lemma 5.3.6. *There is some $p_0 \in \mathbb{N}$, depending only on s, k , such that if*

$$\kappa(p) > 0$$

for all $p \sim \mathcal{W}$ with $p \leq p_0$, then

$$\mathfrak{S}_{\mathcal{W}}(N) > 0.$$

5.3.2 Properties of $\kappa(p)$

For the remainder of the paper, we assume $p \sim \mathcal{W}$. We have $D(1) = 1$ and

$$D(p^n) = \sum_{\substack{a=1 \\ (a,p=1)}}^{p^n} \Upsilon^s(a, p^n) e\left(-\frac{a}{p^n} N\right)$$

for $n \geq 1$, where

$$\Upsilon(a, p^n) := p^{-n} \left(1 - \frac{1}{v_p}\right)^{-1} \sum_{d \in \{1, v_p\}} \frac{\mu_{\mathcal{W}}(d)}{d} \sum_{x=1}^{p^n} e\left(\frac{ad^k x^k}{p^n}\right).$$

Lemma 5.3.7. *Let $p \sim \mathcal{W}$. Suppose $v_p = p^r$. One has*

$$\kappa(p) = \left(1 - \frac{1}{v_p}\right)^{-s} \lim_{\ell \rightarrow \infty} \frac{M(p^\ell)}{p^{\ell(s-1)}},$$

where $\ell = 2r(k-1) - 1$ and $M(p^\ell)$ is defined as the number of solutions of

$$x_1^k + \dots + x_s^k \equiv N \pmod{p^\ell} \tag{5.3.7}$$

with $v_p \nmid x_j$ and $0 < x_j < p^\ell$.

Proof. We follow the proof of [3, Lemma 10]. Let $\ell \geq r$. For $\mathbf{d} \in \mathbb{N}^s$ let $M(\mathbf{d}, p^\ell)$ denote the number of solutions modulo p^ℓ of (5.3.7) with $d_j | x_j$. Recall that $\mu_{\mathcal{W}}(1) = 1$ and $\mu_{\mathcal{W}}(v) = -1$ for all $v \in \mathcal{W}$. Thus

$$M(p^\ell) = \sum_{d_j \in \{1, v_p\}} \mu_{\mathcal{W}}(\mathbf{d}) M(\mathbf{d}, p^\ell) \quad (5.3.8)$$

by the inclusion-exclusion principle. For $d_j \in \{1, v_p\}$, let

$$L(\mathbf{d}, p^\ell) := \sum_{y=1}^{p^\ell} \sum_{x_j=1}^{p^\ell} e\left(\frac{y}{p^\ell} \varphi_{\mathbf{d}}(\mathbf{x})\right).$$

On the one hand,

$$\begin{aligned} L(\mathbf{d}, p^\ell) &= d_1 \cdots d_s \sum_{y=1}^{p^\ell} \sum_{z_j=1}^{p^\ell/d_j} e\left(\frac{y}{p^\ell} ((d_1 z_1)^k + \cdots + (d_s z_s)^k - N)\right) \\ &= d_1 \cdots d_s p^\ell M(\mathbf{d}, p^\ell); \end{aligned} \quad (5.3.9)$$

on the other hand,

$$\begin{aligned} L(\mathbf{d}, p^\ell) &= \sum_{n=0}^{\ell} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^n} \sum_{x_j=1}^{p^\ell} e\left(\frac{ap^{\ell-n}}{p^\ell} \varphi_{\mathbf{d}}(\mathbf{x})\right) \\ &= \sum_{n=0}^{\ell} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^n} (p^{\ell-n})^s \sum_{x_j=1}^{p^n} e\left(\frac{a}{p^n} \varphi_{\mathbf{d}}(\mathbf{x})\right). \end{aligned} \quad (5.3.10)$$

Combining (5.3.9), (5.3.10) and (5.3.8), we deduce

$$\begin{aligned} &M(p^\ell) \\ &= p^{\ell(s-1)} \sum_{n=0}^{\ell} p^{-ns} \sum_{d_j \in \{1, v_p\}} \frac{\mu_{\mathcal{W}}(\mathbf{d})}{d_1 \cdots d_s} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^n} \sum_{x_j=1}^{p^n} e\left(\frac{a}{p^n} \varphi_{\mathbf{d}}(\mathbf{x})\right). \end{aligned} \quad (5.3.11)$$

Recall that $\Pi(\mathcal{P}_{p^n}^+) = \{1, v_p\}$. If $n \geq 1$, we have

$$\begin{aligned} & p^{-ns} \sum_{d_j \in \{1, v_p\}} \frac{\mu_{\mathcal{W}}(\mathbf{d})}{d_1 \cdots d_s} \sum_{\substack{a=1 \\ (a,p)=1}}^{p^n} \sum_{x_j=1}^{p^n} e\left(\frac{a}{p^n} \varphi_{\mathbf{d}}(\mathbf{x})\right) \\ &= \left(1 - \frac{1}{v_p}\right)^s \Upsilon^s(a, p^n) e\left(-\frac{a}{p^n} N\right). \end{aligned} \quad (5.3.12)$$

The summand corresponding to $n = 0$ in the n -sum of (5.3.11) equals

$$\sum_{d_j \in \{1, v_p\}} \frac{\mu_{\mathcal{W}}(\mathbf{d})}{d_1 \cdots d_s} = \sum_{y=1}^s (-p^{-1})^y \binom{s}{y} = \left(1 - \frac{1}{v_p}\right)^s.$$

By this, together with (5.3.12) and (5.3.11), we get

$$\begin{aligned} M(p^\ell) &= p^{\ell(s-1)} \left(1 - \frac{1}{v_p}\right)^s \left(1 + \sum_{n=1}^{\ell} \Upsilon^s(a, p^n) e\left(-\frac{a}{p^n} N\right)\right) \\ &= p^{\ell(s-1)} \left(1 - \frac{1}{v_p}\right)^s \sum_{n=0}^{\ell} D(p^n) \end{aligned}$$

and the lemma follows. \square

5.3.3 Proof of Theorem 4.2.2

Lemma 5.3.8. *Let $p \sim \mathcal{W}$ with $p^2 = v_p$.*

- If $p \nmid k$, one has $\kappa(p) > 0$.
- If $p \mid k$, define τ by $p^\tau \parallel k$ and let $\sigma = \tau + 1$ if $p \neq 2$ and $\sigma = \tau + 2$ if $p = 2$. Then $\kappa(p) > 0$ whenever

$$x_1^k + \dots + x_s^k \equiv N \pmod{p^\sigma}$$

has a solution with $p \nmid x_1$ and $p^2 \nmid x_i$ for $i = 2, \dots, s$.

Proof. By Lemma 5.3.7, it is sufficient to show that $M(p^\ell) > C_p p^{\ell(s-1)}$ for $\ell > 2 + \sigma$, where $C_p > 0$ is some constant depending only on p .

Let $p \nmid k$. It is known (see e.g. [68, Lemma 2.15]) that for every integer N there are integers $1 \leq x_j \leq p$ with $p \nmid x_1$ such that

$$x_1^k + \dots + x_s^k \equiv N \pmod{p}.$$

Clearly, $p^2 \nmid x_i$ for $i = 2, \dots, s$. By [21, Lemma 5.4] there is an integer x such that

$$x^k + x_2^k + \dots + x_s^k \equiv N \pmod{p^2},$$

where $x \equiv x_1 \pmod{p}$ and hence $p \nmid x$. As in [3, page 20], we can obtain by Hensel's Lemma (see e.g. [58, page 87]) the existence of $p^{(s-1)(\ell-2)}$ solutions of

$$y_1^k + \dots + y_s^k \equiv N \pmod{p^\ell} \quad (5.3.13)$$

with $p \nmid y_1$, $p^2 \nmid y_i$ for $i = 2, \dots, s$ and the lemma follows in the case $p \nmid k$.

If $p|k$, we assume a solution of $x_1^k + \dots + x_s^k \equiv N \pmod{p^\sigma}$ with $p \nmid x_1$ and $p^2 \nmid x_i$ for $i = 2, \dots, s$. We can lift this solution as in [21, Lemma 5.5] and obtain $p^{(s-1)(\ell-\sigma)}$ solutions of (5.3.13). \square

The following lemma is useful to prove an analog to Lemma 5.3.8 when $p \in \mathcal{W}$, i.e. $v_p = p$.

Lemma 5.3.9. *Let $p, n \in \mathbb{N}$ with p prime and $p \nmid n$. Then*

$$x^k + y^k \equiv n \pmod{p} \quad (5.3.14)$$

has a solution with $p \nmid xy$ whenever $p > (k-1)^4 + 8k$.

Proof. Denote by ω the number of solutions modulo p of (5.3.14) having $p \nmid xy$, and let Ω stand for the number of solutions modulo p of (5.3.14) with x, y arbitrary.

By [54, Theorem 6.37], one has

$$\Omega \geq p - (k-1)^2 \sqrt{p}.$$

Since the number of $(x, y) \in \{0, \dots, p-1\}^2$ such that $x^k + y^k \equiv N \pmod{p}$ and $p|xy$ is at most $2k$, we have

$$\omega \geq p - (k-1)^2 \sqrt{p} - 2k.$$

By a short computation we get that $\omega > 0$ if $p > (k-1)^4 + 8k$. \square

Lemma 5.3.10. *Let $p \in \mathcal{W}$.*

- *If $p > (k-1)^4 + 8k$, then $\kappa(p) > 0$.*
- *If $p \leq (k-1)^4 + 8k$, then $\kappa(p) > 0$ whenever*

$$x_1^k + \dots + x_s^k \equiv N \pmod{p^\sigma}$$

has a solution with $p \nmid x_1 \cdots x_s$, where σ is as in Lemma 5.3.8.

Proof. Notice that $p > (k-1)^4 + 8k$ implies $p \nmid k$. First we show that

$$x_1^k + \dots + x_s^k \equiv N \pmod{p} \quad (5.3.15)$$

has a solution with $p \nmid x_1 \cdots x_s$ for all p with $p \nmid k$ and $p > (k-1)^4 + 8k$. For all $i \geq 4$ we take $x_i = 1$ and have to find a solution of

$$x_1^k + x_2^k \equiv N - (s-3) - x_3^k \pmod{p},$$

such that $p \nmid x_1 x_2 x_3$. By Lemma 5.3.9, such a solution is guaranteed if there is some x_3 not divisible by p such that

$$N - (s-3) - x_3^k \not\equiv 0 \pmod{p}. \quad (5.3.16)$$

It is known that the number of k -th power residues modulo p is

$$\frac{p-1}{(k, p-1)} \geq \frac{(k-1)^4 + 8k}{k} \geq 3.$$

Thus there are integers $a \not\equiv b \pmod{p}$, both not divisible by p such that $a \equiv x^k \pmod{p}$ and $b \equiv x^k \pmod{p}$ have a solution. Thus (5.3.16) has a solution with $p \nmid x_3^k$.

