THE DISTRIBUTION OF SPACINGS BETWEEN THE FRACTIONAL PARTS OF $n^d\alpha$

MARTINO FASSINA, SUN KIM, AND ALEXANDRU ZAHARESCU

Abstract. We study the distribution of spacings between the fractional parts of $n^d\alpha$. For $\alpha$ of high enough Diophantine type we prove a necessary and sufficient condition for $n^d\alpha \mod 1$, $1 \leq n \leq N$, to be Poissonian as $N \to \infty$ along a suitable subsequence.

1. Introduction

Let $f(x)$ be a polynomial, and consider the sequence of fractional parts $(\{f(n)\})_{n \in \mathbb{N}}$. It is of considerable interest to study the distribution of the spacings between members of the sequence. This problem arose in the context of the distribution of spacings between the energy levels of integrable systems [BT77, CGI87]. When $f(x) = \alpha x$, the spacings are essentially those of the energy levels of a two-dimensional harmonic oscillator (see [PBG89]). In this case, the sequence is not random: for any $\alpha$ and $N$, the consecutive spacings of $n\alpha \mod 1$, $1 \leq n \leq N$, take at most three values (see [S685] and [Sw59]).

In the more challenging case $f(x) = \alpha x^d$, $d \geq 2$, Rudnick and Sarnak [RS98] investigated the pair correlation function, which measures the density of differences between pairs of elements of the sequence. They proved that for almost all $\alpha$ the pair correlation function is Poissonian. For another approach to this result see [BZ00].

For the case $d = 2$ significantly more is known. Rudnick, Sarnak and one of the authors [RSZ01], [Z03] investigated higher order correlations of $n^2\alpha \mod 1$ (more details about these works will be discussed later in the paper). Recently, the size of clusters of $n^2\alpha \mod 1$ played a relevant role in the work of Dunn and one of the authors [DZ19] on a second moment of central values of certain half integral weight Dirichlet series. See also the survey [Sh12] for connections between this sequence and other related topics.

In the present paper we return to the original sequence $n^d\alpha \mod 1$ studied by Rudnick and Sarnak. We let $\alpha$ be an irrational number, $d$ an integer, $d \geq 2$, and consider the problem of studying the distribution of local spacings between the elements of the sequence $n^d\alpha \mod 1$, with $1 \leq n \leq N$. For an integer $m \geq 2$, and a smooth compactly supported function
$f \in \mathcal{C}_c^\infty(\mathbb{R}^{m-1})$, we consider the $m$-level correlation sums

$$R^{(m)}(N, d, \alpha, f) = \frac{1}{N} \sum_{1 \leq n_1, \ldots, n_m \leq N} F_N(n_1^d \alpha - n_2^d \alpha, \ldots, n_{m-1}^d \alpha - n_m^d \alpha),$$

where $F_N(y) = \sum_{l \in \mathbb{Z}^{m-1}} f(N(1 + y))$. We say that the $m$-level correlation of the sequence $n^d \alpha \mod 1$ is Poissonian if for every $f \in \mathcal{C}_c^\infty(\mathbb{R}^{m-1})$ we have

$$\lim_{N \to \infty} R^{(m)}(N, d, \alpha, f) = \int_{\mathbb{R}^{m-1}} f(x) \, dx.$$

We say that the $m$-level correlation of the sequence $n^d \alpha \mod 1$ is Poissonian along a sequence $N_j \to \infty$ if for every $f \in \mathcal{C}_c^\infty(\mathbb{R}^{m-1})$ we have

$$\lim_{j \to \infty} R^{(m)}(N_j, d, \alpha, f) = \int_{\mathbb{R}^{m-1}} f(x) \, dx.$$

If the $m$-level correlation of $n^d \alpha \mod 1$ is Poissonian for any $m \geq 2$ along the same sequence $N_j \to \infty$, we simply say that $n^d \alpha \mod 1$ is Poissonian along $N_j$.

Given $\alpha$ and a sequence of rationals $b_j/q_j \to \alpha$, we say that $n^d \alpha \mod 1$ is Poissonian with respect to $(b_j/q_j)_{j \in \mathbb{N}}$ if there exists a sequence $\{N_j\}_{j \to \infty}$ with $\frac{\log N_j}{\log q_j} \to 1$ such that $n^d \alpha \mod 1$ is Poissonian along $N_j$.

