ON A DIAGONAL QUADRIC IN DENSE VARIABLES

EUGEN KEIL

ABSTRACT. We examine the solubility of a diagonal, translation invariant, quadratic equation system in arbitrary (dense) subsets $\mathcal{A} \subset \mathbb{Z}$ and show quantitative bounds on the size of $\mathcal{A}$ if there are no non-trivial solutions. We use the circle method and Roth's density increment argument. Due to a restriction theory approach we can deal with equations in $s \geq 7$ variables.

1. INTRODUCTION

Diophantine equations with an underlying symmetry group appear naturally in many number theoretic questions and their structure can often be exploited to obtain solutions in situations where standard methods fail. This is one of the main reasons why translation invariant systems have attracted so much interest. The important special case of linear systems was approached by methods ranging from Fourier-analysis [20] over ergodic theory [8] to (additive) combinatorics [10], [24] and gave rise to recent amazing developments in the theory of linear equations in the primes [14].

A first attempt to introduce non-linear terms was made by Lovász. He conjectured that

$$x_1 - x_2 = y^2$$

with $x_1, x_2 \in \mathcal{A} \subset \mathbb{N}$ and $y \in \mathbb{N}$ has solutions for any dense set $\mathcal{A}$. This was proven independently by Furstenberg [8] and Sárközy [22], and a simplified proof can be found in [11]. Generalisations of this result replace y^2 by more general polynomials and consider more equations. An important result arising from this work is the polynomial Szemerédi theorem of Bergelson and Leibman [2].

Quite remarkably, the case of higher degree in the variables x_i was neglected until Smith [23] considered a family of translation invariant quadratic equation systems

$$(1.1) \qquad \begin{aligned} \lambda_1 x_1^2 + \lambda_2 x_2^2 + \ldots + \lambda_s x_s^2 &= 0, \\ \lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_s x_s &= 0, \end{aligned}$$

where $\lambda_i \in \mathbb{Z}$ and the x_i are restricted to an arbitrary set $\mathcal{A} \subset \{1, 2, \ldots, N\}$. For a translation invariant system we expect non-trivial solutions if the set $\mathcal{A}$ has many elements. We ask the quantitative question: Assume there are only trivial solutions to (1.1), what can we say about the size of $\mathcal{A}$?

Smith [23] uses the circle method and uniformity norms to obtain an upper bound on the cardinality of $\mathcal{A}$ of size $CN(\log \log N)^{-c}$ for some $C, c > 0$ as long as $s \geq 9$. In other words, any set with larger cardinality has non-trivial solutions. Our goal here is to improve on his work by removing the uniformity norms from the argument and reducing the number of variables down to $s \geq 7$. This is done under the following natural conditions.

Conditions 1.
(i) $\lambda_1 + \lambda_2 + \ldots + \lambda_s = 0$,

(ii) $s \geq 7$ and $\lambda_i \neq 0$ for all $1 \leq i \leq s$,
(iii) there are at least two positive and at least two negative coefficients λ_i.

The first condition ensures translation invariance of the system, which is the key property in problems of this type, as explained above. If system (1.1) is not translation invariant, it is easy to construct dense sets without non-trivial solutions by using divisibility obstructions. Choose for instance $\mathcal{A}$ to be the set of numbers congruent to 1 modulo n for a natural number $n > |\lambda_1 + \lambda_2 + \ldots + \lambda_s|$.

Before we discuss the other two conditions and give a historical overview, we state the main theorem of this work. Write $|\mathcal{A}|$ for the cardinality of $\mathcal{A}$ and call a solution with $x_i = x_j$ for some $i \neq j$ a *trivial solution* of (1.1).

Theorem 1.1. *Assume that the conditions above hold and system* (1.1) *has only trivial solutions for $x_i \in \mathcal{A} \subset \{1, 2, \ldots, N\}$. Then we have the bound $|\mathcal{A}| \leq CN(\log \log N)^{-1/15}$ for some constant C, which depends on the coefficients λ_i of the system.*

The bound $s \geq 7$ in condition (*ii*) seems to be best possible in what can be achieved by this type of Fourier-analytic methods. If we assume the existence of non-trivial integer solutions of (1.1), then a qualitative version of Theorem 1.1 can be deduced from Szemeredi's theorem for any $s \geq 4$ as follows. First we locate an arithmetic progression in $\mathcal{A}$ of length $2k + 1$. By homogeneity and translation invariance of (1.1), we can rescale to $\{-k, \ldots, k\}$ without changing the shape of the system. When k is large enough, there are non-trivial solutions by assumption on the system and we are done.

To see why condition (*iii*) is needed, we observe that conditions (*i*) and (*ii*) imply that there is at least one positive and at least one negative coefficient in (1.1). But in situations where we have exactly one negative (positive) coefficient λ_i, we have only trivial solutions. To see this, we use the translation invariance. If there is a non-trivial solution, there has to be one with $x_i = 0$. The remaining quadratic equation is positive (negative) definite and this forces the other variables to be zero as well. Therefore, condition (*iii*) is necessary and we use it to ensure the existence of a non-singular real solution to (1.1) in our application of the circle method.

It is possible to derive a simple corollary from Theorem 1.1.

Corollary 1.2. *Under the conditions above, a diagonal quadratic form*
$$\lambda_1 x_1^2 + \lambda_2 x_2^2 + \ldots + \lambda_s x_s^2 = 0$$
has non-trivial solutions in any set $\mathcal{A} \subset \{1, 2, \ldots, N\}$ of density $|\mathcal{A}|/N \geq C(\log \log N)^{-1/15}$ for a constant C, which depends on the coefficients λ_i of the system.

It is apparent that better quantitative estimates in Theorem 1.1 lead to a wider range of sets $\mathcal{A}$ which are covered by the result. One of the major (widely open) goals is to improve on those bounds such that they cover interesting number theoretic sets, such as the primes. (One can handle the corollary in the case of prime numbers by classical techniques already for $s \geq 5$.)

The general interest in quantitative estimates goes back to a conjecture of Erdős and Turan [7] from 1936. Does every subset
$$\mathcal{A} = \{a_1 < a_2 < a_3 \ < \ \ldots\} \ \subset \ \mathbb{N}$$
contain an arithmetic progression of arbitrary length k, if all we know is that
$$\sum_{i=1}^{\infty} \frac{1}{a_i} = \infty?$$

The first progress was made by Roth [20], who showed that in the absence of non-trivial arithmetic progressions of length three the size of $\mathcal{A}$ in an interval of length N is bounded by $CN(\log\log N)^{-1}$ for some constant $C > 0$. There have been several improvements on Roth's theorem, for example by Heath-Brown [16], who obtained an upper bound $|\mathcal{A}| \leq CN\log^{-c} N$ for some small $c > 0$ and later Bourgain [5] with a bound of the form $|\mathcal{A}| \leq CN(\log N)^{-2/3}(\log\log N)^2$. A recent breakthrough is the result $|\mathcal{A}| \leq CN(\log N)^{-1}(\log\log N)^5$ of Sanders [21], which is remarkable since an estimate of the form $CN(\log N)^{-1}(\log\log N)^{-2}$ would be enough to settle the conjecture of Erdős and Turan in the case $k = 3$.

In the case of general k-term progressions, where the classical Fourier-analytic approach fails, the bounds are even weaker. Szemeredi [24] proved by a complicated combinatorial method that $|\mathcal{A}|/N \to 0$ as $N \to \infty$, but his method gave no useful bound on $|\mathcal{A}|$. Gowers [10] gave a quantitative bound of size $C_k N(\log\log N)^{-c_k}$ for arbitrary $k \geq 4$ by using 'uniformity norms' and a variant of Freiman's theorem. As mentioned earlier, there is an ergodic theoretic approach by Furstenberg [8] (see [9] for an exposition), who gave a simpler proof for Szemeredi's result without any explicit bound at all.

Our method here is essentially the one used by Roth. There seem to be no obvious generalisation of the other methods to improve on the density estimate in our result, but it is reasonable to conjecture that the $(\log\log N)^{-1/15}$ is still far away from the truth.

2. Notation and Remarks

Many sections of this paper are independent of each other and it is convenient to introduce some of the notation at the beginning of each section, where it is needed. At this point we focus on the most important things, which are relevant throughout the paper.

Write $e(x) = \exp(2\pi ix)$ and $e_q(x) = e(x/q)$ for $q \in \mathbb{N}$. We use the usual notation $f = O(g)$ to express that $|f| \leq Cg$ for some constant $C > 0$ and similarly Vinogradov's notation $f \ll g$. We indicate dependencies on parameters by subscripts as in $O_p(N^s)$ or $\ll_{P,\epsilon}$, for example. We write $\hat{f}$ for the Fourier transform of a function $f : \mathbb{R} \to \mathbb{R}$. Bold face letters such as $\mathbf{x}$ denote vectors with components x_i and $\mathbf{x} \cdot \mathbf{y}$ is the usual scalar product. Inequalities such as $\mathbf{x} \leq P$ or $\mathbf{x} \leq \mathbf{y}$ should be understood componentwise. Write $(a; q)$ and $(\mathbf{a}; q) := (a_1; a_2; q)$ for the greatest common divisor of the components and $\mathrm{lcm}(q_1, \ldots, q_k)$ for the least common multiple of $q_1, \ldots, q_k$. A sum over natural numbers starts at one, if not otherwise indicated and we use the following abbreviations in our summations.

$$\sum_{(a;q)=1} := \sum_{\substack{a=1 \\ (a;q)=1}}^{q} \quad \text{and} \quad \sum_{(\mathbf{a};q)=1} := \sum_{a_1=1}^{q} \sum_{\substack{a_2=1 \\ (\mathbf{a};q)=1}}^{q}$$

The symbol $\mathbb{T}$ is used to refer to the 'circle' $\mathbb{R}/\mathbb{Z}$ with the circle norm $\|\alpha\| := \min\{|\alpha - z| : z \in \mathbb{Z}\}$, the distance of $\alpha \in \mathbb{R}$ to the nearest integer. Let $f : \mathbb{T}^d \to \mathbb{C}$ be a function on $\mathbb{T}^d$ and $g : B \to \mathbb{C}$ a function with support inside a unit box $B = \prod_{i=1}^{d}[y_i, y_i + 1] \subset \mathbb{R}^d$. The expression

$$\int_{\mathbb{T}^d} f(\boldsymbol{\alpha})g(\boldsymbol{\alpha}) \, d\boldsymbol{\alpha}$$

should be understood as the integral over B. We take the notational freedom to identify $\mathbb{T}$ with different specific intervals of length one, such as $[0, 1]$ or $[-1/2, 1/2]$, for example. This is well defined due to the one-periodicity of f.

The parameter $N \in \mathbb{N}$, governing the size of the variables x_i in (1.1), is the most important parameter in this paper and should be thought of as large. The parameter $Q \in \mathbb{N}$ is used for the major-minor-arc decomposition and we assume throughout the paper that $64\,Q^{52} \leq N$. It will be set to a small power of N eventually.

Now we define the main objects of our study, which are certain quadratic exponential sums associated to the system (1.1). For a function $g : \mathbb{N} \to \mathbb{C}$ and $\mathcal{A} \subset \{1, 2, \ldots, N\}$ we define

$$(2.1) \qquad V_g(\boldsymbol{\alpha}) = \sum_{n \leq N} g(n) e(\alpha_2 n^2 + \alpha_1 n) \ \text{ and } \ V_{\mathcal{A}}(\boldsymbol{\alpha}) = \sum_{n \in \mathcal{A}} e(\alpha_2 n^2 + \alpha_1 n)$$

and write $V(\boldsymbol{\alpha})$ for the sum without the weight function g. The local versions

$$(2.2) \qquad v(\boldsymbol{\alpha}) = \int_0^N e(\alpha_2 t^2 + \alpha_1 t)\, dt, \qquad V(q, \mathbf{a}) = \sum_{r=1}^q e_q(a_2 r^2 + a_1 r).$$

are needed in the argument as well as the linear exponential sum $L(\boldsymbol{\alpha}) := L_{3N}(\alpha_1) L_{3N^2}(\alpha_2)$, where L_M is the usual one-dimensional version

$$(2.3) \qquad\qquad\qquad L_M(\alpha) = \sum_{n \leq M} e(\alpha n).$$

As is common in the circle method approach, the sums $V_{\mathcal{A}}$ are used to encode the number of solutions to system (1.1) as an integral (3.2). To evaluate it, we need to bound L^p-means of the exponential sums V_g for arbitrary $|g| \leq 1$. Due to the presence of arbitrary coefficients in (2.1), Weyl-differencing techniques are not available and Parseval's identity works only for $p \geq 8$. This is the main reason why the result of Smith [23] gives Theorem 1.1 only for $s \geq 9$. Here we use methods inspired by 'restriction theory' instead to prove the following result on L^p-estimates of these exponential sums, which allows us to reduce the number of variables in our analysis down to $s \geq 7$.