It remains to show that a solution of

$$x_1^k + \dots + x_s^k \equiv N \pmod{p^\sigma}$$

with $p \nmid x_1 \cdots x_s$ implies the existence of $p^{(s-1)(\ell-\sigma)}$ solutions of

$$y_1^k + \dots + y_s^k \equiv N \pmod{p^\ell}$$

with $p \nmid y_1 \cdots y_s$ for all $\ell > \sigma$. Similarly to the proof of Lemma 5.3.8, this is a consequence of [21, Lemmas 5.4 and 5.5]. \square

Now from Lemmas 5.3.6, 5.3.8 and 5.3.10, we deduce that $\mathfrak{S}_{\mathcal{W}}(N) > 0$ if the following conditions hold:

C_1 : For all $p^2 \in \mathcal{W}$ with $p|k$ there is a solution of

$$x_1^k + \dots + x_s^k \equiv N \pmod{p^\sigma} \quad (5.3.17)$$

with $p \nmid x_1$ and $p^2 \nmid x_i$ for $i = 2, \dots, s$.

C_2 : For all $p \in \mathcal{W}$ with $p \leq (k-1)^4 + 8k$ there is a solution of (5.3.17) with $p \nmid x_1 \cdots x_s$.

Lemma 5.3.11. *If $p^2 \in \mathcal{W}$ with $p \nmid k$, then Condition C_1 holds unless $pk \neq 4$.*

Proof. Let $pk \neq 4$. It suffices to detect a solution of (5.3.17) with $p \nmid x_1$ and $p^2 \nmid x_i$ for $i = 2, \dots, s$. Notice that $0 \equiv x^k \pmod{p^\sigma}$ has a solution $x = p$ if $\sigma \leq k$. By the definition of σ , the condition $\sigma \leq k$ holds unless $k = p = 2$.

Notice that $s > p^\sigma$ unless $k \leq 4$. Thus if $k \geq 4$, we can construct a solution of (5.3.17) by taking $x_1 = 1$ and $x_i^k \in \{0, 1\}$, i.e. $x_i \in \{1, p\}$, suitable for $i = 1, \dots, s$.

It remains to investigate $p = k = 3$. A solution of (5.3.17) is found since $x^k \equiv 1, -1 \pmod{9}$ for $3 \nmid x$ and $x^k \equiv 1, -1, 0 \pmod{9}$ for $9 \nmid x$. \square

Notice that the case $k = p = 2$ was investigated by Esterman [28]. Since $x_1^2 \equiv 1 \pmod{8}$ if $2 \nmid x_1$, Condition C_1 is reduced to Condition A if $k = 2$ and $4 \in \mathcal{W}$. Now, Theorem 4.2.2 follows.

Part C:
**Waring's Problem, squarefree numbers, and digital
restrictions**

6 Results and context

6.1 Sum-of-digits function

Let $q \geq 2$ be an integer. It is well known that every positive integer n admits a unique representation

$$n = \sum_{j \geq 0} a_j q^j$$

in the q -adic numeration system, where $0 \leq a_j < q$ for all $j \in \mathbb{N}$. Let

$$s_q(n) := \sum_{j \geq 0} a_j$$

be the sum-of-digits function. Its basic property – called q -additivity – is that $s_q(nq^h + m) = s_q(n) + s_q(m)$ holds for all $n, m, h \in \mathbb{N}$ with $m < n^h$.

One of the first investigating the sum of-digits function is Bush [12]. For a fix integer base q he proved in 1940 the asymptotic formula

$$\sum_{n \leq X} s_q(n) \sim \frac{q-1}{2 \log q} X \log X. \quad (6.1.1)$$

For a fix integer a and a real number x such that $|x| < 1$, Bellman and Shapiro [6] made use of identities of the form

$$\prod_{k \geq 0} (1 + ax^{2^k}) = \sum_{n \geq 0} a^{s_2(n)} x^n$$

in order to deduce asymptotic formulas (6.1.1) with explicit error terms. Refinements on the error term are due to Mirsky [57] and Drazin and Griffith [23]. Generalizing a first result of Trollope [66], Hubert Delange [22] proved an explicit error term for the asymptotic formula (6.1.1) in 1975. He showed that

$$\frac{1}{X} \sum_{n \leq X} s_q(n) = \frac{q-1}{2 \log q} \log X + F\left(\frac{\log X}{\log q}\right),$$

where F is some periodic continuous function with period 1 and is defined

in [22, p. 32]. The more general case of digit representation with respect to linear recurrences has been studied by Pethö and Tichy [59].

Let h, m, q with $m > 1, q \geq 2$ be integers such that $(m, q - 1) = 1$. In 1967, Gelfond [32, Théorème 2] showed that for an integer n the condition that n is squarefree, i.e.

$$\mu^2(n) = 1, \quad (6.1.2)$$

and the condition

$$s_q(n) \equiv h \pmod{m} \quad (6.1.3)$$

are in a certain sense independent, i.e. the density of integers n such that (6.1.2) and (6.1.3) holds is

$$\frac{1}{m} \frac{6}{\pi^2},$$

as one expects, since we recall that the density of squarefree numbers is $6/\pi^2$. We want to mention that the condition $(m, q - 1) = 1$ is necessary since $s_q(n) \equiv n \pmod{q - 1}$. Under this condition, it is very easy to see that the density of integers fulfilling (6.1.3) is $1/m$.

Gelfond also conjectured that for given coprime bases q_1, q_2 and integers m_1, m_2, ℓ_1, ℓ_2 such that $(m_1, q_1 - 1) = 1$ and $(m_2, q_2 - 1) = 1$, one has

$$\begin{aligned} & \frac{1}{N} \#\{n \leq N \mid s_{q_1}(n) \equiv \ell_1 \pmod{m_1} \text{ and } s_{q_2}(n) \equiv \ell_2 \pmod{m_2}\} \\ & \sim \frac{1}{m_1 m_2} \end{aligned}$$

as N tends to infinity. In 1972, Bésineau [7] proved this conjecture. An explicit error term and a generalization of the result was given by Kim [52]. For a short survey of this results we refer also to a paper of Thuswaldner and Tichy [64].

An other very prominent example of such hybrid results related to the sum-of-digits function in the question, if there are infinitely many primes p such that (6.1.3) holds with p in place of n . The first results in this direction did show that there are infinitely almost prime numbers fulfilling this condition. More precisely, for an integers $r \geq 1$ the set \mathbb{P}_r is defined as the set of all integers having at most r prime factors. We

mention (see e.g. [62]) the result

$$\#\{n \leq X \mid n = p_1 \cdots p_r \text{ for some primes } p_1, \dots, p_r\} \sim \frac{X(\log \log X)^{r-1}}{(r-1)! \log X}.$$

Fouvry and Mauduit [30], [31] proved that for all integers q, m, a with $m, q \geq 2$ and $(m, (q-1)) = 1$, one has

$$\#\{n \leq X \mid s_q(n) \equiv a \pmod{m} \text{ and } n \in \mathbb{P}_2\} > c \frac{X}{\log X}$$

for some constant c depending on q and m . We also want to mention the works of Dartyge, Mauduit and Tenenbaum [15], [16], [17] where the distribution of almost primes with such digital restrictions has been investigated. Only recently, Mauduit and Rivat [56] proved that there are infinitely many primes p such that (6.1.3) holds with p in place of n . Even more, they showed that for given integers q, m, a with $m, q \geq 2$ and $(m, (q-1)) = 1$ one has

$$\#\{p \leq X \mid s_q(p) \equiv a \pmod{m}\} \sim \frac{1}{m} \frac{x}{\log X}.$$

Indeed, an explicit error term is given in their paper.

We want to remain to Section 3 and recall that such results show that certain properties among the integers are independent. We also want to mention that – besides the presented results concerning the sum-of-digits function – there are further interesting questions concerning digital restriction. For instance, one can suppose that the q -ary representation of a given integer n contains only digits of a set $D \subsetneq \{0, 1, \dots, q-1\}$. Among others, Hybrid results in this direction have been obtained by Erdős et al. [26], [27]; and Dartyge and Mauduit [15]. However, we have not been able yet to prove results concerning Waring's Problem with variables with missing digits. In particular, this might be due to the fact that the sets of integers that do not contain a given digit $d \in \{0, 1, \dots, q-1\}$ in its q -ary representation are not dense.

6.2 Waring's Problem

The purpose of this chapter is to study the independence of the conditions (6.1.2) and (6.1.3) among the set of solutions $(x_1, \dots, x_s) \in \mathbb{N}^s$ of

$$N = x_1^k + \dots + x_s^k, \quad (6.2.1)$$

where $s, k \in \mathbb{N}$ and N is a given integer.

On the one hand, we want to recall Corollary 4.2.3 that we stated at page 29 and proved in the previous chapter of this work. We also want to reformulate the relevant condition. As always, let s and k be integers.

A: Let (N, s) be said to satisfy Condition A if

$$x_1^2 + \dots + x_s^2 \equiv N \pmod{32}$$

has a solution with $4 \nmid x_j$ for $j = 1, \dots, s$.

Condition A holds for all N if $s \geq 8$. Hence Corollary 4.2.3 can be read as the following: Denote by $R_{k,s,\mu^2}(N)$ the number of solutions of (6.2.1) where the variables x_j ($j = 1, \dots, s$) are assumed to be squarefree. For $s > 2^k$, there is some $\rho > 0$ such that

$$R_{k,s,\mu^2}(N) = \mathfrak{S}_{k,s,\mu^2}(N)N^{s/k-1} + O(N^{s/k-1-\rho}) \quad (6.2.2)$$

holds. One has $\mathfrak{S}_{k,s,\mu^2}(N) > 0$ if $k \geq 3$ or Condition A holds.

On the other hand, Thuswaldner and Tichy [65] investigated Waring's Problem where the digit sums of the variables x_j ($j = 1, \dots, s$) are assumed to be in a certain residue class. Denote by $R_{k,s,\mathbf{h},\mathbf{m}}(N)$ the number of solutions of (6.2.1) where for all $j = 1, \dots, s$, the variables x_j are assumed to fulfill

$$s_{q_j}(x_j) \equiv h_j \pmod{m_j}$$

for given integers h_j, m_j, q_j with $m_j, q_j \geq 2$ and $(q_j - 1, m_j) = 1$.

For $s > 2^k$, Thuswaldner and Tichy proved that

$$R_{k,s,\mathbf{h},\mathbf{m}}(N) \sim \frac{1}{m_1 \cdots m_s} r_{k,s}(N) \quad (6.2.3)$$

holds. Indeed, an explicit error term is given in their paper. The proof of this result as well as our main result of this chapter makes use of ideas of auto-correlation results of the sum-of-digits function. Related results can be found in the works of Bésineau [7] and Kim [52]. Recall that in the language of Section 3, Thuswaldner's and Tichy's result shows that the condition that an s -tuple of integers is a solution of (6.2.1) is asymptotically in a first-order approximation independent from the condition that its elements fulfill (6.1.3).