We say that $\alpha$ is not of finite Diophantine type if there exists a sequence of triples $(b_j, q_j, k_j)$ of integers with $k_j \to \infty$ such that for every $j$ we have

$$\left| \alpha - \frac{b_j}{q_j} \right| \leq \frac{1}{q_j^{k_j}}. \tag{1.1}$$

Our main objective is to prove the following surprising result.

**Theorem 1.1.** Let $\alpha$ be an irrational number, not of finite Diophantine type, and let $(b_j, q_j)$ be a sequence such that $b_j/q_j \to \alpha$ as in (1.1). Then there are two alternatives:

1. Either $n^d \alpha \mod 1$ is Poissonian with respect to $(b_j/q_j)_{j \in \mathbb{N}}$ for every $d \geq 2$;
2. or $n^d \alpha \mod 1$ is Poissonian with respect to $(b_j/q_j)_{j \in \mathbb{N}}$ for no $d \geq 2$.

Here the hypothesis that $\alpha$ is not of finite Diophantine type is used only in passing from the distribution of $n^d \alpha \mod 1$ to the distribution of $n^d(b_j/q_j) \mod 1$. We point out that for different values of $d$, corresponding sequences $n^d(b_j/q_j) \mod 1$ have no obvious relations. Nevertheless, as we shall see later, the same exact obstruction to being Poissonian along a sequence applies simultaneously for all $d \geq 2$. 
2. A curve over a finite field

Studying the spacing distribution of sequences of the form $n^d b_j \pmod{q_j}$, $1 \leq n \leq N$, leads naturally to a point count on curves over finite fields. In this section we begin the investigation of such curves.

Let $q$ be a prime number, and let $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ denote the field with $q$ elements. We let $k = \overline{\mathbb{Z}_q}$ be the algebraic closure of $\mathbb{Z}_q$. Let $m, d$ be integers, with $m \geq 2, d \geq 2$. We will consider polynomials of degree $d$ in the ring $k[x_1, \ldots, x_m]$. Let $\mathbf{a} = (a_1, \ldots, a_{m-1}) \in k^{m-1}$. For $j = 1, \ldots, m-1$, we define $g_j \in k[x_1, \ldots, x_m]$ by

$$g_j := x_j^d - x_{j+1}^d - a_j.$$  \hfill (2.1)

Let $\mathcal{C}(d, \mathbf{a}, q)$ be the curve defined in $k^m$ by the system

$$g_j = 0, \quad j = 1, \ldots, m-1.$$  \hfill (2.2)

The goal of this section is to prove the following criterion for the irreducibility of $\mathcal{C}(d, \mathbf{a}, q)$.

**Proposition 2.1.** Assume that $q \nmid d$. Then the curve $\mathcal{C}(d, \mathbf{a}, q)$ is irreducible in $k^m$ if and only if, for $i = 1, \ldots, m-1$, the partial sums $A_i = \sum_{k=i}^{m-1} a_k$ are all distinct and non-zero.

We recall some notions from commutative algebra. The *lexicographic order* is an order $>$ on the monomials of $k[x_1, \ldots, x_m]$ such that $x_1^{\alpha_1} \cdots x_m^{\alpha_m} > x_1^{\beta_1} \cdots x_m^{\beta_m}$ exactly when the first non-zero entry of the vector $(\alpha_1 - \beta_1, \ldots, \alpha_m - \beta_m)$ is positive. For a polynomial $f \in k[x_1, \ldots, x_m]$, we call its maximal monomial with respect to the lexicographic order the *initial term*. We denote the initial term of $f$ by $\text{in}(f)$. For a subset $S$ of a polynomial ring $k[x_1, \ldots, x_m]$, we denote by $\langle S \rangle$ the ideal generated by $S$ in $k[x_1, \ldots, x_m]$.

**Definition 2.2.** Let $I$ be an ideal in $k[x_1, \ldots, x_m]$. A subset $G = \{g_1, \ldots, g_s\}$ of $I$ is called a *Gröbner basis* of $I$ (with respect to the lexicographic order) if

$$\langle \text{in}(f) \mid f \in I \rangle = \langle \text{in}(g_1), \ldots, \text{in}(g_s) \rangle.$$

**Lemma 2.3.** The set $G = \{g_1, \ldots, g_{m-1}\}$, where the $g_j$ are defined as in (2.1), is a Gröbner basis for the ideal $\langle g_1, \ldots, g_{m-1} \rangle$.