Theorem 2.1. *Let $V_g(\boldsymbol{\alpha})$ be defined as in (2.1) for a function g with $|g(n)| \leq 1$. Then for $p > 6$, we have*

$$\int_{\mathbb{T}^2} |V_g(\boldsymbol{\alpha})|^p \, d\boldsymbol{\alpha} \ll_p N^{p-3}.$$

Theorem 2.1 follows from a more general result of Bourgain [4, Prop. 3.114]. We give here a new proof, which differs from that of Bourgain in some technical and conceptual points and has strong parallels with the approach in [12], where similar estimates played a major role in the proof of Roth's theorem in the primes. In our case we deduce it from Theorem 4.1, which is a general theorem for handling L^p-means of exponential sums.

While Theorem 2.1 is a corollary of a known result, the proof methods below also give variants of Theorem 2.1, which are not covered by Bourgain's work. Similarly, Theorem 4.1 seems to be a new result and might prove useful in similar situations.

The main ingredient in the proof of Theorem 2.1 is a decomposition of the representation function

$$(2.4) \qquad R(\mathbf{m}) := \#\{(y_1, y_2, y_3) \leq N : m_1 = y_1 + y_2 + y_3, m_2 = y_1^2 + y_2^2 + y_3^2\},$$

where $\mathbf{m} \in \mathbb{N}^2, \mathbf{y} \in \mathbb{N}^3$ and $\#$ denotes the number of elements in the set. This decomposition will be achieved by using ideas from the circle method and correspond to a major-minor-arc

decomposition of the corresponding exponential sum. The main work goes into obtaining good control on the arithmetical and analytical properties of the different parts, which appear in the decomposition of R.

For this task we introduce the triangular function

$$(2.5) \qquad \chi(x) = \max\{1 - |x|, 0\}$$

and a 'continuous indicator function' of $[-P, P]$ with support $[-2P, 2P]$ by

$$\psi_P(\alpha) = 2\chi(\alpha/(2P)) - \chi(\alpha/P).$$

The two-dimensional version that we use is

$$(2.6) \qquad \psi(\boldsymbol{\alpha}) = \psi_{Q/N}(\alpha_1) \cdot \psi_{Q^2/N^2}(\alpha_2),$$

where Q and N are the parameters introduced before.

3. Proof of Theorem 1.1

For a set $\mathcal{A} \subset \{1, 2, \ldots, N\}$ write $\mathbf{1}_\mathcal{A}$ for the indicator function of $\mathcal{A}$ and $\delta = N^{-1}|\mathcal{A}|$ for the density of $\mathcal{A}$. We define the balanced function f by

$$(3.1) \qquad f(n) := \mathbf{1}_\mathcal{A}(n) - \delta.$$

Write $Z(N)$ for the number of solutions to (1.1) with $x_i \in \{1, 2, \ldots, N\}$ and $Z_\mathcal{A}(N)$ for the corresponding quantity with $x_i \in \mathcal{A}$.

The proof of Theorem 1.1 uses the density increment strategy of Roth [20] and is straightforward, once we have the necessary ingredients. Let us assume Theorem 2.1 and the estimate $Z(N) \gg N^{s-3}$ from Proposition 7.1 to give a proof of Theorem 1.1.

Proof of Theorem 1.1. The number of solutions $Z_\mathcal{A}(N)$ of system (1.1) with variables $x_i \in \mathcal{A}$ can be written as the integral

$$(3.2) \qquad Z_\mathcal{A}(N) = \int_{\mathbb{T}^2} \prod_{i=1}^{s} V_\mathcal{A}(\lambda_i \boldsymbol{\alpha}) \, d\boldsymbol{\alpha}.$$

Use the decomposition $V_\mathcal{A} = \delta V + V_f$ and expand the product above. We are led to a decomposition into a sum of the main term

$$\delta^s Z(N) = \delta^s \int_{\mathbb{T}^2} \prod_{i=1}^{s} V(\lambda_i \boldsymbol{\alpha}) \, d\boldsymbol{\alpha}$$

and $2^s - 1$ 'error terms' of the form

$$\pm \int_{\mathbb{T}^2} V_f(\lambda_{i_s} \boldsymbol{\alpha}) \prod_{j=1}^{s-1} V_{g_j}(\lambda_{i_j} \boldsymbol{\alpha}) \, d\boldsymbol{\alpha},$$

where $g_j = \delta$ or $g_j = f$ and $\lambda_{i_1}, \ldots, \lambda_{i_s}$ is a permutation of $\{\lambda_1, \ldots, \lambda_s\}$. By Hölder's inequality, each error term is bounded up to a constant by

$$(3.3) \qquad H_g = \sup_{\boldsymbol{\alpha}} |V_f(\boldsymbol{\alpha})|^{1/2} \int_{\mathbb{T}^2} |V_g(\boldsymbol{\alpha})|^{s-1/2} \, d\boldsymbol{\alpha}$$

for some function $g \in \{\delta, f\}$. The coefficients ($\lambda_i \neq 0$) disappeared by a change of variables and the 1-periodicity of the exponential sums. By Theorem 2.1 and the trivial bound $|V_g(\boldsymbol{\alpha})| \leq 2\delta N$ the integral in formula (3.3) is $O(\delta^{s-7} N^{s-1/2-3})$ and hence

$$H_g \ll \delta^{s-7} N^{s-1/2-3} \sup_{\boldsymbol{\alpha}} |V_f(\boldsymbol{\alpha})|^{1/2}.$$

Proposition 7.1 provides a lower bound $Z(N) \gg N^{s-3}$ for the main term and Hölder's inequality with Lemma 5.1 give an upper bound $Z_{\mathcal{A}}(N) \ll \delta^{s-7} N^{s-4} \log N$ to the number of trivial solutions to the system (1.1). (The number of trivial solutions is bounded by $\binom{s}{2}$ times the number of solutions to a system with $s - 1 \geq 6$ variables.) Combining the inequalities for $Z(N), Z_{\mathcal{A}}(N), H_g$ and plugging them into $\delta^s Z(N) \leq 2^s H_g + Z_{\mathcal{A}}(N)$, we end up with

$$\delta^s N^{s-3} \ll \delta^{s-7} N^{s-1/2-3} \sup_{\boldsymbol{\alpha}} |V_f(\boldsymbol{\alpha})|^{1/2} + \delta^{s-7} N^{s-4} \log N.$$

A short calculation gives the lower bound

$$\sup_{\boldsymbol{\alpha}} |V_f(\boldsymbol{\alpha})| \gg \delta^{14} N$$

as long as $N \geq D/\delta^8$ for some $D > 1$ (depending on the coefficients λ_i). This large Fourier coefficient can be used with Lemma B.1 to find a progression P of length at least $\delta^{28} N^{1/16}$, such that $\mathcal{A}$ has density at least $\delta + d\delta^{14}$ on P, where $d > 0$ is an absolute constant. Due to the translation and dilation invariance of the system (1.1), we end up with the same problem on a subprogression, but with a slightly higher density.

Since the density is bounded by one, this procedure cannot last more than $d^{-1}\delta^{-14}$ steps before reaching a contradiction. This means that at some stage we have a non-trivial solution or the size of our progression is getting smaller than D/δ^8. The first option is not available by assumption. Therefore, we have

$$\delta^{30} N^{(1/16)^{d^{-1}\delta^{-14}}} \leq D/\delta^8,$$

where D depends only on the coefficients of the system. Rearranging for δ we can deduce that $\delta \ll 1/\log\log^c(N)$ with $c = 1/15$, for example. □

Remark 3.1. *A more careful analysis of the L^p-estimates below can yield a better value for c. We haven't optimized because our bound on $|\mathcal{A}|$ is far away from the expected order of magnitude anyway.*

4. A GENERAL THEOREM FOR L^p-ESTIMATES

Theorem 4.1 below and its proof are strongly connected to 'restriction theory', a subfield of harmonic analysis studying the behaviour of the Fourier transform under restriction to a given subset. Recent years have seen several applications of ideas from restriction theory to number theory, which has led to a better understanding of prime numbers.

The idea for the proof of Theorem 4.1 is inspired by the papers of Green [12] and Green and Tao [13], where the connection to restriction estimates can be seen more explicitly. The new ingredient in our proof is the use of recursion, which allows us to work under slightly weaker assumptions on the involved functions. Therefore, our result applies to a different range of functions than Proposition 4.2 in [13].

For $\mathbf{N} = (N_1, \ldots, N_d) \in \mathbb{N}^d$ define $[1, \mathbf{N}] := \prod_{i=1}^d \{n \in \mathbb{N} : n \leq N_i\}$. Let $\omega : [1, \mathbf{N}] \to [0, \infty)$ be a positive real function and $f : [1, \mathbf{N}] \to \mathbb{C}$ be a 'random' weight function. We study the exponential sums

$$W(\boldsymbol{\alpha}) = \sum_{\mathbf{n} \leq \mathbf{N}} \omega(\mathbf{n}) e(\boldsymbol{\alpha} \cdot \mathbf{n}) \quad \text{and} \quad W_f(\boldsymbol{\alpha}) = \sum_{\mathbf{n} \leq \mathbf{N}} f(\mathbf{n}) \omega(\mathbf{n}) e(\boldsymbol{\alpha} \cdot \mathbf{n}).$$

Consider a general decomposition of ω and $W(\boldsymbol{\alpha})$ into

$$W(\boldsymbol{\alpha}) = \sum_{j \in J} W_j(\boldsymbol{\alpha}) \quad \text{and} \quad \omega(\mathbf{n}) = \sum_{j \in J} \omega_j(\mathbf{n}),$$

where J is an index set and W_j is the exponential sum for ω_j. Define the L^p-norms by

$$\|\omega\|_p := \Big(\sum_{\mathbf{n} \le \mathbf{N}} |\omega(\mathbf{n})|^p \Big)^{1/p} \text{ and } \|W\|_p := \Big(\int_{\mathbb{T}^d} |W(\boldsymbol{\alpha})|^p \, d\boldsymbol{\alpha} \Big)^{1/p}.$$

The typical function ω, of interest for us, obeys $\|\omega\|_1 = O(N)$ but $\|\omega\|_2^2 \ne O(N)$. One-dimensional examples are the function counting the number of representations as sum of two squares and the von Mangoldt function.

Theorem 4.1. *For $p > 2$ and $\mathbf{N} \in \mathbb{N}^d$ we have the estimate*

$$\|W_f\|_p \le \Big(\sum_{\mathbf{n} \le \mathbf{N}} |f(\mathbf{n})|^2 \omega(\mathbf{n}) \Big)^{1/2} \Big(\sum_{j \in J} \|W_j\|_p^{(p-2)/p} \|\omega_j\|_{2p/(p-2)}^{2/p} \Big)^{1/2}.$$

Remark 4.2. *We reduced the estimation of an exponential sum integral with an arbitrary weight function f to one expression which involves a weighted L^2-norm of f, and another one with a decomposition of ω. The first factor is easily estimated in our context and the second factor can be written as*

$$\Big(\sum_{j \in J} \Big(\int_{\mathbb{T}^d} |W_j(\boldsymbol{\alpha})|^p \, d\boldsymbol{\alpha} \sum_{\mathbf{n} \le \mathbf{N}} |\omega_j(\mathbf{n})|^{2p/(p-2)} \Big)^{(p-2)/p^2} \Big)^{1/2},$$

where it is easier to see what kind of expressions we need to estimate.