As already mentioned, we want to show that one can combine the results presented above. We prove that among the solutions of (6.2.1), the conditions (6.1.2) and (6.1.3) are independent. We thus show that for sufficient large N the equation (6.2.1) has a solution where the variables meet conditions (6.1.2) and (6.1.3).

Theorem 6.2.1. *Let $s, k \in \mathbb{N}$ with $s > 2^k$, $h_j, m_j, q_j \in \mathbb{N}$ satisfying $(q_j - 1, m_j) = 1$, $q_j > k$ for all $j = 1, \dots, s$. Furthermore, for all $j = 1, \dots, s$, the integer q_j has the following property: for all integers $0 < b_j < q_j$, there are integers $0 < \ell_j, z_j < q_j$ such that*

$$b_j \ell_j \equiv z_j \pmod{q_j} \quad \text{with} \quad 0 < z_j \leq q_j - k. \quad (6.2.4)$$

Let $R_{k,s,\mathbf{h},\mathbf{m},\mu^2}(N)$ be the number of solutions of (6.2.1) with x_j squarefree and

$$s_{q_j}(x_j) \equiv h_j \pmod{m_j}$$

for all $j = 1, \dots, s$. Then the asymptotic formula

$$R_{k,s,\mathbf{h},\mathbf{m},\mu^2}(N) = \frac{1}{m_1 \cdots m_s} \mathfrak{S}_{k,s,\mu^2}(N) N^{s/k-1} + O\left(\frac{N^{s/k-1}}{(\log \log N)^A}\right) \quad (6.2.5)$$

holds for all non negative $A \in \mathbb{R}$.

Recall that $\mathfrak{S}_{k,s,\mu^2}(N) \gg 1$ if $k \geq 3$ or Condition A holds. Note that condition (6.2.4) is fulfilled for q_j prime with $q_j - k \geq 1$.

Our method of proof does not permit the derivation of a better error

term (see Remark 7.1.4 at the end of Section 7.1). Although the condition $s > 2^k$ can be weakened as in the classical Waring's Problem if one only assumes that the variables meet (6.1.3), the assumption $s > 2^k$ is essential in the proof of Theorem 6.2.1 (see Remark 7.1.2 after Lemma 7.1.1).

At the very beginning (see formula (7.1.4)) of the proof of Theorem 6.2.1, we make use of the convolution formula $\mu^2(x) = \sum_{d^2|x} \mu(d)$. The only difficulty caused by the condition that the variables in (6.2.1) are assumed to be squarefree is that $s_q(x) \equiv h \pmod{m}$ must be changed into $s_q(xd^2) \equiv h \pmod{m}$. Hence, one can adopt literally the proof of Theorem 6.2.1 if the condition (6.1.2) is generalized as follows:

Let \mathcal{V} be a set of pairwise coprime integers not containing 1 and assume that there is some $\delta > 0$ such that

$$\sum_{v \in \mathcal{V}} \frac{1}{v^{1-\delta}}$$

converges. Theorem 6.2.1 remains valid if one replaces the condition $\mu^2(x_j) = 1$ by $\chi_{\mathcal{V}}(x_j) = 1$ on the variables x_j in (6.2.1) for all $j = 1, \dots, s$. We refer the reader to the previous chapter for a definition of $\chi_{\mathcal{V}}$. Notice that if \mathcal{V} is the set of the squares of all primes, we have $\chi_{\mathcal{V}} = \mu^2$. One also finds in the previous chapter an asymptotic formula for the number of solutions of (6.2.1) where the variables x_j meet $\chi_{\mathcal{V}}(x_j) = 1$ for $j = 1, \dots, s$.

7 Proofs

The proof of Theorem 6.2.1 is organized as following. In Subsections 7.1 and 7.2 we show that Theorem 6.2.1 can be deduced from Proposition 7.2.1 that is stated in Subsection 7.3. The remainder of this chapter is devoted to the proof of Proposition 7.2.1. At the end of Subsection 7.3 we say a few words about the method we utilize in order to prove Proposition 7.2.1.

7.1 Preliminaries - the circle method

We fix $A \in \mathbb{R}$ arbitrarily large. Thus

$$R_{k,s,\mathbf{h},\mathbf{m},\mu^2}(N) = \int_0^1 \left(\prod_{i=1}^s u_i(P, \theta) \right) e(-N\theta) d\theta, \quad (7.1.1)$$

where we define

$$u_i(P, \theta) := \sum_{\substack{n_i < P \\ s_{q_i}(n_i) \equiv h_i \pmod{m_i}}} \mu^2(n_i) e(n_i^k \theta)$$

and $P := \lfloor N^{1/k} \rfloor$. In order to remove the congruence condition $s_{q_i}(n_i) \equiv h_i \pmod{m_i}$ in $u_i(P, \theta)$, we write

$$u_i(P, \theta) = \frac{1}{m_i} \sum_{l=0}^{m_i-1} \sum_{n < P} \mu^2(n) e\left(l \frac{s_{q_i}(n) - h_i}{m_i}\right) e(\theta n_i^k)$$

by following Gelfond [32]. We insert this into (7.1.1) and split the obtained expression into a part where all $l_i = 0$ ($i = 1, \dots, s$) and a remain-

ing part. This yields

$$\begin{aligned}
& R_{k,s,\mathbf{h},\mathbf{m},\mu^2}(N) \\
&= \frac{1}{m_1 \cdots m_s} \int_0^1 \sum_{n_1 < P} \mu^2(n_1) \cdots \sum_{n_s < P} \mu^2(n_s) e(\theta(n_1^k + \cdots + n_s^k - N)) d\theta \\
&+ \frac{1}{m_1 \cdots m_s} \underbrace{\sum_{l_1=0}^{m_1-1} \cdots \sum_{l_s=0}^{m_s-1}}_{l_1 + \cdots + l_s \neq 0} \int_0^1 \left(\prod_{i=1}^s S_{i,l_i}(P, \theta) \right) e(-N\theta) d\theta
\end{aligned} \tag{7.1.2}$$

with

$$S_{i,l_i}(P, \theta) := \sum_{n_i < P} e\left(\theta n_i^k + l_i \frac{S_{q_i}(n_i) - h_i}{m_i}\right) \mu^2(n_i).$$

Note, that the first integral in (7.1.2) equals $R_{k,s,\mu^2}(N)$ and we can utilize (6.2.2).

Let $\mathbf{l} := (l_1, \dots, l_s)$ with $0 \leq l_i \leq m_i - 1$ ($i = 1, \dots, s$) and $l_1 + \cdots + l_s \neq 0$, and we define

$$L_{\mathbf{l}} := \int_0^1 \left(\prod_{i=1}^s S_{i,l_i}(P, \theta) \right) e(-N\theta) d\theta.$$

Theorem 6.2.1 follows if we prove that $L_{\mathbf{l}} = O(N^{s/k-1}/(\log \log N)^A)$. Let l_j be an entry of \mathbf{l} that is not equal to 0. Then

$$|L_{\mathbf{l}}| \leq \sup_{\theta \in [0,1]} \left\{ |S_{j,l_j}(P, \theta)| \right\} \max_{i \in \{1, \dots, s\}} \left\{ \int_0^1 |S_{i,l_i}(P, \theta)|^{s-1} d\theta \right\}. \tag{7.1.3}$$

Since $s > 2^k$, we have

$$\begin{aligned}
& \int_0^1 |S_{i,l_i}(P, \theta)|^{s-1} d\theta \\
& \leq P^{s-1-2^k} \int_0^1 S_{i,l_i}(P, \theta)^{2^{(k-1)}} \overline{S_{i,l_i}(P, \theta)^{2^{(k-1)}}} d\theta \\
& \leq P^{s-1-2^k} \\
& \quad \# \{n_1, \dots, n_s < P : n_1^k + \cdots + n_{2^{k-1}}^k = n_{2^{k-1}-1}^k + \cdots + n_{2^k}^k\} \\
& \ll P^{s-k-1},
\end{aligned}$$

where we utilized Vaughan [70, Theorem 2], a strong version of Hua's Lemma. We deduce from (7.1.3) that

$$L_1 = O\left(\sup_{\theta \in [0,1)} \left\{ \left| S_{j,l_j}(P, \theta)^{s-2^k} \right| \right\} P^{s-k-1}\right).$$

Hence, the following lemma yields Theorem 6.2.1.

Lemma 7.1.1. *Let l, m, k, q be positive integers with $m \geq 2, q \geq 2$ and $m \nmid l(q-1)$. Then*

$$\Omega(N) := \sum_{n < N} e\left(\theta n^k + \frac{l}{m} s_q(n)\right) \mu^2(n) \ll \frac{N}{(\log \log N)^A}$$

holds uniformly in $\theta \in [0, 1)$.

Remark 7.1.2. Above, we made use of Vaughan [70, Theorem 2] where the condition $s > 2^k$ is necessary. If $s > 2^k$ does not hold, relevant version's of Hua's Lemma imply an additional factor P^ε for an upper bound which is too big since we can not improve the bound $\Omega(N) \ll N/(\log \log N)^A$ in Lemma 7.1.1.

Applying the convolution formula $\mu^2(n) = \sum_{z^2|n} \mu(z)$, we have

$$\Omega(N) = \sum_{z \geq 1} \mu(z) \sum_{n < N/z^2} e\left(z^{2k} \theta n^k + \frac{l}{m} s_q(nz^2)\right). \quad (7.1.4)$$

We split up the sum into a part with $z \geq (\log \log N)^{2A}$ and a part with $z < (\log \log N)^{2A}$. Therefore

$$\begin{aligned} & \Omega(N) \\ & \ll \sum_{z \geq (\log \log N)^{2A}} \frac{N}{z^2} \\ & \quad + \sum_{z < (\log \log N)^{2A}} |\mu(z)| \left| \sum_{n < N/z^2} e\left(z^{2k} \theta n^k + \frac{l}{m} s_q(nz^2)\right) \right| \end{aligned}$$

and thus

$$\begin{aligned} & \Omega(N) \\ \ll & \frac{N}{(\log \log N)^A} \\ & + (\log \log N)^{2A} \max_{\substack{z < (\log \log N)^{2A} \\ \mu^2(z)=1}} \left\{ \left| \sum_{n < N/z^2} e \left(z^{2k} \theta n^k + \frac{l}{m} s_q(nz^2) \right) \right| \right\}, \end{aligned}$$

by using the trivial bound N/z^2 for the inner sum of (7.1.4) in the case of $z \geq (\log \log N)^{2A}$.

Theorem 7.1.3. *Let $B, D > 0$ and let $q, d \in \mathbb{N}$ satisfying $q \nmid d \vee (q^2 \mid d \wedge q^3 \nmid d)$. Then one has*

$$\sum_{n < N/d} e \left(\theta n^k + \frac{l}{m} s_q(nd) \right) \ll \frac{N}{(\log N)^B}$$

uniformly for $\theta \in \mathbb{R}$ and $d \leq (\log \log N)^D$.