**Proof.** For $1 \leq i < j \leq m-1$, let $H_{ij}$ denote the $s$-polynomial of the pair $(g_i, g_j)$ (see [St98, Definition 2.6]). That is, $H_{ij}$ is the unique linear combination of $g_i$ and $g_j$ canceling the initial terms $\text{in}(g_i), \text{in}(g_j)$, and whose coefficients are relatively prime monic monomials in $k[x_1, \ldots, x_m]$. Hence,

$$H_{ij} = x_j^d (x_i^d - x_{i+1}^d - a_i) - x_i^d (x_j^d - x_{j+1}^d - a_j) = x_i^d x_j^d + a_j x_i^d - x_i^d x_{j+1}^d - a_i x_j^d.$$

Here and in the following computations, the monomial in boldface is the initial term. We now compute the remainder $R_G(H_{ij})$ of $H_{ij}$ by $G$ [St98, Definition 2.2]. Let $H^0 = H_{ij}$. For $k \geq 1$,
the polynomial $H^k$ is obtained by subtracting appropriate multiples of the elements of $G$ from $H^{k-1}$ in order to cancel its initial term in($H^{k-1}$). We thus get

$$H^1 = H^0 - x^d_{i+1}(a_i - x^d_{i+1} - a_i) = a_jx^d_i - x^d_{i+1}x^d_j + x^d_{i+1}x^d_j - a_ix^d_j + a_ix^d_{j+1},$$

$$H^2 = H^1 - a_j(x^d_i - x^d_{i+1} - a_i) = -x^d_{i+1}x^d_j + x^d_{i+1}x^d_j + a_jx^d_j - a_ix^d_j + a_ix^d_{j+1} + a_ia_j,$$

$$H^3 = H^2 + x^d_{i+1}(x^d_j - x^d_{i+1} - a_j) = -a_ix^d_j + a_ix^d_{j+1} + a_ia_j,$$

$$H^4 = H^3 + a_i(x^d_j - x^d_{j+1} - a_j) = 0.$$

Hence $R_G(H_{ij}) = 0$ for every $1 \leq i < j \leq m - 1$. The set $G$ is therefore a Gröbner basis by [St98, Proposition 2.7].

Let $R$ be an integral domain, and $I$ an ideal in the polynomial ring $R[x_1, \ldots, x_m]$. P. Gianni, B. Trager, and G. Zacharias [GTZ88] gave the following algorithm to check if $I$ is a prime ideal in $R[x_1, \ldots, x_m]$. (See also [AL94, Section 4 in Chapter 4]).

| ALGORITHM: Primality Test [AL94, Algorithm 4.4.1] |
|---------------------------------------------------|
| **Input:**  An ideal $I$ in $R[x_1, \ldots, x_m]$. |
| **Output:** TRUE if $I$ is a prime ideal, FALSE otherwise. |
| Set $R_{m+1} = R$, and $R_i := R[x_1, \ldots, x_i]$ for $i = 1, \ldots, m$. |
| Compute $J_i = I \cap R_i$ for $i = 1, \ldots, m + 1$. |
| If $J_{m+1}$ is not a prime ideal of $R$, **then** result:= FALSE. |
| Else result:= TRUE, $i := m + 1$. |
| **While** $i > 1$ **and** result=TRUE **do** |
| $R' := R_i/J_i$, |
| $J' :=$ image of $J_{i-1}$ in $R'[x_{i-1}]$, |
| $k' :=$ quotient field of $R'$. |
| Compute the polynomial $f$ such that $J'k'[x_{i-1}] = \langle f \rangle$. |
| **If** $f$ is not zero and reducible over $k'$, **then** result:= FALSE. |
| Else compute $J'k'[x_{i-1}] \cap R'[x_{i-1}]$. |
| **If** $J'k'[x_{i-1}] \cap R'[x_{i-1}] \neq J'$, **then** result:=FALSE. |
| Else $i := i - 1$. |
| **Return** result. |

We will apply the algorithm to prove that, under the appropriate assumptions on $a$, the ideal $I = \langle g_1, \ldots, g_{m-1} \rangle$ is prime in $k[x_1, \ldots, x_m]$. In our case, $R_{m+1} = k$, and $R_i = k[x_i, \ldots, x_m]$, for $i = 1, \ldots, m$. We now compute $J_i = I \cap R_i$. By Lemma 2.3 and [St98, Proposition 2.13]

$$J_i = \langle G \cap R_i \rangle, \quad i = 1, \ldots, m + 1.$$
In particular, 
\[ J_i = \begin{cases} 
\langle g_i, \ldots, g_{m-1} \rangle, & \text{if } i \in \{1, \ldots, m-1\}, \\
0, & \text{if } i \in \{m, m+1\}. 
\end{cases} \]