Proof. Write as an abbreviation

$$(4.1) \qquad H_p := \int_{\mathbb{T}^d} |W_f(\boldsymbol{\alpha})|^p \, d\boldsymbol{\alpha}$$

for the integral which has to be estimated. Decompose $|W_f(\boldsymbol{\alpha})|^p = W_f(\boldsymbol{\alpha})\overline{h(\boldsymbol{\alpha})}$ where $h(\boldsymbol{\alpha}) = W_f(\boldsymbol{\alpha})|W_f(\boldsymbol{\alpha})|^{p-2}$ and observe the identity

$$(4.2) \qquad H_p = \int_{\mathbb{T}^d} |h(\boldsymbol{\alpha})|^{p'} \, d\boldsymbol{\alpha},$$

where $p' = p/(p-1)$ is the dual exponent of p. We expand the integral (4.1) and apply the Cauchy-Schwarz-inequality to obtain

$$H_p = \int_{\mathbb{T}^d} |W_f(\boldsymbol{\alpha})|^p \, d\boldsymbol{\alpha} = \sum_{\mathbf{n} \le \mathbf{N}} f(\mathbf{n})\omega(\mathbf{n}) \int_{\mathbb{T}^d} \overline{h(\boldsymbol{\alpha})} e(\boldsymbol{\alpha} \cdot \mathbf{n}) \, d\boldsymbol{\alpha}$$

$$\le \Big(\sum_{\mathbf{n} \le \mathbf{N}} |f(\mathbf{n})|^2 \omega(\mathbf{n}) \Big)^{1/2} \Big(\sum_{\mathbf{n} \le \mathbf{N}} \omega(\mathbf{n}) \Big| \int_{\mathbb{T}^d} \overline{h(\boldsymbol{\alpha})} e(\boldsymbol{\alpha} \cdot \mathbf{n}) \, d\boldsymbol{\alpha} \Big|^2 \Big)^{1/2}.$$

Write F as an abbreviation for the first factor on the right hand side, which is already in the form we want it to be. By opening the square in the second factor and changing the order of integration and summation, we see that

$$\sum_{\mathbf{n} \le \mathbf{N}} \omega(\mathbf{n}) \Big| \int_{\mathbb{T}^d} \overline{h(\boldsymbol{\alpha})} e(\boldsymbol{\alpha} \cdot \mathbf{n}) \, d\boldsymbol{\alpha} \Big|^2 = \int_{\mathbb{T}^d} \int_{\mathbb{T}^d} \overline{h(\boldsymbol{\alpha})} h(\boldsymbol{\beta}) W(\boldsymbol{\alpha} - \boldsymbol{\beta}) \, d\boldsymbol{\beta} d\boldsymbol{\alpha}.$$

This expression is bounded with Hölder's inequality by

$$\Big(\int_{\mathbb{T}^d} |h(\boldsymbol{\alpha})|^{p'} \, d\boldsymbol{\alpha} \Big)^{1/p'} \Big(\int_{\mathbb{T}^d} \Big| \int_{\mathbb{T}^d} h(\boldsymbol{\beta}) W(\boldsymbol{\alpha} - \boldsymbol{\beta}) \, d\boldsymbol{\beta} \Big|^p \, d\boldsymbol{\alpha} \Big)^{1/p}.$$

By (4.2) we can write this as $H_p^{1/p'}\|W * h\|_p$ where the convolution $*$ is defined as usual. By using the previous formulae and rearranging, we have shown that

$$(4.3) \qquad\qquad\qquad H_p^{2-1/p'} \le F^2 \|W * h\|_p.$$

The decomposition into functions W_j and the triangle inequality imply

$$\|W * h\|_p \le \sum_{j \in J} \|W_j * h\|_p.$$

In the next step, we interpolate to obtain an estimate for the L^p-norms from L^∞- and L^2-estimates, so that

$$\|W_j * h\|_p^p \le \|W_j * h\|_\infty^{p-2} \|W_j * h\|_2^2.$$

This estimate can be seen more easily by writing the left hand side as an integral. The L^∞- and L^2-norms are more accessible and are treated separately in what follows. For the L^∞-part we have by Hölder's inequality the estimate

$$\|W_j * h\|_\infty \le \|W_j\|_p \|h\|_{p'}.$$

For the L^2-norm we apply Parseval's identity followed by another application of Hölder's inequality and the Hausdorff-Young inequality, and hence deduce the upper bound

$$\|W_j * h\|_2 = \|\omega_j \cdot \widehat{h}\|_2 \le \|\omega_j\|_{2p/(p-2)} \|\widehat{h}\|_p \le \|\omega_j\|_{2p/(p-2)} \|h\|_{p'}.$$

Here $\widehat{h} : \mathbb{Z}^d \to \mathbb{C}$ denotes the Fourier transform of h on $\mathbb{T}^d$. Putting these estimates in (4.3) gives

$$H_p^{2-1/p'} \le F^2 \sum_{j \in J} \|W_j * h\|_\infty^{(p-2)/p} \|W_j * h\|_2^{2/p}$$

$$\le F^2 \sum_{j \in J} (\|W_j\|_p \|h\|_{p'})^{(p-2)/p} (\|h\|_{p'} \|\omega_j\|_{2p/(p-2)})^{2/p}$$

$$\le F^2 \|h\|_{p'} \sum_{j \in J} \|W_j\|_p^{(p-2)/p} \|\omega_j\|_{2p/(p-2)}^{2/p}.$$

Now we use (4.2) and $2 - 2/p' = 2/p$ to obtain

$$H_p^{1/p} \le F \Big(\sum_{j \in J} \|W_j\|_p^{(p-2)/p} \|\omega_j\|_{2p/(p-2)}^{2/p} \Big)^{1/2}.$$

$\square$

5. Lemmata

More Notation: In this section we make use of indicator functions. For a set $\mathcal{B}$ we write $\mathbf{1}_{\mathcal{B}}$ for the function that is one on $\mathcal{B}$ and zero otherwise. When Φ is a mathematical statement, then we write $\mathbf{1}_\Phi$ for the indicator function of the set, where Φ is true.

Before we start with the technical core of this work in the next section, we collect and prove a few useful lemmata. The reader might want to skip this section on the first reading and proceed directly to Section 6.

The first result summarizes two estimates for the function R.

Lemma 5.1. *For $R(\mathbf{m})$ as in (2.4) we have*

$$\sum_{\mathbf{m} \le 3(N, N^2)} R(\mathbf{m})^2 \ll N^3 \log N \quad and \quad |R(\mathbf{m})| \ll_\epsilon N^\epsilon.$$

Proof. Rogovskaya [19] showed the asymptotic formula

$$\sum_{\mathbf{m} \leq 3(N, N^2)} R(\mathbf{m})^2 = 18/\pi^2 N^3 \log N + O(N^3).$$

But the estimate may be derived from the elementary Lemma 11.2.1 in [17] as well.

For the second estimate, Lemma 11.1.1 in [17] bounds $R(\mathbf{m})$ by nine times the number of divisors of $3m_2 - m_1^2$. By the standard divisor bound, we obtain the second formula as long as $3m_2 \neq m_1^2$. In the case $m_1^2 = 3m_2$ we can show by elementary calculations that we have $y_1 = y_2 = y_3$ in (2.4). This gives us at most one solution for such a pair (m_1, m_2). □

The next lemma gives us control on the Fourier coefficients of $\psi(\boldsymbol{\alpha})v(\boldsymbol{\alpha})^3$ (see (2.2) and (2.6)) and is a crucial tool to estimate the 'analytic part' in the decomposition of $R(\mathbf{m})$.

Lemma 5.2. *For* $\mathbf{m} \in \mathbb{N}^2$ *and* $\mathbb{T}^2 = [-1/2, 1/2]^2$ *we have*

$$\int_{\mathbb{T}^2} \psi(\boldsymbol{\alpha})v(\boldsymbol{\alpha})^3 e(-\boldsymbol{\alpha} \cdot \mathbf{m}) \, d\boldsymbol{\alpha} \ll 1.$$

Proof. Recall the definition $v(\boldsymbol{\alpha}) = \int_0^N e(\alpha_2 t^2 + \alpha_1 t) \, dt$ and the decomposition $\psi(\boldsymbol{\alpha}) = \psi_{Q/N}(\alpha_1) \cdot \psi_{Q^2/N^2}(\alpha_2)$. By inserting this into the integral in Lemma 5.2 and changing the order of integration, noting that $\psi(\boldsymbol{\alpha})$ has finite support, we obtain

$$\int_{[0,N]^3} \prod_{i=1}^{2} \int_{\mathbb{R}} \psi_{Q^i/N^i}(\alpha_i)e(-\alpha_i(m_i - K_i(\mathbf{t}))) \, d\alpha_i \, d\mathbf{t},$$

where we used $K_i(\mathbf{t}) = t_1^i + t_2^i + t_3^i$ as an abbreviation. The inner integral is a Fourier transform and our expression can be written as

$$N^3 Q^{-3} \int_{[0,N]^3} \prod_{i=1}^{2} \widehat{\psi_1}\Big(Q^i N^{-i}(m_i - K_i(\mathbf{t}))\Big) \, d\mathbf{t},$$

where $\psi_1 = \psi_P$ with $P = 1$ and $\widehat{\psi_1}$ its Fourier transform. Change the variables to $x_i = Qt_iN^{-1}$ and rename $y_i = Q^im_iN^{-i}$ to get

(5.1) $$\int_{[0,Q]^3} \widehat{\psi_1}(y_1 - K_1(\mathbf{x}))\widehat{\psi_1}(y_2 - K_2(\mathbf{x})) \, d\mathbf{x}.$$

The dependence on N disappeared completely and we are left with the task to bound this integral independent of Q and $y_i \in \mathbb{R}$. We use a Riemann sum approach. Consider the level sets

$$B_l^i := \{\mathbf{x} \in \mathbb{R}^3 : |x_1^i + x_2^i + x_3^i - l| \leq 1/2\}.$$

Then the integral (5.1) above is bounded by the sum

$$\sum_{l_1=0}^{\infty} \sum_{l_2=0}^{\infty} \mu(B_{l_1}^1 \cap B_{l_2}^2) \sup_{\substack{|z_1-l_1|\leq 1/2 \\ |z_2-l_2|\leq 1/2}} |\widehat{\psi_1}(y_1 - z_1)||\widehat{\psi_1}(y_2 - z_2)|,$$

where μ is the Lebesgue measure. The set $B_{l_1}^1$ is a 'plane' with thickness less than two and $B_{l_2}^2$ is a spherical shell centered at the origin with 'radius' $l_2^{1/2}$ and thickness $\sqrt{l_2 + 1} - \sqrt{l_2 - 1} \leq 2l_2^{-1/2}$ for $l_2 \geq 1$. The volume of the intersection of these two objects is maximal for $l_1 = 0$. It is a volume around a circle with radius $O(l_2^{1/2})$. The width in the radial direction is

$O(l_2^{-1/2})$ and bounded by absolute constants otherwise. Therefore, the volume $B_{l_1}^1 \cap B_{l_2}^2$ is bounded by a constant independent of l_2 or l_1. We are left with the product of two sums

$$\Big(\sum_{l_1=0}^{\infty} \sup_{|z_1-l_1|\leq 1/2} |\widehat{\psi_1}(y_1 - z_1)| \Big) \Big(\sum_{l_2=0}^{\infty} \sup_{|z_2-l_2|\leq 1/2} |\widehat{\psi_1}(y_2 - z_2)| \Big).$$

The Fourier transform of $\psi_1 = 2\chi(\alpha/2) - \chi(\alpha)$ can be understood by using the well known identity $\widehat{\chi}(x) = \frac{\sin^2(\pi x)}{(\pi x)^2}$. The sums are easily seen to be convergent with an upper bound independent of the y_i. $\qquad\square$

The idea for the next lemma is borrowed from [13] and is the arithmetic counterpart to Lemma 5.2.