Theorem 6.2.1 is proved by applying Theorem 7.1.3 with $d = z^2$ and $D = 4A$. Notice, that the condition $\mu^2(z) = 1$ implies $q \nmid d \vee (q^2 \mid d \wedge q^3 \nmid d)$ and $N(\log \log N)^2 / (\log N)^B \ll N / (\log \log N)^A$. The proof of Theorem 7.1.3 is the objective of the remaining paper.

Remark 7.1.4. The bound of Theorem 7.1.3 is stronger than necessary. However, we can not achieve a better error term in Theorem 6.2.1 since the condition $d \leq (\log \log N)^D$ in Theorem 7.1.3 is necessary and forces us to bound the summands in (7.1.4) with $z \geq (\log \log N)^{2A}$ trivially by N/z^2 . Therefore, we are not able to improve the error term

$$O \left(N^{s/k-1} / (\log \log)^A \right)$$

in (6.2.5).

7.2 Weyl's inequality

Let $k \in \mathbb{N}$, $\rho : \mathbb{N} \rightarrow \mathbb{C}$ and $n, h_1, h_2, \dots \in \mathbb{N}$. We define the higher difference operators Δ_k recursively by

$$\Delta_1(\rho(n); h_1) := \rho(n + h_1) - \rho(n)$$

and

$$\Delta_{j+1} := \Delta_1(\Delta_j(\rho(n); h_1, \dots, h_j); h_{j+1})$$

for $j \in \mathbb{N}$. Notice, that $\Delta_k(n^k; h_1, \dots, h_k)$ is independent on n .

We define $I \subseteq \mathbb{N}$ to be an interval of integers if $I := \{n \in \mathbb{N} : a \leq n < b\}$ for certain $a, b \in \mathbb{N}$. The aim of this section is to show that the following proposition implies Theorem 7.1.3.

Proposition 7.2.1. *Let $B, D > 0$ and let d, k, m, h, q, N be positive integers such that $m \geq 2$, $q \geq 2$ and $m \nmid h(q-1)$. Let further U_1, \dots, U_k, J be intervals of integers with $\sqrt{N}/d < |U_i|$ for all $i = 1, \dots, k$. Assume $|J| \leq N$. We further define*

$$\begin{aligned} & Y(U_1, \dots, U_k, J) \\ & := \sum_{h_1 \in U_1} \cdots \sum_{h_k \in U_k} \left| \sum_{n \in J} e\left(\frac{h}{m} \Delta_k(s_q(dn); h_1, \dots, h_k)\right) \right|^2. \end{aligned} \quad (7.2.1)$$

Then

$$Y(U_1, \dots, U_k, J) \ll |U_1| \cdots |U_k| |J|^2 \frac{1}{(\log N)^B}$$

holds uniformly for all $d \leq (\log \log N)^D$ satisfying $q \nmid d \vee (q^2 |d \wedge q^3 \nmid d)$.

We can argue literally as in Section 8 of [65] to prove that Theorem 7.1.3 can be deduced from Proposition 7.2.1. Therefore, we only give short sketch of this statement.

Proof of (Proposition 7.2.1 \Rightarrow Theorem 7.1.3). For abbreviation, we define $M := \lfloor N/d \rfloor$. Using the classical version of Weyl's Lemma (see e.g.

[68, Lemma 2.3]), we get

$$\begin{aligned} & \left| \sum_{n < M} e \left(\theta n^k + \frac{l}{m} s_q(dn) \right) \right|^{2^k} \\ \leq & (2M)^{2^k - k - 1} \sum_{|h_1|, \dots, |h_k| < M} \left| \sum_{n \in H_k(h_1, \dots, h_k)} e \left(\frac{l}{m} \Delta_k(s_q(dn); h_1, \dots, h_k) \right) \right|, \end{aligned}$$

where $H_k(h_1, \dots, h_k)$ is an interval of integers depending linearly on the parameters h_1, \dots, h_k . We remove this dependence by splitting up the sums into parts of reasonable size. Besides, we make use of the Cauchy-Schwarz inequality in order to get a square of the modulus of the innermost sum. Now, we can apply Proposition 7.2.1. \square

In order to prove Proposition 7.2.1, we refine a method which has been developed in the work of Thuswaldner and Tichy [65] that we mentioned in Subsection 6.2. Very roughly speaking, the main idea is to split up the intervals U_1, \dots, U_k, J in (7.2.1) such that $Y(U_1, \dots, U_k, J)$ can be bounded by a sum of elements having the same shape as $Y(U_1, \dots, U_k, J)$. This process will be applied iteratively until two summands V_1 and V_2 can be bounded non trivially. In the next Subsection, we give preliminary definitions and construct sequences \mathcal{V}_1 and \mathcal{V}_2 that will indicate the summands V_1 and V_2 . In Subsection 7.4 we perform the iterations. In Subsection 7.5 we simply make use of the inequality $(1 - \sigma)^t < e^{-t\sigma}$ that is valid for all $0 < \sigma < 1$ and $t > 0$ in order to conclude the proof of Proposition 7.2.1 that yields Theorem 6.2.1.

7.3 Auto-correlation functions

Let d always denote a positive integer with $q \nmid d \vee (q^2 | d \wedge q^3 \nmid d)$. Let

$$\begin{aligned} \mathcal{Q} & := \{0, 1, 2, \dots, q - 1\}, \\ M & := \{1, 2, \dots, k\}, \\ M' & := \{0, 1, 2, \dots, k + d\}, \end{aligned}$$

and

$$\mathcal{F} := \{f : \mathcal{P}(M) \rightarrow M'\},$$

where $\mathcal{P}(M)$ denotes the set of all subsets of M . For $\mathbf{r} = (r_1, r_2, \dots, r_k) \in \mathcal{Q}^k$, $i \in \mathcal{Q}$ and $S \subseteq M$ we define

$$\Xi_{\mathbf{r},i}(f)(S) := \left\lfloor di + \sum_{t \in S} r_t + f(S) \right\rfloor_q,$$

with $\lfloor x \rfloor_q := \lfloor x/q \rfloor$. Notice that $f \in \mathcal{F}$ implies $\Xi_{\mathbf{r},i}(f) \in \mathcal{F}$. Let $F_0, F_1 \in \mathcal{F}$ be defined by

$$F_0(S) := 0$$

for all $S \subseteq M$ and

$$F_1(M) := 1, \quad F_1(S) := 0$$

for all $S \subsetneq M$. Further, we define iterates of $\Xi_{\mathbf{r},i}$ by

$$\Xi_{\{\mathbf{r}_\ell, i_\ell\}_{1 \leq \ell \leq L}} := \Xi_{\mathbf{r}_L, i_L} \circ \dots \circ \Xi_{\mathbf{r}_1, i_1},$$

where the composition is defined by

$$(\Xi_{\mathbf{r}_2, i_2} \circ \Xi_{\mathbf{r}_1, i_1})(f)(S) := \Xi_{\mathbf{r}_2, i_2}(\Xi_{\mathbf{r}_1, i_1}(f))(S)$$

for $f \in \mathcal{F}, S \subseteq M$. For the sake of a simple notation, let $\Xi_{\{\mathbf{r}_\ell, i_\ell\}_{\ell \in \emptyset}}(f) := f$, where \emptyset denotes the empty set.

Let $L \in \mathbb{N}$, $\ell \leq L$ and $\mathbf{r}_\ell \in \mathcal{Q}^k, i_{\ell 1}, i_{\ell 2} \in \mathcal{Q}$. Let further $f_1, f_2, g_1, g_2 \in \mathcal{F}$. We define

$$(f_1, f_2) \xrightarrow{(\mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2})_{1 \leq \ell \leq L}} (g_1, g_2)$$

to be an equivalent expression for

$$\Xi_{\{\mathbf{r}_\ell, i_{\ell 1}\}_{1 \leq \ell \leq L}}(f_1) = g_1 \quad \wedge \quad \Xi_{\{\mathbf{r}_\ell, i_{\ell 2}\}_{1 \leq \ell \leq L}}(f_2) = g_2.$$

Lemma 7.3.1. *There is a sequence $(\hat{\mathbf{r}}_\ell, \hat{i}_{\ell 1}, \hat{i}_{\ell 2})_{1 \leq \ell \leq L'}$ with*

$$L' := \left\lfloor \frac{\log(d(k+d))}{\log q} \right\rfloor + 1$$

such that for any $(f_1, f_2) \in \mathcal{F}^2$ one has

$$(f_1, f_2) \xrightarrow{(\hat{\mathbf{r}}_\ell, \hat{i}_{\ell 1}, \hat{i}_{\ell 2})_{1 \leq \ell \leq L'}} (F_1, F_0).$$

We denote this sequence the (F_1, F_0) -sequence with length L' .

Proof. Given a sequence $(\mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2})_{1 \leq \ell \leq L''}$, we define for all integers $n \geq 1$ $G_n, H_n \in \mathcal{F}$ such that

$$(F_0, F_0) \xrightarrow{(\mathbf{r}_1, i_{11}, i_{12})} (G_1, H_1) \xrightarrow{(\mathbf{r}_2, i_{21}, i_{22})} (G_2, H_2) \xrightarrow{(\mathbf{r}_3, i_{31}, i_{32})} (G_3, H_3) \cdots \dots$$

holds.

We first show that there is a sequence $(\mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2})_{1 \leq \ell \leq L''}$ such that

$$(F_0, F_0) \xrightarrow{(\mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2})_{1 \leq \ell \leq L''}} (F_1, F_0) \quad (7.3.1)$$

with $L'' < \log d / \log q$. In that what follows, we define this sequence recursively.

The following frequently used trick is to define $\mathbf{r} = (r_1, \dots, r_k)$ such that $\sum_{t \in S} r_t$ only peaks the critical value $q - 1$ if $S = M$.

We choose $i_{\ell 2} := 0$ for all $1 \leq \ell \leq L''$ and $i_{\ell 1} := 0$ for all $2 \leq \ell \leq L''$. For $S \subseteq M$ we have

$$G_1(S) = \left\lfloor di_{11} + \sum_{t \in S} r_{1t} \right\rfloor_q.$$

We need to distinguish two cases. Let $d = \alpha q + \beta$ with integers α, β and $\beta \in \mathcal{Q}$.