**Remark 2.4.** Note that \( I \cap k[x_j] = 0 \) for every \( j \). Indeed, if \( I \cap k[x_j] \neq 0 \) for some \( j \), then, looking at the generators \( g_i \) of \( I \), we see that \( I \cap k[x_j] \neq 0 \) for every \( j = 1, \ldots, m \). This contradicts \( J_m = I \cap k[x_m] = 0 \).

The algorithm requires studying, at every step, the (ir)reducibility of a polynomial \( f \) over an appropriate field. We will need the following standard result.

**Lemma 2.5.** Let \( F \) be an arbitrary field, \( n \geq 1 \), and \( a \in F \). Then \( x^n - a \) is irreducible over \( F \) if and only if \( a \notin F^p \) for all primes \( p \) dividing \( n \) and \( a \notin -4F^4 \) whenever \( 4 \mid n \).

**Proof.** See [K89, Theorem 2.6 on page 425].

**Proof of Proposition 2.1.** If the hypothesis on \( a \) is not satisfied, then \( a_i + a_{i+1} + \cdots + a_j = 0 \) for some \( 1 \leq i \leq j \leq m-1 \). Hence, in the system (2.2) defining our curve, we can replace the equation \( g_i = 0 \) with \( x_i^d - x_j^d = 0 \). Since the characteristic \( q \) of the field \( k \) does not divide \( d \), the polynomial \( x_i^d - x_j^d \) is the product of \( d \) distinct irreducible factors. In particular, the curve \( C(d, a, q) \) is reducible.

Conversely, assume that the sums \( A_i = \sum_{k=i}^{m-1} a_k \) are all distinct and non-zero. We prove that the ideal \( \langle g_1, \ldots, g_{m-1} \rangle \) is prime in \( k[x_1, \ldots, x_m] \). We argue by strong induction on \( m \).

First, consider the case \( m = 2 \). Following the algorithm, we obtain \( f = 0 \) for \( i = 3 \). At the second (and last) iteration, for \( i = 2 \), we have \( f = x_i^d - x_2^d - a_1 \), which is irreducible over the field \( k(x_2) \). Let \( p \) be a prime, with \( p \mid d \). Assume by contradiction that \( x_2^d + a_1 = \alpha^p \) for some \( \alpha \in k(x_2) \). Let \( \alpha = A/B \) for coprime polynomials \( A, B \in k[x_2] \). Hence,

\[ (B(x_2))^p(x_2^d + a_1) = (A(x_2))^p. \quad (2.3) \]

Let \( \theta \in k \) be such that \( \theta^d + a_1 = 0 \). Recall that \( a_1 \neq 0 \) by assumption. Hence, \( \theta \neq 0 \). It follows from (2.3) that \( A(\theta) = 0 \). Taking a derivative on both sides of (2.3), we obtain

\[ pB'(x_2)B(x_2) - (x_2^d + a_1) + B(x_2)^pdx_2^{d-1} = pA'(x_2)(A(x_2))^{p-1}. \quad (2.4) \]

Evaluating (2.4) at \( \theta \) yields

\[ (B(\theta))^p d\theta^{d-1} = 0. \quad (2.5) \]

Since \( \theta \neq 0 \) and \( d \) is not a multiple of the characteristic of \( k \), (2.5) implies \( B(\theta) = 0 \). We have now reached a contradiction, since \( A \) and \( B \) were taken to be coprime. Hence, \( x_2^d + a_1 \notin \langle k(x_2) \rangle^p \). By the same argument, \( x_2^d + a_1 \notin -4(k(x_2))^4 \) if \( 4 \mid d \). Lemma 2.5 then implies that \( x_2^d - x_j^d - a_1 \) is irreducible over \( k(x_2) \), and the proof of the case \( m = 2 \) is complete.