Lemma 5.3. *Let $g : \mathbb{N}^2 \to \mathbb{C}$ be a function with $|g(a,q)| \leq Cq^{-1}$ for some $C \geq 1$. Consider the function $\beta : \mathbb{N} \to \mathbb{C}$, given by*

$$\beta(m) = \sum_{q\leq X} \sum_{a\leq q} g(a,q) e_q(-am).$$

Then for $k \in \mathbb{N}$ and $X^{4k} \leq M$ one has

$$\sum_{m\leq M} |\beta(m)|^{2k} \ll_{\epsilon,k} MX^{\epsilon}.$$

Proof. First, we insert the definition of β and expand to obtain

$$(5.2) \qquad \sum_{m\leq M} |\beta(m)|^{2k} = \sum_{q_1,\ldots,q_{2k}\leq X} \sum_{a_1,\ldots,a_{2k}\leq q} \Big(\prod_{j\leq 2k} g_j(a_j, q_j) \Big) \sum_{m\leq M} e\Big(m\sum_{i\leq 2k} \epsilon_i a_i/q_i\Big),$$

where $g_j = g$ and $\epsilon_i = -1$ for $i, j \leq k$, and $g_j = \overline{g}$ and $\epsilon_i = 1$ for $k < i, j \leq 2k$. Write Φ for the condition

$$\Big(\sum_{i\leq 2k} \epsilon_i a_i/q_i \Big) \in \mathbb{Z}.$$

Evaluating the innermost sum in (5.2), we get the expression $M\mathbf{1}_\Phi + O(q_1 \cdots q_{2k})$. Together with the estimate $|g(a,q)| \leq Cq^{-1}$ this gives

$$\sum_{m\leq M} |\beta(m)|^{2k} \ll \sum_{q_1,\ldots,q_{2k}\leq X} \sum_{a_1,\ldots,a_{2k}\leq q} \frac{M}{q_1 \cdots q_{2k}} \mathbf{1}_\Phi + O(X^{4k}).$$

The function $\mathbf{1}_\Phi$ can now be written as exponential sum again and we gain the original expression

$$\sum_{m\leq M} |\beta(m)|^{2k} \ll \sum_{m\leq M} \Big| \sum_{q\leq X} q^{-1} \sum_{a\leq q} e_q(-am) \Big|^{2k} + O(X^{4k}),$$

but now with $g(a,q)$ replaced by q^{-1}. The exponential sum inside is 0, except when q divides m. In that case it gives q and we are left with the task to estimate

$$\sum_{m\leq M} \tau_X(m)^{2k},$$

where $\tau_X(m) = \sum_{q \le X} \mathbf{1}_{q|m}$ is a restricted divisor function. By expanding again, we have

$$\sum_{m \le M} \tau_X(m)^{2k} = \sum_{m \le M} \Big(\sum_{q \le X} \mathbf{1}_{q|m} \Big)^{2k} = \sum_{q_1,\dots,q_{2k} \le X} \sum_{m \le M} \mathbf{1}_{q_1|m,\dots,q_{2k}|m}$$

$$\le \sum_{q_1,\dots,q_{2k} \le X} \frac{M}{\operatorname{lcm}(q_1,\dots,q_{2k})} \le M \sum_{l \le X^{2k}} \frac{\tau(l)^{2k}}{l}.$$

The last inequality follows from the fact that the equation $l = \operatorname{lcm}(q_1,\dots,q_{2k})$ has at most $\tau(l)^{2k}$ solutions where τ is the usual divisor function. Using the standard estimate $\tau(l) \ll_\eta l^\eta$ in the range $l \le X^{2k}$ and choosing $\eta = \epsilon/5k^2$, we get

$$\sum_{l \le X^{2k}} \tau(l)^{2k} l^{-1} \ll_{k,\epsilon} ((X^{2k})^\eta)^{2k} \sum_{l \le X^{2k}} l^{-1} \ll_{k,\epsilon} X^\epsilon.$$

$\square$

The slightly technical Lemma 5.4 is needed to transform a two-dimensional exponential sum into a one-dimensional version.

Lemma 5.4. *For fixed $q \in \mathbb{N}$ and $\mathbf{m} \in \mathbb{N}^2$ we can write*

(5.3) $$\sum_{(\mathbf{a};q)=1} V(q,\mathbf{a})^3 e_q(-\mathbf{a} \cdot \mathbf{m}) = q \sum_{(a;q)=1} G_{m_1}(q,a) \, e_q(-am_2),$$

where

$$G_{m_1}(q,a) = \sum_{r_1,r_2 \le q} e_q(aF_2(r_1,r_2) + aF_{1,m_1}(r_1,r_2))$$

with $F_2(r_1,r_2) = 2r_1^2 + 2r_1 r_2 + 2r_2^2$ and $F_{1,m_1}(r_1,r_2) = -2m_1(r_1 + r_2) + m_1^2$.

Remark 5.5. *The exact form of the polynomial above is not very important. The only fact we need is that F_2 is a non-degenerate quadratic form.*

Proof. Use the well known identity $\mathbf{1}_{t=1} = \sum_{d|t} \mu(d)$ to rewrite the condition $(\mathbf{a};q) = 1$ on the left hand side $\mathcal{L}$ of equation (5.3). We get

$$\mathcal{L} = \sum_{(\mathbf{a};q)=1} V(q,\mathbf{a})^3 e_q(-\mathbf{a} \cdot \mathbf{m}) = \sum_{\mathbf{a} \le q} \sum_{d|(\mathbf{a};q)} \mu(d) V(q,\mathbf{a})^3 e_q(-\mathbf{a} \cdot \mathbf{m}).$$

Next we observe that $d|(\mathbf{a};q)$ if and only if $d|q$ and $d|\mathbf{a}$. Rearranging gives

$$\mathcal{L} = \sum_{d|q} \mu(d) \sum_{d|\mathbf{a}} V(q,\mathbf{a})^3 e_q(-\mathbf{a} \cdot \mathbf{m})$$

Note that the first sum is over all d dividing q and the second sum runs over all $\mathbf{a} \le q$ with components divisible by d. Now we look closer at the inner sum and insert the definition $V(q,\mathbf{a}) = \sum_{r=1}^q e_q(a_2 r^2 + a_1 r)$. Using the abbreviation $K_i(\mathbf{r}) = r_1^i + r_2^i + r_3^i$, we obtain the identity

$$\mathcal{L} = \sum_{d|q} \mu(d) \sum_{\mathbf{r} \le q} \sum_{d|a_2} e_q(a_2(K_2(\mathbf{r}) - m_2)) \sum_{d|a_1} e_q(a_1(K_1(\mathbf{r}) - m_1)).$$

An evaluation of the two exponential sums gives

$$\mathcal{L} = \sum_{d|q} \mu(d) q^2 d^{-2} \sum_{\mathbf{r} \le q} \mathbf{1}_{\mathbf{r},\mathbf{m},q/d},$$

where $\mathbf{1}_{\mathbf{r},\mathbf{m},q/d}$ is indicator function with conditions

$$K_2(\mathbf{r}) - m_2 \equiv 0 \pmod{q/d} \quad \text{and} \quad K_1(\mathbf{r}) - m_1 \equiv 0 \pmod{q/d}.$$

Recalling the definitions of $K_i(\mathbf{r})$, we can insert the second congruence into the first. We arrive at the relation

$$(5.4) \qquad\qquad r_1^2 + r_2^2 + (m_1 - r_1 - r_2)^2 - m_2 \equiv 0 \pmod{q/d}.$$

Since r_3 disappeared from the first condition, we can perform the sum over r_3, which reduces to the evaluation

$$\sum_{r_3 \le q} \mathbf{1}_{[K_1(\mathbf{r}) - m_1 \equiv 0 \pmod{q/d}]} = d.$$

Therefore, by rearranging (5.4), we get

$$\mathcal{L} = q \sum_{d|q} \mu(d) q d^{-1} \sum_{r_1, r_2 \le q} \mathbf{1}_{[H(r_1, r_2, m_1, m_2) \equiv 0 \pmod{q/d}]},$$

where $H(r_1, r_2, m_1, m_2) = F_2(r_1, r_2) + F_{1,m_1}(r_1, r_2) - m_2$. Then we can rewrite the indicator function as an exponential sum and get

$$\mathcal{L} = q \sum_{d|q} \mu(d) \sum_{r_1, r_2 \le q} \sum_{d|a} e_q(a H(r_1, r_2, m_1, m_2)).$$

Changing the order of the sums and using the identity with the Möbius function again gives the right hand side of the equation in Lemma 5.4. $\qquad\qquad\square$

6. Decomposition of R and proof of Theorem 2.1

In this section we perform a decomposition of $R(\mathbf{m})$ and give estimates for its analytic and arithmetic parts in Propositions 6.2 and 6.3. In combining these propositions with Theorem 4.1, we are able to deduce Theorem 2.1.

To motivate the technical material below, let us first look at the structure of the proof of Theorem 2.1.

Proof of Theorem 2.1. We apply Theorem 4.1 with $\omega(\mathbf{m}) = R(\mathbf{m})$. Let $\mathbf{N} = 3(N, N^2)$ and define $W_h(\boldsymbol{\alpha})$ by

$$V_g(\boldsymbol{\alpha})^3 = \sum_{\mathbf{m} \le 3(N, N^2)} h(\mathbf{m}) R(\mathbf{m}) e(\boldsymbol{\alpha} \cdot \mathbf{m})$$

where $|h(\mathbf{m})| \le 1$ is chosen in such a way that

$$h(\mathbf{m}) R(\mathbf{m}) = \sum_{\substack{x_1, x_2, x_3 \le N \\ m_1 = x_1 + x_2 + x_3 \\ m_2 = x_1^2 + x_2^2 + x_3^2}} g(x_1) g(x_2) g(x_3).$$

Then we have

$$\sum_{\mathbf{m} \le 3(N, N^2)} |h(\mathbf{m})|^2 R(\mathbf{m}) \le \sum_{\mathbf{m} \le 3(N, N^2)} R(\mathbf{m}) = N^3$$

for the first term in Theorem 4.1.

Let $J = \{1, 2, 4, \ldots, 2^{D-1}, 2^D\}$ with $D \approx \log_2 Q$. To estimate the second term, we need a suitable decomposition of $R(\mathbf{m})$. Later in this section we construct the decomposition

$$R(\mathbf{m}) = \sum_{Y \in J} R_Y(\mathbf{m}) + R'(\mathbf{m})$$

and for the corresponding exponential sum $W(\boldsymbol{\alpha}) = V(\boldsymbol{\alpha})^3$ similarly

$$W(\boldsymbol{\alpha}) = \sum_{Y \in J} W_Y(\boldsymbol{\alpha}) + W'(\boldsymbol{\alpha}).$$

Write J' for the index set $J \cup \{0\}$ and write $W_0 = W'$ and $R_0 = R'$ to simplify notation. Since $p > 6$, we have $b = p/3 > 2$ and Theorem 4.1 gives us the estimate

$$\int_{\mathbb{T}^2} |V_g(\boldsymbol{\alpha})|^p \, d\boldsymbol{\alpha} = \int_{\mathbb{T}^2} |W_h(\boldsymbol{\alpha})|^b \, d\boldsymbol{\alpha}$$

$$\leq N^{3b/2} \left(\sum_{Y \in J'} \left(\int_{\mathbb{T}^2} |W_Y(\boldsymbol{\alpha})|^b \, d\boldsymbol{\alpha} \sum_{\mathbf{n} \leq \mathbf{N}} |R_Y(\mathbf{n})|^{2b/(b-2)} \right)^{(b-2)/b^2} \right)^{b/2}.$$

The necessary moment estimates to handle this expression are given by Proposition 6.2 and Proposition 6.3 below. (The exponent $2b/(b-2)$ of R_Y might not be of the form $2k$ with $k \in \mathbb{N}$ as in Proposition 6.3, but it is easily seen by Hölder's inequality to be applicable nevertheless if we choose $Q^{4b/(b-2)+1} \leq N$.) We use Proposition 6.2 and the estimate

$$\int_{\mathbb{T}^2} |W_Y(\boldsymbol{\alpha})|^b \, d\boldsymbol{\alpha} \ll \sup_{\boldsymbol{\alpha} \in \mathbb{T}^2} |W_Y(\boldsymbol{\alpha})|^{b-2} \int_{\mathbb{T}^2} |W_Y(\boldsymbol{\alpha})|^2 \, d\boldsymbol{\alpha}$$

to bound the integral over W_Y. Summing over Y and singling out the term with $Y = 0$, we get the upper bound

$$\ll_{b,\epsilon} N^{3b/2} \left(\sum_{i=0}^{D} \left(2^{(-3(b-2)/2+\epsilon)i} N^{3b} \right)^{(b-2)/b^2} + \left(Q^{2-b} N^{3b+\epsilon} \right)^{(b-2)/b^2} \right)^{b/2},$$

where we already absorbed the logarithms into the N^ϵ term. For $\epsilon = \epsilon(b)$ small enough, the sum over i is convergent and if Q is a small power of N, depending on $b = p/3$, another short calculation leaves us with the result

$$\int_{\mathbb{T}^2} |V_g(\boldsymbol{\alpha})|^p \, d\boldsymbol{\alpha} \ll_b N^{3b-3} \ll_p N^{p-3}.$$

$\square$

To fill in the gaps in the proof of Theorem 2.1, we need to construct a suitable decomposition of $R(\mathbf{m})$. We start with an auxiliary function $U_Y(\boldsymbol{\alpha})$, that is motivated by Lemma A.2. Use the cutoff-function ψ to restrict the major arc approximation from Lemma A.2 to a $(Q/N, Q^2/N^2)$-neighbourhood of $\mathbf{a}/q$. Define for $Y \leq 2Q$

(6.1) $$U_Y(\boldsymbol{\alpha}) := \sum_{Y \leq q < 2Y} q^{-3} \sum_{(\mathbf{a};q)=1} V(q, \mathbf{a})^3 v(\boldsymbol{\alpha} - \mathbf{a}/q)^3 \psi(\boldsymbol{\alpha} - \mathbf{a}/q)$$

and consider $U_Y(\boldsymbol{\alpha})$ as a function on

$$\mathbb{T}^2 = [2QN^{-1}, 1 + 2QN^{-1}] \times [2Q^2N^{-2}, 1 + 2Q^2N^{-2}]$$

(see notational conventions). The functions $U_Y(\boldsymbol{\alpha})$ arise from the main term in the major arc approximation of $V(\boldsymbol{\alpha})$ for denominators $Y \leq q < 2Y$. It is a sum of disjointly supported pieces due to the restriction $64\,Q^{52} \leq N$. Take the corresponding arithmetical functions

(6.2) $$R_Y(\mathbf{m}) = \int_{\mathbb{T}^2} U_Y(\boldsymbol{\alpha}) e(-\boldsymbol{\alpha}\mathbf{m}) \, d\boldsymbol{\alpha},$$

but restrict to $1 \leq \mathbf{m} \leq 3(N, N^2)$. Set $R_Y(\mathbf{m}) = 0$ for other values of $\mathbf{m}$.