- If $\beta \neq 0$, we make use of the condition (6.2.4). We thus can choose a non-negative integer $i_{11} \in \mathcal{Q}$ such that $i_{11}\beta \equiv z \pmod{q}$ with $0 < z \leq q - k$. Thus $i_{11}\beta = \gamma q + z$ with $\gamma \in N$ and consequently $di_{11} = q\alpha_1 + z$ with $0 \leq \alpha_1 = \alpha i_{11} + \gamma \leq d$. We take $\mathbf{r}_1 := (q - k - z + 1, 1, 1, \dots, 1)$. Hence,

$$\sum_{t \in S} r_{1t} < q - z$$

if $S \subsetneq M$ and

$$\sum_{t \in M} r_{1t} = q - z.$$

Thus, we obtain

$$G_1(S) = \alpha_1 + \left[z + \sum_{t \in S} r_{1t} \right]_q = \alpha_1 + F_1(S).$$

Since $\sum_{t \in S} r_{1t} < q$ for all $S \subseteq M$ and $i_{12} = 0$, we have

$$H_1(S) = \left[\sum_{t \in S} r_{1t} \right]_q = F_0(S).$$

If $\alpha_1 = 0$, we take $L'' := 1$ and (7.3.1) is shown if $\beta \neq 0$. If $\alpha_1 > 0$, we have to go on and get

$$G_2(S) = \left[\sum_{t \in S} r_{2t} + \alpha_1 + F_1(S) \right]_q.$$

Recall that we defined $i_{\ell 1} = i_{\ell 2} = 0$ if $\ell \geq 2$. We define the integers α_2, β_2 via $\alpha_1 = q\alpha_2 + \beta_2$ with $\beta_2 \in \mathcal{Q}$. By taking $\mathbf{r}_2 := (q - \beta_2 - 1, 0, 0, \dots, 0)$ we have

$$G_2(S) = \alpha_2 + \left[\beta_2 + \sum_{t \in S} r_{1t} + F_1(S) \right]_q = \alpha_2 + F_1(S)$$

and $H_2 = F_0$. We repeat this procedure until $\alpha_j = 0$ for the first time. We take $L'' := j$ and (7.3.1) follows in the case $\beta \neq 0$ since $j < \log d / \log q$.

- If $\beta = 0$, we take $i_{11} := 1$. We set $\mathbf{r}_1 := (q - k, 2, 1, \dots, 1)$ and get

$$G_1(S) = \alpha + \left[\sum_{t \in S} r_{1t} \right]_q = \alpha + F_1(S).$$

However, we have

$$H_1(S) = \left[\sum_{t \in S} r_{1t} \right]_q = F_1(S).$$

Since $q|d$, we have $q|\alpha$ and $q^2 \nmid \alpha$ by our assumption $q \nmid d \vee (q^2|d \wedge q^3 \nmid d)$.

d). Hence, $\alpha = q\alpha_2$ with an integer α_2 with $q \nmid \alpha_2$. Hence, $\alpha_2 \neq 0$. Take $\mathbf{r}_2 := (q - k, 1, 1, \dots, 1)$, thus

$$G_2(S) = \alpha_2 + \left\lfloor \sum_{t \in S} r_{2t} + F_1(S) \right\rfloor_q = \alpha_2 + F_1(S)$$

and

$$H_2(S) = \left\lfloor \sum_{t \in S} r_{2t} + F_1(S) \right\rfloor_q = F_1(S).$$

Since $q \nmid \alpha_2$, we have $\alpha_2 = q\alpha_3 + \beta_3$ with $0 \neq \beta_3 \in \mathcal{Q}$. We take $\mathbf{r}_3 := (q - 1 - \beta_3, 0, 0, \dots, 0)$ and obtain

$$G_3(S) = \alpha_3 + \left\lfloor \beta_3 + \sum_{t \in S} r_{3t} + F_1(S) \right\rfloor_q = \alpha_3 + F_1(S).$$

Since $\sum_{t \in S} r_{3t} < q - 1$ for all $S \subseteq M$, it follows

$$H_3(S) = \left\lfloor \sum_{t \in S} r_{3t} + F_1(S) \right\rfloor_q = F_0(S).$$

If $\alpha_3 = 0$, we get (7.3.1) by choosing $L'' := 3$. If $\alpha_3 > 0$, we can now proceed as in the case $\beta \neq 0$ and define L'' as the smallest index $j \geq 3$, where $\alpha_j = 0$. Again, $L'' < \log d / \log q$ holds and (7.3.1) is proved.

Secondly, it is easy to see that

$$(f_1, f_2) \xrightarrow{(0,0,0)_{1 \leq \ell \leq L'''}} (F_0, F_0)$$

holds for all $L''' \geq \log(k + d) / \log q$. Thus we take

$$L''' := L' - L'' \geq \frac{\log(k + d)}{\log q}$$

with $L' := \lfloor \frac{\log(d(k+d))}{\log q} \rfloor + 1$ as stated in the lemma and define the (F_1, F_0) -

sequence by

$$\begin{aligned} (\hat{\mathbf{r}}_\ell, \hat{i}_{\ell 1}, \hat{i}_{\ell 2}) &:= (\mathbf{0}_\ell, 0, 0) \quad \text{for } 1 \leq \ell \leq L''', \\ (\hat{\mathbf{r}}_{\ell+L'''}, \hat{i}_{(\ell+L''')1}, \hat{i}_{(\ell+L''')2}) &:= (\mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2}) \quad \text{for } 1 \leq \ell \leq L''. \end{aligned}$$

□

Let

$$\mathbf{r}^* := (q - k, 1, 1, 1, \dots, 1) \in \mathcal{Q}^k. \quad (7.3.2)$$

Notice that the sum of the entries of \mathbf{r}^* equals $q - 1$. Thus, the equations

$$\begin{aligned} \Xi_{(\mathbf{r}^*, 0)}(F_0) &= F_0, \\ \Xi_{(\mathbf{r}^*, 0)}(F_1) &= F_1, \\ \Xi_{(\mathbf{0}, 0)}(F_1) &= F_0, \\ \Xi_{(\mathbf{0}, 0)}(F_0) &= F_0, \end{aligned} \quad (7.3.3)$$

are easily proved. Let

$$L := L' + 2, \quad (7.3.4)$$

where L' is as in Lemma 7.3.1.

We now define two sequences

$$\mathcal{V}_1 = (\mathbf{r}_l, i_{l1}, i_{l2})_{1 \leq l \leq L}$$

and

$$\mathcal{V}_2 = (\tilde{\mathbf{r}}_l, \tilde{i}_{l1}, \tilde{i}_{l2})_{1 \leq l \leq L}$$

that play an important role in the proof of Theorem 6.2.1. For $1 \leq l \leq L'$ let

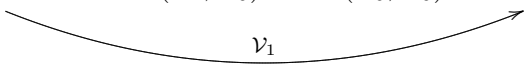
$$\begin{aligned} (\mathbf{r}_l, i_{l1}, i_{l2}) &:= (\hat{\mathbf{r}}_l, \hat{i}_{l1}, \hat{i}_{l2}) \quad \text{and} \\ (\tilde{\mathbf{r}}_l, \tilde{i}_{l1}, \tilde{i}_{l2}) &:= (\hat{\mathbf{r}}_l, \hat{i}_{l1}, \hat{i}_{l2}), \end{aligned}$$

where $(\hat{\mathbf{r}}_l, \hat{i}_{l1}, \hat{i}_{l2})$ are the entries of the (F_1, F_0) -sequence with length L'

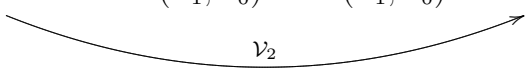
defined in Lemma 7.3.1. Let further

$$\begin{aligned} \mathbf{r}_l &:= (0, 0, \dots, 0), & \tilde{\mathbf{r}}_l &:= \mathbf{r}^* & \text{for } l = L - 1, \\ \mathbf{r}_l &= \tilde{\mathbf{r}}_l := (0, 0, \dots, 0), & & & \text{for } l = L, \\ i_{l1} = i_{l2} = \tilde{i}_{l1} = \tilde{i}_{l2} &:= 0 & \text{for } l = L - 1 \text{ or } l = L. \end{aligned} \quad (7.3.5)$$

Thus we conclude by (7.3.3) and Lemma 7.3.1 that

$$(f_1, f_2) \xrightarrow{(F_1, F_0)\text{-sequence}} (F_1, F_0) \xrightarrow{(\mathbf{0}, \mathbf{0}, \mathbf{0})} (F_0, F_0) \xrightarrow{(\mathbf{0}, \mathbf{0}, \mathbf{0})} (F_0, F_0) \quad (7.3.6)$$


and

$$(f_1, f_2) \xrightarrow{(F_1, F_0)\text{-sequence}} (F_1, F_0) \xrightarrow{(\mathbf{r}^*, \mathbf{0}, \mathbf{0})} (F_1, F_0) \xrightarrow{(\mathbf{0}, \mathbf{0}, \mathbf{0})} (F_0, F_0) \quad (7.3.7)$$


holds for all $(f_1, f_2) \in \mathcal{F}^2$.

Later, the following lemma will be of use. Its proof is straightforward.

Lemma 7.3.2. *Let G be a finite set and $A := (a_{ij})_{i,j \in G}$ be a matrix with non negative real entries. For $y \in \mathbb{N}$, let $\left(a_{ij}^{(y)} \right)_{i,j \in G} := A^y$. Let $X > 0$ with $\sum_{k \in G} a_{ik} \leq X$, for all $i \in G$. One has*

$$\sum_{k \in G} a_{ik}^{(t)} \leq X^y$$

for all $i \in G$.

7.4 Iterations

Recall that our aim is to show Proposition 7.2.1. Let $B, D > 0$ and $d \leq (\log \log N)^D$.

Let I be an interval of integers, i.e. $I := \{n \in \mathbb{N} : a \leq n < b\}$ for certain integers $a < b$. For $c \in \mathbb{N}$ we define $cI := \{n \in \mathbb{N} : cn \leq n < cb\}$.