Let now \( m \geq 3 \), and assume that \( \langle g_1, \ldots, g_{j-1} \rangle \) is a prime ideal in \( k[x_1, \ldots, x_j] \) for every \( j \in \{1, \ldots, m-1\} \). We want to prove that \( \langle g_1, \ldots, g_{m-1} \rangle \) is a prime ideal in \( k[x_1, \ldots, x_m] \).
Running the primality algorithm, we see that the result follows if, for every \( i = 2, \ldots, m \), the polynomial \( f = x^d_{i-1} - x^d_i - a_{i-1} \) is irreducible over \( k' \), where \( k' \) is the quotient field of

\[
R' = \frac{k[x_i, \ldots, x_m]}{(x^d_i - x^d_{i+1} - a_i, \ldots, x^d_{m-1} - x^d_m - a_{m-1})}.
\]  

(2.6)

Note that \( R' \) is an integral domain by the inductive hypothesis. To prove the irreducibility of \( f \), we will use Lemma 2.5. Let \( p \) be a prime, with \( p \mid d \). Assume by contradiction that \( x^d_i + a_{i-1} = \alpha^p \), for some \( \alpha \in k' \). Let \( \bar{x}_j \) denote the equivalence class of \( x_j \) in \( k' \). Since the elements \( \bar{x}_i, \ldots, \bar{x}_{m-1} \) are algebraic over the field \( k(x_m) \), we have that \( k' = k(x_m)[\bar{x}_i, \ldots, \bar{x}_{m-1}] \).

We can thus find a representative of \( \alpha \in k' \) which is a polynomial in the variables \( x_i, \ldots, x_{m-1} \) with coefficients in \( k(x_m) \). After clearing denominators, we obtain a representation of \( \alpha \) as a quotient \( A(x_i, \ldots, x_m)/B(x_m) \), where \( A \in k[x_i, \ldots, x_m] \) and \( B \in k[x_m] \). The equality \( x^d_i + a_{i-1} = \alpha^p \) in \( k' \) yields

\[
(B(x_m))^p(x^d_i + a_{i-1}) - (A(x_i, \ldots, x_m))^p \in (x^d_i - x^d_{i+1} - a_i, \ldots, x^d_{m-1} - x^d_m - a_{m-1}).
\]  

(2.7)

We can assume without loss of generality that \( A \) is of degree at most \( d - 1 \) in the variables \( x_{i+1}, \ldots, x_m \). Hence,

\[
(B(x_m))^p(x^d_i + a_{i-1}) - \left( \sum_{1 \leq j_1 + \ldots + j_m \leq d} c_{j_1 + \ldots + j_m}(x_i)x^{j_1}_{i+1} \cdots x^{j_m}_m \right)^p = \sum_{j=i}^{m-1} f_j \cdot (x^d_j - x^d_{j+1} - a_j)
\]  

(2.8)

for some polynomials \( f_j \in k[x_i, \ldots, x_m] \) and \( c_{j_1 + \ldots + j_m} \in k[x_i] \). Now let \( (\theta_i, \ldots, \theta_m) \in k^m \) satisfying

\[
\begin{align*}
\theta_i^d &= -a_{i-1}, \\
\theta_{i+1}^d &= -a_{i-1} - a_i, \\
&\vdots \\
\theta_{m-1}^d &= -a_{i-1} - a_i - \cdots - a_{m-2}, \\
\theta_m^d &= -a_{i-1} - a_i - \cdots - a_{m-2} - a_{m-1}.
\end{align*}
\]  

(2.9)

By our hypotheses on \( a \), the sums of the \( a_j \) appearing in (2.9) are never equal to zero. Moreover, since \( d \) is not a multiple of the characteristic of the base field \( k \), there are \( d \) distinct values for every \( \theta_j \). Substituting \( \theta_i, \ldots, \theta_m \in k \) satisfying (2.9) in (2.8) gives \( A(\theta_i, \ldots, \theta_m) = 0 \). Note that \( A(\theta_i, \ldots, \theta_{m-1}, x_m) \) is a polynomial of degree at most \( d - 1 \) in \( x_m \) with \( d \) distinct roots in \( k \). Hence each of its coefficients must be equal to zero. Fixing \( \theta_i, \ldots, \theta_{m-2} \) in each of those coefficients, we obtain polynomials of degree at most \( d - 1 \) in \( x_{m-1} \) with \( d \) roots in \( k \). Inductively, we conclude that every polynomial \( c_{j_1 + \ldots + j_m}(x_i) \) appearing in (2.8) must vanish for all \( \theta_i \) such that \( \theta_i^d = -a_{i-1} \). It follows that \( A(x_i, \ldots, x_m) = (x^d_i + a_{i-1})V(x_i, \ldots, x_m) \) for some \( V \in k[x_i, \ldots, x_m] \). From (2.7) we thus get