Let D be an integer between $\log_2 Q$ and $\log_2 Q + 1$, where $\log_2$ is the logarithm to base two and set $J = \{1, 2, 4, \ldots, 2^{D-1}, 2^D\}$. We write

$$R(\mathbf{m}) = \sum_{Y \in J} R_Y(\mathbf{m}) + R'(\mathbf{m}).$$

This is the decomposition used in the proof of Theorem 2.1 above.

Remark 6.1. *The part $R'(\mathbf{m})$ may be thought of as corresponding to the minor arcs, but it also contains the approximation error on the major arcs.*

Write $W(\boldsymbol{\alpha})$ for

$$V^3(\boldsymbol{\alpha}) = \sum_{\mathbf{m} \leq 3(N, N^2)} R(\mathbf{m}) e(\boldsymbol{\alpha} \cdot \mathbf{m}),$$

and define the corresponding exponential sums for $R_Y(\mathbf{m})$ as

$$W_Y(\boldsymbol{\alpha}) = \sum_{\mathbf{m} \leq 3(N, N^2)} R_Y(\mathbf{m}) e(\boldsymbol{\alpha} \cdot \mathbf{m}).$$

By inserting the definition of $R_Y(\mathbf{m})$ we see that

$$(6.3) \qquad W_Y(\boldsymbol{\alpha}) = \int_{\mathbb{T}^2} U_Y(\boldsymbol{\beta}) L(\boldsymbol{\alpha} - \boldsymbol{\beta}) \, d\boldsymbol{\beta},$$

where L is the linear exponential sum defined in Section 2. As in the case of $R(\mathbf{m})$, we obtain a decomposition

$$(6.4) \qquad W(\boldsymbol{\alpha}) = \sum_{Y \in J} W_Y(\boldsymbol{\alpha}) + W'(\boldsymbol{\alpha}),$$

where W' corresponds to R'. Now we are ready to give the first proposition that was needed for the proof of Theorem 2.1.

Proposition 6.2. *For $Y \leq 2Q$ we have the estimates*

$$\int_{\mathbb{T}^2} |W_Y(\boldsymbol{\alpha})|^2 \, d\boldsymbol{\alpha} \ll N^3, \qquad \int_{\mathbb{T}^2} |W'(\boldsymbol{\alpha})|^2 \, d\boldsymbol{\alpha} \ll N^3 \log^2 N,$$

$$\sup_{\boldsymbol{\alpha}} |W_Y(\boldsymbol{\alpha})| \ll Y^{-3/2} N^3, \qquad \sup_{\boldsymbol{\alpha}} |W'(\boldsymbol{\alpha})| \ll N^3 Q^{-1} \log^2 N.$$

Proof. By inserting (6.3) into the first interal, we obtain

$$\int_{\mathbb{T}^2} |W_Y(\boldsymbol{\alpha})|^2 \, d\boldsymbol{\alpha} = \int_{\mathbb{T}^6} U_Y(\boldsymbol{\beta}) \overline{U_Y(\boldsymbol{\gamma})} L(\boldsymbol{\alpha} - \boldsymbol{\beta}) \overline{L(\boldsymbol{\alpha} - \boldsymbol{\gamma})} \, d\boldsymbol{\beta} d\boldsymbol{\gamma} d\boldsymbol{\alpha}.$$

The integration with respect to $\boldsymbol{\alpha}$ can be performed explicitly by writing out the definition of the linear exponential sum L and using orthogonality. Changing the order of summation and integration, we arrive at

$$\int_{\mathbb{T}^2} |W_Y(\boldsymbol{\alpha})|^2 \, d\boldsymbol{\alpha} = \sum_{\mathbf{m} \leq 3(N, N^2)} \left| \int_{\mathbb{T}^2} U_Y(\boldsymbol{\beta}) e(-\boldsymbol{\beta} \cdot \mathbf{m}) \, d\boldsymbol{\beta} \right|^2.$$

By the Bessel-inequality on the Hilbert space $L^2(\mathbb{T}^2)$, we can bound this by $\|U_Y\|_2^2$. We insert the definition (6.1) of $U_Y(\boldsymbol{\alpha})$ and recall that the functions in this sum have disjoint supports. We obtain

$$\|U_Y\|_2^2 = \sum_{Y \leq q < 2Y} q^{-6} \sum_{(\mathbf{a};q)=1} |V(q, \mathbf{a})|^6 \int_{\mathbb{T}^2} |v(\boldsymbol{\beta} - \mathbf{a}/q)|^6 \psi^2(\boldsymbol{\beta} - \mathbf{a}/q) \, d\boldsymbol{\beta}.$$

This is $O(N^3)$ by Lemma A.4 and Lemma A.5.

We proceed with the corresponding bound for W' and observe that by (6.5) we have

$$\int_{\mathbb{T}^2} |W'(\boldsymbol{\alpha})|^2 \, d\boldsymbol{\alpha} \ll \int_{\mathbb{T}^2} |W(\boldsymbol{\alpha})|^2 \, d\boldsymbol{\alpha} + \int_{\mathbb{T}^2} \Big| \sum_{Y \in J} W_Y(\boldsymbol{\alpha}) \Big|^2 \, d\boldsymbol{\alpha}.$$

By Lemma 5.1, the bound for the first integral on the right hand side is

$$\int_{\mathbb{T}^2} |W(\boldsymbol{\alpha})|^2 \, d\boldsymbol{\alpha} = \sum_{\mathbf{m} \leq 3(N, N^2)} R(\mathbf{m})^2 \ll N^3 \log N.$$

To estimate the second integral, we use the estimates for $W_Y(\boldsymbol{\alpha})$ and the Cauchy-Schwarz-inequality for the sum over $Y \in J$. This leads to a bound of $O(N^3 \log^2 N)$.

Now we turn to the second part of the proposition concerning the L^∞-estimates. Using (6.3) we obtain for $W_Y(\boldsymbol{\alpha})$ the bound

$$|W_Y(\boldsymbol{\alpha})| \leq \int_{\mathbb{T}^2} |U_Y(\boldsymbol{\beta})||L(\boldsymbol{\alpha} - \boldsymbol{\beta})| \, d\boldsymbol{\beta}.$$

Using definition (6.1) of $U_Y(\boldsymbol{\alpha})$ and Lemma A.5 again, this gives the bound

$$|W_Y(\boldsymbol{\alpha})| \leq \sum_{Y \leq q < 2Y} q^{-3} \sum_{(\mathbf{a};q)=1} |V(q, \mathbf{a})|^3 \int_{\mathbb{T}^2} |v(\boldsymbol{\beta} - \mathbf{a}/q)|^3 \psi(\boldsymbol{\beta} - \mathbf{a}/q)|L(\boldsymbol{\alpha} - \boldsymbol{\beta})| \, d\boldsymbol{\beta}$$

$$\ll Y^{-3/2} \sum_{Y \leq q < 2Y} \sum_{(\mathbf{a};q)=1} \int_{\mathbb{T}^2} |v(\boldsymbol{\beta} - \mathbf{a}/q)|^3 \psi(\boldsymbol{\beta} - \mathbf{a}/q)|L(\boldsymbol{\alpha} - \boldsymbol{\beta})| \, d\boldsymbol{\beta}.$$

It remains to estimate the inner integral in dependence on $\mathbf{a}$ and q in such a way that the sum is of size $O(N^3)$. For fixed $\boldsymbol{\alpha}$, there is at most one triple $(q, \mathbf{a})$ such that $\|\boldsymbol{\alpha} - \mathbf{a}/q\| \leq (2q)^{-2}$. Otherwise, we would get

$$(qq')^{-1} \leq |a_1/q - a_1'/q'| \leq (2q)^{-2} + (2q')^{-2},$$

which is impossible if q and q' differ by a factor of at most 2. For this triple we apply the Cauchy-Schwarz-inequality and obtain

$$\int_{\mathbb{T}^2} |v(\boldsymbol{\beta} - \mathbf{a}/q)|^3 \psi(\boldsymbol{\beta} - \mathbf{a}/q)|L(\boldsymbol{\alpha} - \boldsymbol{\beta})| \, d\boldsymbol{\beta}$$

$$\leq \Big(\int_{\mathbb{T}^2} |v(\boldsymbol{\beta} - \mathbf{a}/q)|^6 \psi^2(\boldsymbol{\beta} - \mathbf{a}/q) \, d\boldsymbol{\beta} \Big)^{1/2} \Big(\int_{\mathbb{T}^2} |L(\boldsymbol{\alpha} - \boldsymbol{\beta})|^2 \, d\boldsymbol{\beta} \Big)^{1/2}.$$

This is $O(N^3)$ by Lemma A.4 and orthogonality. For the other triples $(q, \mathbf{a})$ we use the trivial estimates $|L(\alpha)| \leq \|\alpha\|^{-1}$ and $|v(\boldsymbol{\beta} - \mathbf{a}/q)| \leq N$. This leaves us with the bound for the remaining part of the form

$$N^3 \sum_{Y \leq q < 2Y} \sum_{(\mathbf{a};q)=1}^* \int_{\mathbb{T}^2} \psi(\boldsymbol{\beta} - \mathbf{a}/q) \|\alpha_1 - \beta_1\|^{-1} \|\alpha_2 - \beta_2\|^{-1} \, d\boldsymbol{\beta}.$$

The $*$ at the sum indicates that we are leaving out the (possibly existing) triple $(q, \mathbf{a})$ with $\|\boldsymbol{\alpha} - \mathbf{a}/q\| \leq (2q)^{-2}$. This implies that $\boldsymbol{\alpha}$ is at least $(3q)^{-2}$ apart from the support of any remaining $\psi(\boldsymbol{\beta} - \mathbf{a}/q)$ and $\|\alpha_i - \beta_i\|^{-1}$ can be bounded by $O(Q^2)$. The support of ψ is of size $O(Q^3 N^{-3})$, which allows us to use the crude estimate $\int_\Omega f(x) \, d\mu \leq \mu(\Omega) \sup_{x \in \Omega} |f(x)|$ for each summand. It leads to a bound of size $O(Q^{10})$ for the whole expression, which is far better than needed.

Now we come to the last part of the proof, the L^∞-estimate for W'. Write

$$(6.5) \qquad U^*(\boldsymbol{\alpha}) = \sum_{Y \in J} U_Y(\boldsymbol{\alpha})$$

to simplify notation. We can rewrite the identity $W(\boldsymbol{\alpha}) = V^3(\boldsymbol{\alpha})$ in a slightly complicated way as

$$W(\boldsymbol{\alpha}) = \int_{\mathbb{T}^2} V^3(\boldsymbol{\beta}) L(\boldsymbol{\alpha} - \boldsymbol{\beta}) \, d\boldsymbol{\beta},$$

as can be seen by calculating the right hand side explicitly.

By Lemma A.1 and equations (6.4) and (6.3), we can write

$$|W'(\boldsymbol{\alpha})| \leq \int_{\mathbb{T}^2} |V^3(\boldsymbol{\beta}) - U^*(\boldsymbol{\beta})||L(\boldsymbol{\alpha} - \boldsymbol{\beta})| \, d\boldsymbol{\beta} \leq \|V^3 - U^*\|_\infty \log^2 N$$

where the L^∞-norm is taken over $\mathbb{T}^2 = [2QN^{-1}, 1 + 2QN^{-1}] \times [2Q^2 N^{-2}, 1 + 2Q^2 N^{-2}]$.