For $f_1, f_2 \in \mathcal{F}$ and I_1, \dots, I_k, J intervals of integers let

$$\begin{aligned} & \Phi(h_1, \dots, h_k; J, f_1) \\ := & \sum_{n \in J} e \left(\frac{h}{m} \sum_{S \subseteq M} (-1)^{k-|S|} s_q \left(dn + \sum_{t \in S} h_t + f_1(s) \right) \right). \end{aligned}$$

We further define

$$\begin{aligned} & \Psi(I_1, \dots, I_{k-1}; I_k, J, f_1, f_2) \\ := & \sum_{h_k \in I_k} \Phi(h_1, \dots, h_k; J, f_1) \overline{\Phi(h_1, \dots, h_k; J, f_2)} \end{aligned}$$

and

$$\begin{aligned} & X(I_1, \dots, I_k; J, f_1, f_2) \\ := & \sum_{h_1 \in I_1} \cdots \sum_{h_{k-1} \in I_{k-1}} \Psi(h_1, \dots, h_{k-1}; I_k, J, f_1, f_2). \end{aligned}$$

Since

$$\Delta_k(s_q(dn), h_1, \dots, h_k) = \sum_{S \subseteq M} (-1)^{k-|S|} s_q \left(dn + \sum_{t \in S} dh_t \right),$$

we have

$$\begin{aligned} & Y(U_1, \dots, U_k, J) \\ = & \sum_{h_1 \in U_1} \cdots \sum_{h_k \in U_k} \left| \sum_{n \in J} e \left(\frac{h}{m} \sum_{S \subseteq M} (-1)^{k-|S|} s_q \left(dn + \sum_{t \in S} dh_t \right) \right) \right|^2 \\ \leq & \sum_{h_1 \in dU_1} \cdots \sum_{h_k \in dU_k} \left| \sum_{n \in J} e \left(\frac{h}{m} \sum_{S \subseteq M} (-1)^{k-|S|} s_q \left(dn + \sum_{t \in S} h_t \right) \right) \right|^2 \\ = & X(I_1, \dots, I_k; J, F_0, F_0), \end{aligned}$$

where $I_i := dU_i$. Thus $\sqrt{N} < |I_i|$. Note that we substitute in the inner sum dh_i by h_i since we extend the intervals U_i to $I_i = qU_i$. This is the

essential trick of this paper. Our aim is now to show

$$X(I_1, \dots, I_k; J, f_1, f_2) \ll |I_1| \cdots |I_k| |J|^2 \frac{1}{(\log N)^{2B}} \quad (7.4.1)$$

for arbitrary $f_1, f_2 \in \mathcal{F}$,

$$\sqrt{N} < |I_i| \quad \text{and} \quad |J| \leq N. \quad (7.4.2)$$

Recall $d \leq (\log \log N)^D$. Provided that we can show (7.4.1), we take $f_1, f_2 = F_0$ and obtain

$$\begin{aligned} Y(U_1, \dots, U_k, J) &\leq X(I_1, \dots, I_k; J, f_0, f_0) \\ &\ll |I_1| \cdots |I_k| |J|^2 \frac{1}{(\log N)^2} \\ &\ll |U_1| \cdots |U_k| |J|^2 (\log \log N)^{kD} \frac{1}{(\log N)^{2B}} \\ &\ll |U_1| \cdots |U_k| |J|^2 \frac{1}{(\log N)^B}. \end{aligned}$$

Thus, to prove Proposition 7.2.1 and consequently to prove Theorem 6.2.1, it suffices to show (7.4.1). The proof of (7.4.1) is the matter of the remaining paper. To do so, we need the following technical lemma which is similar to [65, Proposition 5.1].

Lemma 7.4.1. *For $f_1, f_2 \in \mathcal{F}$, $L \in \mathbb{N}$ we have*

$$\begin{aligned} &X(q^L I_1, \dots, q^L I_k; q^L J, f_1, f_2) \\ &= \sum_{\mathbf{r}_1, \dots, \mathbf{r}_L \in \mathcal{Q}^k} \sum_{\mathbf{i}_1, \dots, \mathbf{i}_L \in \mathcal{Q}^2} \\ &\quad \prod_{\ell=1}^L \alpha(\Xi_{\{\mathbf{r}_j, i_{j1}\}_{1 \leq j \leq \ell-1}}(f_1), \Xi_{\{\mathbf{r}_j, i_{j2}\}_{1 \leq j \leq \ell-1}}(f_2), \mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2}) \quad (7.4.3) \\ &X(I_1, \dots, I_k, J; \Xi_{\{\mathbf{r}_1, i_{\ell 1}\}_{1 \leq \ell \leq L}}, \Xi_{\{\mathbf{r}_1, i_{\ell 2}\}_{1 \leq \ell \leq L}}(f_1)), \end{aligned}$$

where

$$\begin{aligned} &\alpha(f_1, f_2, \mathbf{r}, i_1, i_2) \\ &:= e \left(\frac{h}{m} \sum_{S \subseteq M} (-1)^{k-|S|} (b(f_1, S, \mathbf{r}, i_1) - b(f_2, S, \mathbf{r}, i_2)) \right), \end{aligned}$$

and $b(f, S, \mathbf{r}, i) \in \mathcal{Q}$ is defined via

$$di + \sum_{t \in S} r_t + f(S) = zq + b(f, S, \mathbf{r}, i)$$

with $z \in \mathbb{N}$.

Remark 7.4.2. Note that $z = \Xi_{\mathbf{r}, i}(f)(S) = \lfloor di + \sum_{t \in S} r_t + f(S) \rfloor_q$.

Proof. Note that for an interval of integers I , we have

$$qI = \{qh + r : h \in I, r \in \mathcal{Q}\}.$$

We first prove the case $L = 1$. Therefore, we consider

$$\begin{aligned} & \Phi(qh_1 + r_1, \dots, qh_k + r_k; qJ, f_1) \\ = & \sum_{i \in \mathcal{Q}} \sum_{n \in J} e \left(\frac{h}{m} \sum_{S \subseteq M} (-1)^{k-|S|} \right. \\ & \left. + s_q \left(q \left(dn + \sum_{t \in S} h_t \right) + di + \sum_{t \in S} r_t + f_1(s) \right) \right). \end{aligned}$$

Since

$$di + \sum_{t \in S} r_t + f_1(s) = q\Xi_{\mathbf{r}, i}(f_1)(S) + b(f_1, S, \mathbf{r}, i),$$

we get due to the q -additivity of the sum-of-digits function

$$\begin{aligned} & s_q \left(q \left(dn + \sum_{t \in S} h_t \right) + di + \sum_{t \in S} r_t + f_1(S) \right) \\ = & s_q \left(dn + \sum_{t \in S} h_t + \Xi_{\mathbf{r}, i}(f_1)(S) \right) + b(f_1, S, \mathbf{r}, i). \end{aligned}$$

By the definition of $X(I_1, \dots, I_k; J, f_1, f_2)$, the lemma is proved in the case $L = 1$. Repeating the procedure $L - 1$ times yields the result. \square

Lemma 7.4.3. *One has*

$$\begin{aligned}\alpha(F_0, F_0, \mathbf{0}, 0, 0) &= 1, \\ \alpha(F_1, F_0, \mathbf{0}, 0, 0) &= e\left(\frac{h}{m}\right) \quad \text{and} \\ \alpha(F_1, F_0, \mathbf{r}^*, 0, 0) &= e\left((1-q)\frac{h}{m}\right),\end{aligned}$$

where \mathbf{r}^* is defined in (7.3.2).

Proof. Let

$$\Upsilon_{\mathbf{r},i}(f)(S) := di + \sum_{t \in S} r_t + f(S).$$

The remainder occurring at the division of $\Upsilon_{\mathbf{r},i}(f)(S)$ by q is $b(f, S, \mathbf{r}, i)$. Since $\Upsilon_{\mathbf{0},0}(F_0)(S) = 0$ for all $S \subseteq M$, the first statement of the lemma is valid. We have further $\Upsilon_{\mathbf{0},0}(F_1)(S) = 0$ for all $S \subsetneq M$ and $\Upsilon_{\mathbf{0},0}(F_1)(M) = 1$, thus $\alpha(F_1, F_0, \mathbf{0}, 0, 0) = e(h/m)$.

It remains to prove the last statement of the lemma. For all $S \subsetneq M$ we have $\Upsilon_{\mathbf{r}^*,0}(F_1)(S) = \Upsilon_{\mathbf{r}^*,0}(F_0)(S)$ and consequently $b(F_1, S, \mathbf{r}^*, 0) = b(F_0, S, \mathbf{r}^*, 0)$. Hence

$$\alpha(F_1, F_0, \mathbf{r}^*, 0, 0) = e\left(\frac{h}{m} (b(F_1, M, \mathbf{r}^*, 0) - b(F_0, M, \mathbf{r}^*, 0))\right).$$

We have $\Upsilon_{\mathbf{r}^*,0}(F_1)(M) = q$ and $\Upsilon_{\mathbf{r}^*,0}(F_0)(M) = q - 1$. Hence

$$b(F_1, M, \mathbf{r}^*, 0) - b(F_0, M, \mathbf{r}^*, 0) = q - 1,$$

and the lemma follows. \square

Recall that we need to show (7.4.1) in order to proof Theorem 6.2.1.

Lemma 7.4.4. *Let $L := L' + 2$, where L' as in Lemma 7.3.1. Let further $m \nmid h(q-1)$, and $f_1, f_2 \in \mathcal{F}$. Then the inequality*

$$\begin{aligned}& |X(q^{Lt}I_1, \dots, q^{Lt}I_k, q^{Lt}J; f_1, f_2)| \\ & \leq \left(1 - \frac{\pi^2}{(4m^2q^{(k+2)L})}\right)^t (q^{Lt}|I_1|) \cdots (q^{Lt}|I_k|) (q^{Lt}|J|)^2\end{aligned}$$

holds for all $t \in \mathbb{N}$.

Proof. We extract two summands V_1 and V_2 from (7.4.3) that correspond to the sequences \mathcal{V}_1 and respectively \mathcal{V}_2 defined in (7.3.5). Thus Lemma 7.4.1 yields

$$\begin{aligned} & X(q^L I_1, \dots, q^L I_k; q^L J, f_1, f_2) \\ &= V_1 + V_2 \\ &+ \sum_{\Gamma} \prod_{\ell=1}^L \alpha(\Xi_{\{\mathbf{r}_j, i_{j1}\}_{1 \leq j \leq \ell-1}}(f_1), \Xi_{\{\mathbf{r}_j, i_{j2}\}_{1 \leq j \leq \ell-1}}(f_2), \mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2}) \\ & X(I_1, \dots, I_k, J; \Xi_{\{\mathbf{r}_1, i_{\ell 1}\}_{1 \leq \ell \leq L}}, \Xi_{\{\mathbf{r}_1, i_{\ell 2}\}_{1 \leq \ell \leq L}}(f_1)), \end{aligned} \quad (7.4.4)$$

where Γ denotes the set of all $(\mathbf{r}_1, \dots, \mathbf{r}_L, \mathbf{i}_1, \dots, \mathbf{i}_L) \in (\mathcal{Q}^k)^L \times (\mathcal{Q}^2)^L$ apart from the two elements corresponding to \mathcal{V}_1 or \mathcal{V}_2 . Thus $|\Gamma| = q^{(k+2)L} - 2$. We use the abbreviation

$$A(f_1, f_2) := \prod_{\ell=1}^{L-2} \alpha(\Xi_{\{\mathbf{r}_j, i_{j1}\}_{1 \leq j \leq \ell-1}}(f_1), \Xi_{\{\mathbf{r}_j, i_{j2}\}_{1 \leq j \leq \ell-1}}(f_2), \mathbf{r}_\ell, i_{\ell 1}, i_{\ell 2}).$$

We obtain by (7.3.6) and (7.3.7) that

$$\begin{aligned} V_1 = & A(f_1, f_2) \alpha(F_1, F_0, \mathbf{0}, 0, 0) \alpha(F_0, F_0, \mathbf{0}, 0, 0) \\ & X(I_1, \dots, I_k, J; F_0, F_0) \end{aligned}$$

and

$$\begin{aligned} V_2 = & A(f_1, f_2) \alpha(F_1, F_0, \mathbf{r}^*, 0, 0) \alpha(F_1, F_0, \mathbf{0}, 0, 0) \\ & X(I_1, \dots, I_k, J; F_0, F_0). \end{aligned}$$