If we are outside the support of U^*, we have $|V(\boldsymbol{\alpha})| \ll NQ^{-1/3}$ by Lemma $A.6$. This leads to the bound $O(N^3 Q^{-1} \log^2 N)$. If $\boldsymbol{\alpha}$ is in the support of U^* (major arc case), we have an approximation $\alpha_i = a_i/q + \beta_i$ with $q \leq 4Q$ and $|\beta_i| \leq 2Q^i N^{-i}$, where $\mathbf{a}, q$ and $\boldsymbol{\beta}$ are defined as in Lemma A.2. By (6.1), (6.5) and the choice of the parameter Q we see that U^* is a sum of disjointly supported functions. Unsing the approximation for $V(\boldsymbol{\alpha})$ from Lemma A.2, we obtain the expression

$$V^3(\boldsymbol{\alpha}) - U^*(\boldsymbol{\alpha}) = (q^{-1}V(q, \mathbf{a})v(\boldsymbol{\beta}) + \Delta)^3 - q^{-3}V(q, \mathbf{a})^3 v(\boldsymbol{\beta})^3 \psi(\boldsymbol{\beta}).$$

The trivial estimate is $O(N^3)$ and the task is to save a factor of Q. We have $\Delta \ll Q^3$ and can safely ignore terms involving Δ as long as $Q^3 \leq NQ^{-1}$, which is true by our choice of Q. We are left with the task to estimate

$$q^{-3}V(q, \mathbf{a})^3 v(\boldsymbol{\beta})^3 (1 - \psi(\boldsymbol{\beta})^3) \leq v(\boldsymbol{\beta})^3 (1 - \psi(\boldsymbol{\beta})^3).$$

This is zero if $\psi(\boldsymbol{\beta}) = 1$. Otherwise, we have $|\beta_i| \geq Q^i/N^i$ for some $i \in \{1, 2\}$ by (2.6) and Lemma A.3 provides $|v(\boldsymbol{\beta})| \ll NQ^{-1/2}$. This gives an estimate of the shape $O(N^3 Q^{-3/2})$ which is acceptable as long as Q is a small power of N. $\qquad \square$

The next part is concerned with the arithmetic estimates.

Proposition 6.3. *For each $k \in \mathbb{N}$ with $Q^{4k} \leq N$ we have*

$$\sum_{\mathbf{m} \leq 3(N, N^2)} |R_Y(\mathbf{m})|^{2k} \ll_{\epsilon, k} Y^\epsilon N^3 \quad and \quad \sum_{\mathbf{m} \leq 3(N, N^2)} |R'(\mathbf{m})|^{2k} \ll_{\epsilon, k} N^{3+\epsilon}.$$

Remark 6.4. *Notice that we can choose k as big as we like by reducing Q.*

Proof. We plug in formula (6.1) into (6.2). This gives an expression for R_Y which we transform by changing the order of summation and integration and the change of variables $\boldsymbol{\alpha} = \mathbf{a}/q + \boldsymbol{\beta}$ into

$$R_Y(\mathbf{m}) = \sum_{Y \leq q < 2Y} \frac{1}{q^3} \sum_{(\mathbf{a}; q) = 1} V(q, \mathbf{a})^3 e_q(-\mathbf{a} \cdot \mathbf{m}) \int_{\mathbb{T}^2} \psi(\boldsymbol{\beta}) v(\boldsymbol{\beta})^3 e(-\boldsymbol{\beta}\mathbf{m}) \, d\boldsymbol{\beta}.$$

This form is more suitable for estimates, because the arithmetic part and the analytic part are separated. By Lemma 5.2, the integral, appearing in the formula for R_Y, may be estimated

by a constant. Using Lemma 5.4, we can write the arithmetic part in the form

$$\frac{1}{q^3} \sum_{(\mathbf{a};q)=1} V(q,\mathbf{a})^3 e_q(-\mathbf{a}\cdot\mathbf{m}) = \frac{1}{q^2} \sum_{\substack{a=1 \\ (a;q)=1}}^{q} G_{m_1}(q,a)\, e_q(-am_2).$$

Lemma A.5 provides the estimate $q^{-2}G_{m_1}(q,a) \ll q^{-1}$ if $(a;q)=1$ and we set $G_{m_1}(q,a)=0$ if $(a;q)>1$. By Lemma 5.3, we have

$$\sum_{m_2 \leq 3N^2} |R_Y(\mathbf{m})|^{2k} \ll_{\epsilon,k} Y^\epsilon N^2$$

as long as $Q^{4k} \leq N$, which implies the first result by summing over m_1.

For the second estimate, we observe that $R'(\mathbf{m}) = R(\mathbf{m}) - \sum_{Y \in J} R_Y(\mathbf{m})$. The result follows from an application of Hölder's inequality, part one of this proof and Lemma 5.1. $\square$

7. Finding integer solutions of the system

This is the part of our paper which has not changed significantly compared to the work of Smith [23]. We use the circle method to prove the following proposition, which together with Theorem 2.1 concludes the proof of Theorem 1.1. Write $Z(N)$ for the number of solutions to (1.1) with $x_i \in \{1,\dots,N\}$.

Proposition 7.1. *Assume that the conditions of Section 1 hold. Then* $Z(N) \gg N^{s-3}$, *where the implied constant is only dependent on the coefficients* λ_i *of the system.*

By orthogonality, we can rewrite $Z(N)$ as the integral

$$(7.1) \qquad\qquad Z(N) = \int_{\mathbb{T}^2} \prod_{i=1}^{s} V(\lambda_i \boldsymbol{\alpha})\, d\boldsymbol{\alpha}.$$

Define the major arcs $\mathfrak{M} \subset \mathbb{T}^2$ to be the (disjoint) union of

$$\mathfrak{M}(q,\mathbf{a}) = \{\boldsymbol{\alpha} \in \mathbb{T}^2 : \|\alpha_i - a_i/q_i\| \leq Q^i N^{-i}\},$$

where $q \leq Q$ and $\mathbf{a} \leq q$ with $(\mathbf{a};q)=1$. The minor arcs are the complement $\mathfrak{m} = \mathbb{T}^2\backslash\mathfrak{M}$.

We decompose the right hand side of (7.1) into an integral over $\mathfrak{M}$ and one over $\mathfrak{m}$. By using Lemma A.2 and the crude estimates $|V(q,\lambda_i \mathbf{a})| \leq q$, $|v(\alpha)| \leq N$, $|\Delta| \leq Q^3$ and the bound $\mu(\mathfrak{M}(q,\mathbf{a})) \leq Q^3/N^3$ for the Lebesgue measure of $\mathfrak{M}$, we obtain by a standard calculation

$$\int_{\mathfrak{M}} \prod_{i=1}^{s} V(\lambda_i \boldsymbol{\alpha})\, d\boldsymbol{\alpha} = J(Q/N)\mathfrak{S}(Q) + O(Q^9 N^{s-4}),$$

with the truncated singular integral

$$J(Q/N) = \int_{|\alpha_1| \leq Q/N} \int_{|\alpha_2| \leq Q^2/N^2} \prod_{i=1}^{s} v(\lambda_i \boldsymbol{\alpha})\, d\boldsymbol{\alpha},$$

and the truncated singular series

$$(7.2) \qquad\qquad \mathfrak{S}(Q) = \sum_{q \leq Q} q^{-s} \sum_{(\mathbf{a};q)=1} \prod_{i=1}^{s} V(q,\lambda_i \mathbf{a}).$$

It follows from Lemma A.5 and the condition $s \geq 7$ that the limit $\mathfrak{S} := \lim_{Q \to \infty} \mathfrak{S}(Q)$ exists and we have $\mathfrak{S}(Q) = \mathfrak{S} + O(Q^{-1/2})$. Similarly, we complete $J(Q/N)$ to an integral

$$(7.3) \qquad J = \int_{\mathbb{R}^2} \prod_{i=1}^{s} v(\lambda_i \boldsymbol{\alpha}) \, d\boldsymbol{\alpha}$$

over $\mathbb{R}^2$. Convergence and the formula $J(Q/N) = J + O(N^{s-3}Q^{-1/2})$ follow by Lemma A.3. This gives a major arcs contribution of

$$\int_{\mathfrak{M}} \prod_{i=1}^{s} V(\lambda_i \boldsymbol{\alpha}) \, d\boldsymbol{\alpha} = \mathfrak{S}J + O(Q^9 N^{s-4} + N^{s-3}Q^{-1/2}).$$

For $\boldsymbol{\alpha} \in \mathfrak{m}$ we observe the bound $O(NQ^{-1/3})$ for the L^∞-norm of $V(\boldsymbol{\alpha})$ by Lemma $A.6$. The actual exponential sums $V(\lambda_i \boldsymbol{\alpha})$ can be bounded similarly by $O(NQ^{-1/3})$, where the implied constant is now dependent on the fixed coefficient $\lambda_i \in \mathbb{Z}$. Using Hölder's inequality and the bound from Lemma 5.1 for the sixth moment of the exponential sum, we obtain

$$\int_{\mathfrak{m}} \prod_{i=1}^{s} V(\lambda_i \boldsymbol{\alpha}) \, d\boldsymbol{\alpha} \ll (NQ^{-1/3})^{s-6} \int_{\mathbb{T}^2} |V(\boldsymbol{\alpha})|^6 \, d\boldsymbol{\alpha} \ll_\epsilon N^{s-3+\epsilon} Q^{-1/3}.$$

Setting $Q = N^{4\eta}$ for a small $\eta > 0$, the number of solutions is given by

$$Z(N) = \mathfrak{S}J + O(N^{s-3-\eta}).$$

If we can show that $\mathfrak{S} > 0$ and $J \gg N^{s-3}$, then Proposition 7.1 is proven. These are the remaining tasks for this section.

Lemma 7.2. *We have $\mathfrak{S} > 0$.*

Proof. We denote the summand in (7.2) by

$$V(q) = q^{-s} \sum_{(\mathbf{a};q)=1} \prod_{i=1}^{s} V(q, \lambda_i \mathbf{a}).$$

It is not too difficult to check that $V(qt, \lambda_i t \mathbf{a} + \lambda_i q \mathbf{b}) = V(q, \lambda_i \mathbf{a})V(t, \lambda_i \mathbf{b})$ as long as $(t; q) = 1$. This implies that $V(q)$ is multiplicative by another short calculation. For details, the reader is referred to [25, p. 20]. Furthermore $V(q) \ll q^{-3/2}$ by Lemma A.5 and $s \geq 7$. If we define

$$T(p) := \sum_{k=0}^{\infty} V(p^k)$$

as the part corresponding to the prime p, then $T(p) = 1 + O(p^{-3/2})$ and we can write $\mathfrak{S}$ as an absolutely convergent product $\mathfrak{S} = \prod_p T(p)$. Therefore, we have $\prod_{p \geq p_0} T(p) \geq 1/2$ for some p_0. To show that $T(p) > 0$ for the finitely many remaining factors, we relate $T(p)$ to the number of solutions modulo p^k and the result follows from the following two lemmata. $\qquad \square$

Lemma 7.3. *We have*

$$T(p) = \lim_{k \to \infty} p^{(2-s)k} S(p^k)$$

where $S(q)$ is the number of solutions to the system (1.1) *modulo q.*

Proof. By orthogonality and a direct calculation, the number of solutions $S(q)$ can be written as

$$S(q) = \sum_{r_1, \ldots, r_s \leq q} q^{-2} \sum_{a_1, a_2 \leq q} e_q(a_1(\lambda_1 r_1^2 + \ldots + \lambda_s r_s^2)) e_q(a_2(\lambda_1 r_1 + \ldots + \lambda_s r_s)).$$

Here we are in the special situation of $q = p^k$. We can introduce another parameter l and sort according to the condition $(a_1; a_2) = p^l$. After rearrangement, we have the intermediate form

$$S(p^k) = p^{-2k} \sum_{l=0}^{k} \sum_{(a_1;a_2)=p^l} \prod_{i=1}^{s} V(p^k, \lambda_i a_1, \lambda_i a_2).$$

The change $a_i = p^l b_i$ and the corresponding change of $V(p^k, \lambda_i a_1, \lambda_i a_2)$ to $p^{ls} V(p^{k-l}, \lambda_i b_1, \lambda_i b_2)$ together with some elementary transformations give us

$$\sum_{l=0}^{k} V(p^l) = p^{(2-s)k} S(p^k).$$

Taking limits on both sides gives the statement of the lemma. $\qquad \square$

The next task is to bound the number of solutions modulo p^k from below.

Lemma 7.4. *For each prime p there is an $u = u(p) \in \mathbb{N}$, such that*

$$S(p^k) \gg p^{(k-u)(s-2)}.$$

For the proof we need a version of Hensel's lemma rewritten in the language of p-adic valuations. Denote by $\mathbb{Z}_p$ the p-adic integers and let $| \cdot |_p$ be the standard p-adic valuation.

Lemma 7.5. *Suppose that $F_1(X_1, X_2), F_2(X_1, X_2) \in \mathbb{Z}_p[X_1, X_2]$, and that $a_0, b_0 \in \mathbb{Z}_p$ satisfy*

$$\max\{|F_1(a_0, b_0)|_p, |F_2(a_0, b_0)|_p\} < |\Delta_0|_p^2,$$

where $\Delta_0 = \Delta(F_1, F_2)|_{(a_0,b_0)} = \left(\frac{\partial F_1}{\partial X_1} \frac{\partial F_2}{\partial X_2} - \frac{\partial F_2}{\partial X_1} \frac{\partial F_1}{\partial X_2} \right)_{(a_0,b_0)}$ is non-zero, $\frac{\partial F_1}{\partial X_1}$ etc. being formal derivatives. Then there is a unique $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p$, such that $F_1(a, b) = F_2(a, b) = 0$ and

$$\max\{|a - a_0|_p, |b - b_0|_p\} \leq p^{-1} \cdot |\Delta_0|_p.$$

Proof. This is Proposition 5.20 in [15]. $\qquad \square$

Proof of Lemma 7.4. The first step is to obtain a non-singular p-adic solution. The system (1.1) can be written as a quadratic equation in $s-1$ variables by inserting the linear equation into the quadratic one.

$$\lambda_s(\lambda_1 x_1^2 + \ldots + \lambda_{s-1} x_{s-1}^2) + (\lambda_1 x_1 + \ldots + \lambda_{s-1} x_{s-1})^2 = 0$$

By a well known theorem of Meyer [18], a quadratic form has a non-trivial (not all $x_i = 0$) p-adic solution, as long as the number of variables is at least five. We have $s - 1 \geq 6$, so we have one variable 'left'. We use this variable to ensure that our solution is not only non-trivial, but also non-singular. A solution of (1.1) is *non-singular*, if one of the 2×2 matrices $\left(\begin{smallmatrix} 2\lambda_i x_i & 2\lambda_j x_j \\ \lambda_i & \lambda_j \end{smallmatrix} \right)$ has a non-zero determinant. This is the case if and only if $x_i \neq x_j$ for some $i \neq j$. To achieve this, we fix $x_2 = 0$ and use Meyer's theorem with the remaining $s - 2 \geq 5$ variables. Since $x_2 = 0$ and $x_i \neq 0$ for some i by non-triviality, the result follows.

Let $\mathbf{y} \in \mathbb{Z}_p$ be the non-singular solution we have found above. We switch back to the representation of (1.1) as two equations and assume for simplicity that $y_1 \neq 0$, which may be achieved by renaming the variables. Define for $\mathbf{x}'' = (x_3, \ldots, x_s)$ the binary polynomials

$$F_{i,\mathbf{x}''}(x_1, x_2) := \lambda_1 x_1^i + \lambda_2 x_2^i + \lambda_3 x_3^i + \ldots + \lambda_s x_s^i \qquad (i \in \{1, 2\}).$$

For the point $(a_0, b_0) = (y_1, 0)$ we set $\Delta_0 = 2\lambda_1\lambda_2 y_1$, as in Lemma 7.5. For vectors $\mathbf{x}''$ with $|x_j - y_j|_p < |\Delta_0|_p^2$ for $3 \leq j \leq s$, we have

$$|F_{i,\mathbf{x}''}(y_1, 0)|_p = |F_{i,\mathbf{x}''}(y_1, 0) - F_{i,\mathbf{y}''}(y_1, 0)|_p < |\Delta_0|_p^2$$

by an elementary calculation, and, therefore, the condition of Lemma 7.5 is satisfied. This means that, as long as $\mathbf{x}''$ is close enough to $\mathbf{y}''$, we can extend $\mathbf{x}''$ in a unique way to a solution $\mathbf{x}$.

Looking at this from the congruence point of view (by using the definition of the p-adic valuation), we have to ensure that $\mathbf{x}''$ is congruent to $\mathbf{y}''$ modulo p^u, where u is defined by $|\Delta_0|_p^2 = p^{-u+1}$. The number of choices for $\mathbf{x}''$ modulo p^k, which are congruent to $\mathbf{y}''$ modulo p^u for $k \geq u$, is $(p^{k-u})^{s-2}$. For each such choice $\mathbf{x}''$ we have by Lemma 7.5 a unique $(x_1, x_2) \in \mathbb{Z}_p$ with $F_{i,\mathbf{x}''}(x_1, x_2) = 0$. This leads to a unique solution modulo p^k and the lemma follows. $\square$

Now we get to the second main task, the lower bound for J.

Lemma 7.6. *Under the usual assumptions for system* (1.1)*, we have* $J \gg N^{s-3}$*, where the implied constant depends on the coefficients* λ_i*.*

Proof. Similar to the p-adic case, we first show the existence of a non-singular real solution. This is a solution with $x_i \neq x_j$ for some $i \neq j$, as observed in the proof of Lemma 7.4. We will perform a pertubation argument and create a non-sigular solution from a singular one. This is where condition (iii) for system (1.1) comes into play. We know that there are at least two positive and two negative coefficients λ_i. We sort and rename the coefficients and variables according to their signs and obtain

$$\lambda_1 x_1^2 + \ldots + \lambda_t x_t^2 = \mu_1 x_{t+1}^2 + \ldots + \mu_t x_{t+r}^2,$$
$$\lambda_1 x_1 + \ldots + \lambda_t x_t = \mu_1 x_{t+r} + \ldots + \mu_t x_{t+r},$$

where $r + t = s$ with $r, t \geq 2$ and $\lambda_i > 0, \mu_j > 0$. By condition (i) for (1.1), there is always the trivial solution $\mathbf{x} = (1, \ldots, 1)$. Now fix all the variables x_i to be 1 except x_1, x_2 and $y_1 = x_{t+1}, y_2 = x_{t+2}$. Then we are in the situation

$$(7.4) \qquad \begin{aligned} \lambda_1 x_1^2 + \lambda_2 x_2^2 + c &= \mu_1 y_1^2 + \mu_2 y_2^2, \\ \lambda_1 x_1 + \lambda_2 x_2 + c &= \mu_1 y_1 + \mu_2 y_2, \end{aligned}$$

for some suitable constant $c \in \mathbb{Z}$. Put $x_1 = 1 + \lambda_2\theta, x_2 = 1 - \lambda_1\theta$ and $y_1 = 1 + \mu_2\varphi, y_2 = 1 - \mu_1\varphi$. System (7.4) is satisfied with $\theta = \varphi = 0$ and the linear equation for all choices of θ and φ. This simplifies (7.4) to

$$\lambda_1\lambda_2(\lambda_1 + \lambda_2)\theta^2 = \mu_1\mu_2(\mu_1 + \mu_2)\varphi^2.$$

Hence there is a solution with $\theta > 0, \varphi > 0$, which is non-singular.

Now we prove the lower bound on J by connecting it to the manifold of real solutions around a non-singular point. By (7.3), the dominated convergence theorem and (2.5), we have

$$J = \lim_{P \to \infty} \int_{\mathbb{R}^2} \chi(\alpha_2 N^2/P)\chi(\alpha_1 N/P) \prod_{i=1}^s v(\lambda_i \boldsymbol{\alpha})\, d\boldsymbol{\alpha}.$$

Inserting the definition (2.2) of v and interchanging the order of integration (Λ has finite support), leads to

$$J = \lim_{P \to \infty} \int_{[0,N]^s} \int_{\mathbb{R}^2} \chi(\alpha_2 N^2/P)\chi(\alpha_1 N/P)e(\alpha_2 K_2(\mathbf{x}) + \alpha_1 K_1(\mathbf{x}))\, d\boldsymbol{\alpha} d\mathbf{x},$$

where $K_i(\mathbf{x}) = \sum_{l=1}^{s} \lambda_l x_l^i$ (with coefficients λ_l as in (1.1)). The change of variables $x_i = N y_i$ and $\beta_i = N^i \alpha_i$ separates the parameter N and we obtain

$$J = N^{s-3} \lim_{P \to \infty} \int_{[0,1]^s} \int_{\mathbb{R}^2} \chi(\beta_2/P)\chi(\beta_1/P)e(\beta_2 K_2(\mathbf{y}) + \beta_1 K_1(\mathbf{y})) \, d\boldsymbol{\beta} d\mathbf{y}.$$

The two inner integrals are Fourier transforms and we get

$$J = N^{s-3} \lim_{P \to \infty} \int_{[0,1]^s} P\widehat{\chi}(-PK_2(\mathbf{y}))P\widehat{\chi}(-PK_1(\mathbf{y})) \, d\mathbf{y}.$$

The Fourier transform $\widehat{\chi}$ is given by $\frac{\sin(\pi y)^2}{(\pi y)^2}$ and is positive. Therefore, we can estimate this integral from below by estimating $\frac{\sin(\pi y)^2}{(\pi y)^2}$ from below by $1/2$ when $|y| \le 1/10$, for example. We obtain the lower bound

(7.5) $$4^{-1}P^2\mu(\{\mathbf{y} \in [0,1]^s : |K_2(\mathbf{y})| \le (10P)^{-1}, |K_1(\mathbf{y})| \le (10P^{-1})\}),$$

where μ is the Lebesgue measure. By the argument above, the quadric has a non-singular real solution $\mathbf{x}$ (let $x_1 \neq x_2$). By translation and dilation invariance of the system (1.1), we can assume that $\mathbf{x}$ lies in $(0,1)^s$.

We use the implicit function theorem. This allows us to write $y_1 = \phi_1(\mathbf{y}'')$ and $y_2 = \phi_2(\mathbf{y}'')$ where $\mathbf{y}'' = (y_3, \ldots, y_s)$ and ϕ_1, ϕ_2 are differentiable functions, such that $K_i(\phi_1(\mathbf{y}''), \phi_2(\mathbf{y}''), \mathbf{y}'') = 0$ ($i \in \{1, 2\}$) for all $\mathbf{y}''$ in a neighbourhood of $\mathbf{x}'' = (x_3, \ldots, x_s)$. If we fix one of these points $\mathbf{y}''$, then we can vary the y_1 and y_2-coordinates by at least $|\epsilon_i| = (40P|\lambda_i|)^{-1}$ ($i \in \{1, 2\}$) without leaving the set in (7.5). Therefore, its volume is $\gg P^{-2}$. $\qquad\square$

Appendix A. Collection of various estimates for exponential sums

Lemma A.1. *For the linear exponential sum L_M in (2.3) with $M \ge 2$ we have*

$$\int_{\mathbb{T}} |L_M(\alpha)| \, d\alpha \ll \log M.$$

Proof. The standard estimate $|L_M(\alpha)| \le \min\{M, \|\alpha\|^{-1}\}$ follows by an application of the finite geometric sum formula. Now decompose the integral into two parts $\|\alpha\| \le 1/M$ and $\|\alpha\| > 1/M$. The result is immediate. $\qquad\square$

The next three lemmata are specialised versions of results from [25]. First we have an approximation to $V(\boldsymbol{\alpha})$ by the local versions (2.2) on the major arcs.

Lemma A.2. *Let $\alpha_i = b_i/q_i + \beta_i$ ($i = 1, 2$) with $b_i, q_i \in \mathbb{Z}$ and suppose that $q = \mathrm{lcm}(q_1, q_2)$ and $a_i = b_i q q_i^{-1}$. Then*

$$V(\boldsymbol{\alpha}) = q^{-1}V(q, \mathbf{a})v(\boldsymbol{\beta}) + \Delta,$$

where

$$\Delta \ll q(1 + |\beta_1|N + |\beta_2|N^2).$$

Proof. This is the special case $k = 2$ of [25, Theorem 7.2]. $\qquad\square$

Now we give an estimate for the local function $v(\boldsymbol{\alpha})$.

Lemma A.3. *We have the estimate*

$$|v(\boldsymbol{\alpha})| \ll N(1 + |\alpha_1|N + |\alpha_2|N^2)^{-1/2}.$$

Proof. This is the special case $k = 2$ of [25, Theorem 7.3]. $\qquad\square$

The next result is an easy corollary of the previous lemma.

Lemma A.4. *For $p > 4$ and $\mathbb{T}^2 = [-1/2, 1/2]^2$ we have*

$$\int_{\mathbb{T}^2} \psi^2(\boldsymbol{\alpha}) \, |v(\boldsymbol{\alpha})|^p \, d\boldsymbol{\alpha} \ll_p N^{p-3},$$

where $\psi(\boldsymbol{\alpha})$ is defined in (2.6).