By 7.4.3, we thus get

$$\begin{aligned} V_1 + V_2 = & A(f_1, f_2) e\left(\frac{h}{m}\right) \left(1 + e\left((1-q)\frac{h}{m}\right)\right) \\ & X(I_1, \dots, I_k, J, F_0, F_0). \end{aligned}$$

For given functions $f_1, f_2, g_1, g_2 \in \mathcal{F}$, let E_{f_1, f_2, g_1, g_2} denote the set of

all $(\mathbf{r}_1, \dots, \mathbf{r}_L, \mathbf{i}_1, \dots, \mathbf{i}_L) \in \Gamma$ satisfying

$$\begin{aligned} & X(I_1, \dots, I_k, J; \Xi_{\{\mathbf{r}_1, i_{\ell 1}\}_{1 \leq \ell \leq L}}, \Xi_{\{\mathbf{r}_1, i_{\ell 2}\}_{1 \leq \ell \leq L}}(f_1)) \\ = & X(I_1, \dots, I_k, J, g_1, g_2). \end{aligned}$$

We define

$$a'(f_1, f_2, g_1, g_2) := \sum_{E_{f_1, f_2, g_1, g_2}} \alpha(f_1, f_2, \mathbf{r}, i_1, i_2).$$

Recall that $|\Gamma| = q^{(k+2)L} - 2$. The absolute value of the function α is at most 1. Hence, for all $f_1, f_2 \in \mathcal{F}$ one has

$$\sum_{(g_1, g_2) \in \mathcal{F}^2} |a'(f_1, f_2, g_1, g_2)| \leq q^{(k+2)L} - 2.$$

We rearrange the sum (7.4.4) and get

$$\begin{aligned} & X(q^L I_1, \dots, q^L I_k; q^L J, f_1, f_2) \\ = & \sum_{(F_0, F_0) \neq (g_1, g_2) \in \mathcal{F}} a'(f_1, f_2, g_1, g_2) X(I_1, \dots, I_k, J, g_1, g_2) \\ & + \left(a'(F_0, F_0) + A(f_1, f_2) e\left(\frac{h}{m}\right) \left(1 + e\left((1-q)\frac{h}{m}\right)\right) \right) \\ & X(I_1, \dots, I_k, J, F_0, F_0). \end{aligned}$$

Let

$$a(f_1, f_2, g_1, g_2) := a'(f_1, f_2, g_1, g_2)$$

if $(g_1, g_2) \neq (F_0, F_0)$ and let

$$\begin{aligned} & a(f_1, f_2, F_0, F_0) \\ := & a'(f_1, f_2, F_0, F_0) + A(f_1, f_2) e\left(\frac{h}{m}\right) \left(1 + e\left((1-q)\frac{h}{m}\right)\right). \end{aligned}$$

We have

$$\left| e\left(\frac{h}{m}\right) \left(1 + e\left((1-q)\frac{h}{m}\right)\right) \right| \leq \left| 1 + e\left(\frac{1}{m}\right) \right| \leq 2 - \left(\frac{\pi}{2m}\right)^2,$$

by our assumption $m \nmid h(q-1)$. We therefore obtain

$$\begin{aligned} & \sum_{(g_1, g_2) \in \mathcal{F}^2} |a(f_1, f_2, g_1, g_2)| \\ & \leq q^{(k+2)L} - \left(\frac{\pi}{2m}\right)^2 = q^{(k+2)L} \left(1 - \frac{\pi^2}{(4m^2 q^{(k+2)L})}\right). \end{aligned} \quad (7.4.5)$$

Now, we define an $|\mathcal{F}^2| \times |\mathcal{F}^2|$ matrix Z by

$$Z := (|a(f_1, f_2, g_1, g_2)|)_{(f_1, f_2) \in \mathcal{F}^2, (g_1, g_2) \in \mathcal{F}^2}.$$

We get the inequality

$$\begin{aligned} & (|X(q^L I_1, \dots, q^L I_k, q^L; f_1, f_2)|)_{(f_1, f_2) \in \mathcal{F}^2} \\ & \leq Z (|X(q I_1, \dots, q I_k, q; f_1, f_2)|)_{(g_1, g_2) \in \mathcal{F}^2} \end{aligned} \quad (7.4.6)$$

which is meant componentwise.

Let $t \in \mathbb{N}$. Due to (7.4.5), we are able to apply Lemma 7.3.2 and we obtain by the t -fold iterations of the inequality (7.4.6) together with the trivial bound

$$|X(I_1, \dots, I_k, J; f_1, f_2)| \leq |I_1| \cdots |I_k| |J|^2$$

the inequality

$$\begin{aligned} & |X(q^{Lt} I_1, \dots, q^{Lt} I_k, q^{Lt} J; f_1, f_2)| \\ & \leq \left(1 - \frac{\pi^2}{(4m^2 q^{(k+2)L})}\right)^t (q^{Lt} |I_1|) \cdots (q^{Lt} |I_k|) (q^{Lt} |J|)^2. \end{aligned}$$

□

7.5 Conclusion

Let $D, B > 0$. We assume $N \geq k$. We take

$$t := \left\lfloor \frac{\log N}{8D \log \log \log N} \right\rfloor.$$

Since $d \leq (\log \log N)^D$, we have

$$L \leq \frac{\log(d(k+d))}{\log q} + 3 \leq 2D \left(\frac{\log \log \log N}{\log q} + 1 \right)$$

and

$$q^{Lt} \leq N^{1/4 + \log q / (4 \log \log N)}$$

for all $N \in N$ with $(\log \log N)^D \geq k$. Thus there is an integer N_0 and some $\varepsilon > 0$, depending only on q, k and D such that for all $N \geq N_0$ we have

$$\frac{\sqrt{N}}{q^{Lt}} \leq N^{-\varepsilon}. \quad (7.5.1)$$

For any $0 < \sigma < 1$ one has $(1 - \sigma)^t < e^{-t\sigma}$. Thus we get

$$\left(1 - \frac{\pi^2}{(4m^2 q^{(k+2)L})} \right)^t \ll e^{-c \log N / (\log \log \log N (\log \log N)^{(2D+1)(k+2)})},$$

where $c = \pi^2 / (36Dm^2)$. Hence

$$\begin{aligned} \left(1 - \frac{\pi^2}{(4m^2 q^{(k+2)L})} \right)^t &\ll (\log N)^{-c \log N / (\log \log \log N (\log \log N)^{(2D+1)(k+2)+1})} \\ &\ll (\log N)^{-2B}. \end{aligned} \quad (7.5.2)$$

Now, we are able to show (7.4.1) which yields Proposition 7.2.1 and concludes the proof of Theorem 6.2.1. We need to estimate

$$X(I_1, \dots, I_k; J, f_1, f_2)$$

where the intervals satisfy (7.4.2). For $1 \leq j \leq k+1$, the integers a_j and b_j are defined by $I_j = [a_j, b_j]$ and $J = [a_{k+1}, b_{k+1}]$. Besides the integers u_j, v_j, r_j, s_j with $0 \leq r_j, s_j < q^{Lt}$ are uniquely defined by

$$a_j = q^{Lt} u_j + r_j, \quad b_j = q^{Lt} v_j + s_j$$

for all $1 \leq j \leq k+1$. Notice that $u_j \neq v_j$ by (7.4.2) and (7.5.1). We

finally define

$$\tilde{I}_j := [u_j, v_j], \quad \tilde{J} := [u_{k+1}, v_{k+1}]$$

for $1 \leq j \leq k$. It is a straightforward exercise to verify

$$\begin{aligned} & X(I_1, \dots, I_k, J; f_1, f_2) \\ &= X(q^{Lt} \tilde{I}_1, \dots, q^{Lt} \tilde{I}_k, q^{Lt} \tilde{J}; f_1, f_2) + O\left(|I_1| \cdots |I_k| |J|^2 \frac{\sqrt{N}}{q^{Lt}}\right). \end{aligned}$$

By Lemma 7.4.4, we finally get

$$\ll \left(\left(1 - \frac{\pi^2}{(4m^2 q^{(k+2)L})}\right)^t + \frac{\sqrt{N}}{q^{Lt}} \right) |I_1| \cdots |I_k| |J|^2.$$

Proposition 7.2.1 is proved by applying (7.5.1) and (7.5.2).

References

- [1] E. ALKAN, *On the sizes of gaps in the Fourier expansion of modular forms*, *Canad. J. Math.*, 57 (2005), pp. 449–470.
- [2] E. ALKAN AND A. ZAHARESCU, *B-free numbers in short arithmetic progressions*, *J. Number Theory*, 113 (2005), pp. 226–243.
- [3] R. C. BAKER AND J. BRÜDERN, *Sums of cubes of square-free numbers*, *Monatsh. Math.*, 111 (1991), pp. 1–21.
- [4] ———, *Sums of cubes of square-free numbers. II*, *Monatsh. Math.*, 112 (1991), pp. 177–207.
- [5] A. BALOG AND A. SÁRKÖZY, *On sums of integers having small prime factors. I, II*, *Studia Sci. Math. Hungar.*, 19 (1984), pp. 35–47, 81–88.
- [6] R. BELLMAN AND H. N. SHAPIRO, *On a problem in additive number theory*, *Ann. of Math. (2)*, 49 (1948), pp. 333–340.
- [7] J. BÉSINEAU, *Indépendance statistique d’ensembles liés à la fonction “somme des chiffres”*, *Acta Arith.*, 20 (1972), pp. 401–416.
- [8] V. BLOMER, *The average value of divisor sums in arithmetic progressions*, *Q. J. Math.*, 59 (2008), pp. 275–286.
- [9] J. BRÜDERN, *Einführung in die analytische Zahlentheorie*, Springer, 1995.
- [10] ———, *Binary additive problems and the circle method, multiplicative sequences and convergent sieves*, *Astérisque*, (2009).
- [11] J. BRÜDERN AND É. FOUVRY, *Lagrange’s four squares theorem with almost prime variables*, *J. Reine Angew. Math.*, 454 (1994), pp. 59–96.
- [12] L. E. BUSH, *An asymptotic formula for the average sum of the digits of integers*, *Amer. Math. Monthly*, 47 (1940), pp. 154–156.
- [13] A. CAUCHY, *Recherches sur les nombres*, *J. Ecole polytech*, 9 (1813), pp. 99–123.