Proof. Use $(1 + |\alpha_1|N + |\alpha_2|N^2)^{-2} \ll (1 + |\alpha_1|N)^{-1}(1 + |\alpha_2|N^2)^{-1}$ and $|\psi(\boldsymbol{\alpha})| \leq 1$. $\qquad\square$

The following result gives a well-known estimate for Gauß sums. It allows us to bound $V(q, \mathbf{a})$ and the quadratic exponential sum $G_{m_1}(q, a)$ appearing in Lemma 5.4.

Lemma A.5. *Let $F_2(\mathbf{x}) = \mathbf{x}^t M \mathbf{x}$ be a quadratic form with $M \in \mathbb{Z}^{d \times d}$ a symmetric matrix of determinant $\Delta \neq 0$ and $F_1(\mathbf{x})$ an arbitrary affine linear polynomial. Let*

$$G(q, a) = \sum_{\mathbf{x} \leq q} e_q(aF_2(\mathbf{x}) + F_1(\mathbf{x})).$$

Then for $(a; q) = 1$ we have

$$|G(q, a)| \ll_{d, \Delta} q^{d/2}$$

uniformly in F_1. In particular, this implies

$$|V(q, \mathbf{a})| \ll q^{1/2}.$$

Proof. Let F_1' be the linear part of F_1. By squaring $G(q, a)$, a change of variables and the q-periodicity of e_q we obtain

$$
\begin{aligned}
|G(q, a)|^2 &= \sum_{\mathbf{x} \leq q} \sum_{\mathbf{y} \leq q} e_q(a(F_2(\mathbf{x}) - F_2(\mathbf{y})) + (F_1(\mathbf{x}) - F_1(\mathbf{y}))) \\
&= \sum_{\mathbf{h} \leq q} \sum_{\mathbf{y} \leq q} e_q(a(F_2(\mathbf{y} + \mathbf{h}) - F_2(\mathbf{y}))) + (F_1(\mathbf{y} + \mathbf{h}) - F_1(\mathbf{y}))) \\
&= \sum_{\mathbf{h} \leq q} e_q(aF_2(\mathbf{h}) + F_1'(\mathbf{h})) \sum_{\mathbf{y} \leq q} e_q(a2\mathbf{h}^t M \mathbf{y}) \\
&= q^d \sum_{\mathbf{h} \leq q} e_q(aF_2(\mathbf{h}) + F_1'(\mathbf{h})) \mathbf{1}_{q | 2aM\mathbf{h}} \leq q^d \sum_{\mathbf{h} \leq q} \mathbf{1}_{q | 2aM\mathbf{h}}.
\end{aligned}
$$

Since $(a; q) = 1$ the number of vectors $2aM\mathbf{h}$ divisible by q componentwise is bounded by $2^d \Delta$ and the estimate follows. $\qquad\square$

We need a good estimate for $V(\boldsymbol{\alpha})$ on the minor arcs as well.

Lemma A.6. *Assume that $|V(\boldsymbol{\alpha})| \geq NQ^{-1/3}$ for $N \geq N_0(\epsilon)$ with $N^{3\epsilon} \leq Q$. Then there exists $q \leq Q$ and $a_1, a_2 \in \mathbb{Z}$, such that $(q; a_1; a_2) = 1$ and $|\alpha_i q - a_i| \leq QN^{-i}$ for $i \in \{1, 2\}$.*

Proof. This is a special case of Theorem 5.1 in [1]. Choose the parameters in [1] to be $M = 1$, $P = NQ^{-1/3}$, $k = 2$ and $\epsilon > 0$ such that $N^{3\epsilon} \leq Q$. $\qquad\square$

Appendix B. From exponential correlation to a density increment

In this appendix we are going to prove the simple but crucial Lemma B.1. It enables us to transfer a correlation estimate for exponential sums into a density increment on a subprogression.

Let f be the balanced function as defined in (3.1) and consider the corresponding exponential sum V_f as defined in (2.1).

Lemma B.1. *If $|V_f(\boldsymbol{\alpha})| \geq \eta N$ for some $\boldsymbol{\alpha} \in \mathbb{T}^2$ and $\eta > 0$, then there is an arithmetic progression $P \subset \{1, 2, \ldots, N\}$ of length $|P| \gg \eta^2 N^{1/16}$ with*

$$|\mathcal{A} \cap P| \geq (\delta + \eta/4)|P|.$$

Results of this kind are well known (see [10], for example), but in the current literature usually given in the $\mathbb{Z}/N\mathbb{Z}$-setting. We give here a proof for completeness and use the following classical result of Heilbronn in diophantine approximation.

Lemma B.2. *Let $\alpha \in \mathbb{R}$ and $Q \in \mathbb{N}$. Then there is $q \leq Q$ such that $\|\alpha q^2\| \ll_\epsilon Q^{-1/2+\epsilon}$.*

Proof. A proof can be found in [1, p. 26]. $\qquad\square$

Remark B.3. *Zaharescu [26] got the exponent $-4/7$ instead of $-1/2$. But for our purpose the result of Heilbronn is sufficient and we even fix $\epsilon = 1/6$ for simplicity.*

Proof of Lemma B.1. The idea is to cover $\{1, 2, \ldots, N\}$ by long progressions in such a way that the function $h : n \mapsto e(\alpha_1 n^2 + \alpha_2 n)$ is almost constant on each progression.

By Lemma B.2 we can find $q \leq N^{3/4}$, such that $\|\alpha_2 q^2\| \leq CN^{-1/4}$ for some absolute constant $C \geq 1$. We can assume that $N \geq (2^8 C/\eta^2)^{16}$. Otherwise, the lemma is true for a singleton $P = \{n\}$ with $n \in \mathcal{A}$. We decompose $\{1, 2, \ldots, N\}$ in congruence classes modulo q and split those into progressions $\{m + kq : 0 \leq k < K\}$ of length K between $2^{-4}C^{-1}\eta N^{1/8}$ and $2^{-3}C^{-1}\eta N^{1/8}$. The expression $\alpha_2 n^2 + \alpha_1 n$ varies on such a progression by at most

$$\|(\alpha_2(m + qk)^2 + \alpha_1(m + qk)) - (\alpha_2(m + ql)^2 + \alpha_1(m + ql))\|$$
$$= \|(2\alpha_2 mq + \alpha_1 q)(k - l) + \alpha_2 q^2(k^2 - l^2)\|$$
$$\leq \|(2\alpha_2 mq + \alpha_1 q)(k - l)\| + \|\alpha_2 q^2\|K^2 \leq \|\beta(k - l)\| + 2^{-6}\eta^2,$$

where $\beta := 2\alpha_2 mq + \alpha_1 q$. For a given progression from the decomposition above, the expression β is constant and we have reduced our quadratic problem to a linear one. By Dirichlet's approximation theorem we can find a value $r \leq K^{1/2}$ with $\|\beta r\| \leq K^{-1/2}$. We partition the given progression into congruence classes modulo r and then further in subprogressions P_i ($i \in I$, where I is a set of indices) of length between $2^{-6}\eta K^{1/2}$ and $2^{-5}\eta K^{1/2}$. This leads to

$$\|\beta(k - l)\| = \|\beta tr\| \leq 2^{-5}\eta.$$

Observe that for $\|x_1 - x_2\| \leq y$ we get $|e(x_1) - e(x_2)| \leq 2\pi y$. Therefore, the function $h(n) = e(\alpha_1 n^2 + \alpha_2 n)$ varies at most $\eta/2$ on each of these progressions. Now write $h(n) = h(m_i) + (h(n) - h(m_i))$ on each progression P_i, where $m_i \in P_i$. Since $|h(n) - h(m_i)|$ is bounded by $\eta/2$, we have

$$\eta N \leq |V_f(\boldsymbol{\alpha})| = \Big| \sum_{n \leq N} f(n)h(n) \Big| = \Big| \sum_{i \in I} \sum_{n \in P_i} f(n)h(n) \Big|$$
$$\leq \Big| \sum_{i \in I} h(m_i) \sum_{n \in P_i} f(n) \Big| + \eta N/2 \leq \sum_{i \in I} \Big| \sum_{n \in P_i} f(n) \Big| + \eta N/2.$$

The average $\sum_{i \in I} \sum_{n \in P_i} f(n)$ is zero by definition of f. We can add it to the right hand side and use the identity $|x| + x = 2\max\{0, x\}$. This gives

$$\sum_{i \in I} \max\Big\{0, \sum_{n \in P_i} f(n)\Big\} \geq \eta N/4.$$

It follows that there has to be at least one $i \in I$ with $\sum_{n \in P_i} f(n) \geq \eta|P_i|/4$. The result follows from the rearranging and using the formula $f(n) = 1_{\mathcal{A}}(n) - \delta$. $\qquad\square$

References

[1] R. C. Baker, Diophantine inequalities. The Clarendon Press, Oxford University Press, New York, 1986.

[2] V. Bergelson, A. Leibman, Polynomial extensions of van der Waerden's and Szemerédi's theorems. *J. Amer. Math. Soc.* 9 (1996), no. 3, 725–753.

[3] J. Bourgain, On $\Lambda(p)$-subsets of squares. *Israel J. Math.* 67 (1989), no. 3, 291–311.

[4] J. Bourgain, Fourier transform restriction phenomena for certain lattice subsets and applications to nonlinear evolution equations. I. Schrödinger equations. *Geom. Funct. Anal.* 3 (1993), no. 2, 107–156.

[5] J. Bourgain, Roth's theorem on progressions revisited. *J. Anal. Math.* 104 (2008), 155–192.

[6] H. Davenport, Analytic methods for Diophantine equations and Diophantine inequalities. Second edition. Cambridge University Press, Cambridge, 2005.

[7] P. Erdős, P. Turan On some sequences of integers. *J. Lond. Math. Soc.* 11, 261–264 (1936).

[8] H. Furstenberg, Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *J. Analyse Math.* 31 (1977), 204–256.

[9] H. Furstenberg, Y. Katznelson and D. Ornstein, The ergodic theoretical proof of Szemerédi's theorem. *Bull. Amer. Math. Soc. (N.S.)* 7 (1982), no. 3, 527–552.

[10] T. Gowers, A new proof of Szemerédi's theorem. *Geom. Funct. Anal.* 11 (2001), no. 3, 465–588.

[11] B. Green, On arithmetic structures in dense sets of integers. *Duke Math. J.* 114 (2002), no. 2, 215–238.

[12] B. Green, Roth's theorem in the primes. *Ann. of Math.* (2) 161 (2005), no. 3, 1609–1636.

[13] B. Green and T. Tao, Restriction theory of the Selberg sieve, with applications. *J. Théor. Nombres Bordeaux* 18 (2006), no. 1, 147–182.

[14] B. Green and T. Tao, Linear equations in primes. *Ann. of Math.* (2) 171 (2010), no. 3, 1753–1850.

[15] M. J. Greenberg, Lectures on forms in many variables. W. A. Benjamin, Inc., New York-Amsterdam 1969

[16] D. R. Heath-Brown, Integer sets containing no arithmetic progressions. *J. London Math. Soc.* (2) 35 (1987), no. 3, 385–394.

[17] M. N. Huxley, Area, lattice points, and exponential sums. The Clarendon Press, Oxford University Press, New York, 1996.

[18] A. Meyer, Über die Auflösung der Gleichung $ax^2 + by^2 + cz^2 + du^2 + ev^2 = 0$ in ganzen Zahlen. *Vierteljahrsschr.* Naturforsch. Ges. Zürich 29 (1884), 209–222.

[19] N. N. Rogovskaya, An asymptotic formula for the number of solutions of a system of equations. (Russian) *Diophantine approximations*, Part II (Russian), 78–84, Moskov. Gos. Univ., Moscow, 1986.

[20] K. F. Roth, On certain sets of integers. *J. London Math. Soc.* 28, (1953), 104–109.

[21] T. Sanders, On Roth's theorem on progressions. *Ann. of Math.* (2) 174 (2011), no. 1, 619–636.

[22] A. Sárközy, On difference sets of sequences of integers. I. *Acta Math. Acad. Sci. Hungar.* 31 (1978), no. 1–2, 125–149.

[23] M. Smith, On solution-free sets for simultaneous quadratic and linear equations. *J. Lond. Math. Soc.* (2) 79 (2009), no. 2, 273–293.

[24] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression. *Acta Arith.* 27 (1975), 199–245.

[25] R. C. Vaughan, The Hardy-Littlewood method. Second edition. Cambridge University Press, Cambridge, 1997.

[26] A. Zaharescu, Small values of $n^2\alpha \pmod 1$. *Invent. Math.* 121 (1995), no. 2, 379–388.