- [14] I. CHOWLA, *A theorem on the addition of residue classes: Application to the number $\gamma(k)$ in Waring's problem*, The Quarterly Journal of Mathematics, 8 (1936), pp. 99–102.
- [15] C. DARTYGE AND C. MAUDUIT, *Nombres presque premiers dont l'écriture en base r ne comporte pas certains chiffres*, J. Number Theory, 81 (2000), pp. 270–291.
- [16] —, *Ensembles de densité nulle contenant des entiers possédant au plus deux facteurs premiers*, Journal of Number Theory, 91 (2001), pp. 230–255.
- [17] C. DARTYGE AND G. TENENBAUM, *Sommes des chiffres de multiples d'entiers*, in Annales de l'institut Fourier, vol. 55, 2005, pp. 2423–2474.
- [18] H. DAVENPORT, *On the addition of residue classes*, Journal of the London Mathematical Society, 1 (1935), p. 30.
- [19] —, *On Waring's Problem for cubes*, Acta. Math., 71 (1939), pp. 123–143.
- [20] —, *On Waring's Problem for fourth powers*, Ann. Math., 40 (1939), pp. 731–747.
- [21] —, *Analytic methods for Diophantine equations and Diophantine inequalities*, Cambridge University Press, Cambridge, second ed., 2005.
- [22] H. DELANGE, *Sur la fonction sommatoire de la fonction "somme des chiffres"*, Enseignement Math. (2), 21 (1975), pp. 31–47.
- [23] M. P. DRAZIN AND J. S. GRIFFITH, *On the decimal representation of integers*, Proc. Cambridge Philos. Soc., 48 (1952), pp. 555–565.
- [24] N. D. ELKIES, *Distribution of supersingular primes*, Astérisque, (1991), pp. 127–132 (1992). Journées Arithmétiques, 1989 (Luminy, 1989).
- [25] P. ERDŐS, *On the difference of consecutive terms of sequences defined by divisibility properties*, Acta Arith, 12 (1966/1967), pp. 175–182.

- [26] P. ERDŐS, C. MAUDUIT, AND A. SÁRKÖZY, *On arithmetic properties of integers with missing digits. I. Distribution in residue classes*, J. Number Theory, 70 (1998), pp. 99–120.
- [27] —, *On arithmetic properties of integers with missing digits. II. Prime factors*, Discrete Math., 200 (1999), pp. 149–164. Paul Erdős memorial collection.
- [28] T. ESTERMANN, *On sums of squares of square-free numbers*, Proc. London Math. Soc. (2), 53 (1951), pp. 125–137.
- [29] K. B. FORD, *New estimates for mean values of Weyl sums*, Internat. Math. Res. Notices, (1995), pp. 155–171 (electronic).
- [30] E. FOUVRY AND C. MAUDUIT, *Methodes des crible et fonctions sommes des chiffres*, Acta Arith, 77 (1996), pp. 339–351.
- [31] —, *Sommes des chiffres et nombres presque premiers*, Mathematische Annalen, 305 (1996), pp. 571–599.
- [32] A. O. GEL'FOND, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith., 13 (1967/1968), pp. 259–265.
- [33] G. HARCOS, *Waring's problem with small prime factors*, Acta Arith., 80 (1997), pp. 165–185.
- [34] G. HARDY AND S. RAMANUJAN, *Asmptotic formulae in combinatory analysis*, Proc. London Math. Soc., 17 (1918), pp. 75–115.
- [35] G. H. HARDY AND J. E. LITTLEWOOD, *Some problems of 'Partitio Numerorum': I A New solution of Waring's problem*, Göttinger Nachrichten, (1920), pp. 33–54.
- [36] —, *Some problems of 'Partitio Numerorum': II Proof that every large number is the sum of at most 21 biquadrates*, Math. Z., 9 (1921), pp. 14–27.
- [37] —, *Some problems of 'Partitio Numerorum': IV The singular series in Waring's problem*, Math. Z., 12 (1922), pp. 161–188.
- [38] —, *Some problems of 'Partitio Numerorum': VI Further recherche in Waring's problem*, Math. Z., 23 (1925), pp. 1–37.

- [39] G. H. HARDY AND E. M. WRIGHT, *An introduction to the theory of numbers*, The Clarendon Press Oxford University Press, New York, fifth ed., 1979.
- [40] —, *An introduction to the theory of numbers*, Oxford University Press, Oxford, sixth ed., 2008. Revised by D. R. Heath-Brown and J. H. Silverman.
- [41] D. HILBERT, *Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n -ter Potenzen (Waringsche Problem)*, Königl. G. Wiss. Göttingen, (1909), pp. 17–36.
- [42] M. D. HIRSCHHORN, *A simple proof of Jacobi's four-square theorem*, J. Austral. Math. Soc. Ser. A, 32 (1982), pp. 61–67.
- [43] —, *A simple proof of Jacobi's four-square theorem*, Proc. Amer. Math. Soc., 101 (1987), pp. 436–438.
- [44] C. HOOLEY, *A note on square-free numbers in arithmetic progressions*, Bull. London Math. Soc., 7 (1975), pp. 133–138.
- [45] L. K. HUA, *On Waring's problem*, Quart. J. Math. Oxford, 9 (1938), pp. 199–202.
- [46] —, *Die Abschätzung von Exponentialsummen und ihre Anwendung in der Zahlentheorie*, vol. 2 of Enzyklopädie der mathematischen Wissenschaften: Mit Einschluss ihrer Anwendungen, Bd. I, B. G. Teubner Verlagsgesellschaft, Leipzig, 1959.
- [47] —, *Additive theory of prime numbers*, Translations of Mathematical Monographs, Vol. 13, American Mathematical Society, Providence, R.I., 1965.
- [48] M. JANCEVSKIS, *Convergent sieve sequences in arithmetic progressions*, J. Number Theory, 129 (2009), pp. 1595–1607.
- [49] —, *A hybrid result related to Waring's problem, squarefree numbers, and digital restrictions*, submitted, . (2009), p. .
- [50] —, *A note on Waring's problem with convergent sieve sequences*, Unif. Distrib. Theory, 4 (2009), p. .

- [51] K. KAWADA AND T. D. WOOLEY, *On the Waring-Goldbach problem for fourth and fifth powers*, Proc. London Math. Soc. (3), 83 (2001), pp. 1–50.
- [52] D.-H. KIM, *On the joint distribution of q -additive functions in residue classes*, J. Number Theory, 74 (1999), pp. 307–336.
- [53] J. M. KUBINA AND M. C. WUNDERLICH, *Extending Waring’s conjecture to 471,600,000*, Math. Comp., 55 (1990), pp. 815–820.
- [54] R. LIDL AND H. NIEDERREITER, *Finite fields*, vol. 20 of Encyclopedia of Mathematics and its Applications, Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983.
- [55] U. LINNIK, *On the representation of large numbers as sums of seven cubes*, Matematicheskii Sbornik, 54 (1943), pp. 218–224.
- [56] C. MAUDUIT AND J. RIVAT, *Sur un problème de gelfond : la somme des chiffres des nombres premiers*, Ann. Math., 112 (to appear), pp. 177–207.
- [57] L. MIRSKY, *A theorem on representations of integers in the scale of r* , Scripta Math., 15 (1949), pp. 11–12.
- [58] I. NIVEN, H. S. ZUCKERMAN, AND H. L. MONTGOMERY, *An introduction to the theory of numbers*, John Wiley & Sons Inc., New York, fifth ed., 1991.
- [59] A. PETHŐ AND R. F. TICHY, *On digit expansions with respect to linear recurrences*, J. Number Theory, 33 (1989), pp. 243–256.
- [60] E. V. PODSYPANIN, *On the representation of the integer by positive quadratic forms with square-free variables*, Acta Arith., 27 (1975), pp. 459–488.
- [61] K. PRACHAR, *Über die kleinste quadratfreie Zahl einer arithmetischen Reihe*, Monatsh. Math., 62 (1958), pp. 173–176.
- [62] G. TENENBAUM, *Introduction à la théorie analytique et probabiliste des nombres*, vol. 1 of Cours Spécialisés [Specialized Courses], Société Mathématique de France, Paris, second ed., 1995.

- [63] K. THANIGASALAM, *Improvement on Davenport's iterative method and new results in additive number theory. III*, Acta Arith., 48 (1987), pp. 97–116.
- [64] J. M. THUSWALDNER AND R. F. TICHY, *An Erdős-Kac theorem for systems of q -additive functions*, Indag. Math. (N.S.), 11 (2000), pp. 283–291.
- [65] —, *Waring's problem with digital restrictions*, Israel J. Math., 149 (2005), pp. 317–344. Probability in mathematics.
- [66] J. R. TROLLOPE, *An explicit expression for binary digital sums*, Math. Mag., 41 (1968), pp. 21–25.
- [67] K. M. TSANG, *The distribution of r -tuples of squarefree numbers*, Mathematika, 32 (1985), pp. 265–275 (1986).
- [68] R. C. VAUGHAN, *The Hardy-Littlewood method*, vol. 80 of Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge, 1981.
- [69] —, *On Waring's problem for smaller exponents*, Proc. London Math. Soc. (3), 52 (1986), pp. 445–463.
- [70] —, *On Waring's problem for smaller exponents. II*, Mathematika, 33 (1986), pp. 6–22.
- [71] R. C. VAUGHAN AND T. D. WOOLEY, *Further improvements in Waring's problem. III. Eighth powers*, Philos. Trans. Roy. Soc. London Ser. A, 345 (1993), pp. 385–396.
- [72] —, *Further improvements in Waring's problem. II. Sixth powers*, Duke Math. J., 76 (1994), pp. 683–710.
- [73] —, *Further improvements in Waring's problem*, Acta Math., 174 (1995), pp. 147–240.
- [74] —, *Further improvements in Waring's problem. IV. Higher powers*, Acta Arith., 94 (2000), pp. 203–285.
- [75] —, *Waring's problem: a survey*, in Number theory for the millennium, III (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 301–340.

- [76] I. M. VINOGRADOV, *The method of trigonometrical sums in the theory of numbers*, Trav. Inst. Math. Stekloff, 23 (1947), p. 109.
- [77] A. WALFISZ, *Zur additiven Zahlentheorie. II*, Math. Z., 40 (1936), pp. 592–607.
- [78] E. WARING, *Meditationes Algebraicae (translation of the edition from 1782)*, American Math. Soc., Providence, 1991.
- [79] R. WARLIMONT, *On squarefree numbers in arithmetic progressions*, Monatshefte für Mathematik, 73 (1969), pp. 433–448.
- [80] G. WATSON, *A proof of the seven cube theorem*, J. London Math. Soc, 26 (1951), pp. 153–156.
- [81] H. WEYL, *Über die Gleichverteilung von Zahlen mod. eins*, Mathematische Annalen, 77 (1916), pp. 313–352.
- [82] T. D. WOOLEY, *Large improvements in Waring’s problem*, Ann. of Math. (2), 135 (1992), pp. 131–164.
- [83] —, *New estimates for smooth Weyl sums*, J. London Math. Soc. (2), 51 (1995), pp. 1–13.
- [84] D. ZAGIER, *A one-sentence proof that every prime $p \equiv 1 \pmod{4}$ is a sum of two squares*, Amer. Math. Monthly, 97 (1990), p. 144.