\[
(x^d_i + a_{i-1}) \left( (B(x_m))^p - (V(x_i, \ldots, x_m))^p (x^d_i + a_{i-1})^{p-1} \right) \in (x^d_i - x^d_{i+1} - a_i, \ldots, x^d_{m-1} - x^d_m - a_{m-1}).
\]
The ideal \((x_i^d - x_{i+1}^d - a_i, \ldots, x_m^d - x_m^d - a_m)\) is prime in \(k[x_i, \ldots, x_m]\) by the inductive hypothesis. Remark 2.4 then implies

\[
(B(x_m))^p - (V(x_i, \ldots, x_m)) = \sum_{j=1}^{m-1} h_j \cdot (x_j^d - x_{j+1}^d - a_j)
\]

(2.10)

for some polynomials \(h_j \in k[x_i, \ldots, x_m]\). Substituting in (2.10) elements \(\theta_1, \ldots, \theta_m \in k\) that satisfy (2.9), we obtain \(B(\theta_m) = 0\) for every \(\theta_m\) such that \(\theta_m = -a_i - \cdots - a_m\). Therefore

\[
B(x_m) = W(x_m)(x_m^d + a_m - \cdots + a_m)
\]

for some polynomial \(W \in k[x_m]\). Note that \(x_m^d + a_m - \cdots + a_m = x_i^d + a_i\) in \(k'\), and therefore the elements \(A\) and \(B\) representing \(\alpha\) have a common factor in \(R'\). We can thus remove this common factor and write \(\alpha = \bar{A}(x_i, \ldots, x_m)/\bar{B}(x_m)\), where \(\bar{A} \in k[x_i, \ldots, x_m]\) and \(\bar{B} \in k[x_m]\) are polynomials whose degrees satisfy \(\deg \bar{A} = \deg A - d\), \(\deg \bar{B} = \deg B - d\). Repeating the reasoning above with \(A\) and \(B\) replaced by \(\bar{A}\) and \(\bar{B}\) respectively, we deduce that \(\bar{A}\) and \(\bar{B}\) again share a common factor in \(R'\). We remove that common factor, and repeat the same argument once more. After finitely many steps, we reach a contradiction. We have thus proved that \(x_i^d + a_i \not\in (k')^p\). With the same argument, one can show that \(x_i^d + a_i \not\in -4(k')^4\) if \(4 \mid d\). Lemma 2.5 then implies that \(f = x_i^{d} - x_i^d - a_i - 1\) is irreducible over \(k'\), as wanted. \(\square\)

3. Point count on the curve

Let \(b, d, q\) be positive integers, with \(d \geq 2\) and \((b, q) = 1\). Let \(a = (a_1, \ldots, a_{m-1}) \in Z_q^{m-1}\). Define

\[
\nu(d, a, q) = \# \{ x \in Z_q^m : bx_i^d - bx_{i+1}^d = a_i (\text{mod } q), 1 \leq i \leq m - 1 \}.
\]

(3.1)

Remark 3.1. When \(q\) is a prime, the quantity \(\nu(d, a, q)\) corresponds to the number of points in \(Z_q^m\) of the curve \(\mathcal{C}(d, a\bar{b}, q)\), following the notation of Section 2. Here \(\bar{b} \in Z_q\) is such that \(b\bar{b} = 1\), and \(a\bar{b}\) is the element \((a_1\bar{b}, \ldots, a_{m-1}\bar{b}) \in Z_q^{m-1}\).

Notation 3.2. From now on we use the notation \(\mathcal{C}(d, a\bar{b}, q)\) even when \(q\) is not prime (but still \((b, q) = 1\)) to indicate the curve consisting of the points \((x_1, \ldots, x_m)\) satisfying the equations \(bx_i^d - bx_{i+1}^d = a_i (\text{mod } q)\) for \(1 \leq i \leq m - 1\).

Let \(q = \prod_{j=1}^r p_j^e_j\) be a prime factorization of \(q\). By the Chinese Remainder Theorem,

\[
\nu(d, a, q) = \prod_{j=1}^r \nu(d, a, p_j^{e_j}).
\]

(3.2)

For every \(j \in \{1, \ldots, r\}\), we define the number \(A(d, a, p_j^{e_j})\) by

\[
A(d, a, p_j^{e_j}) = \nu(d, a, p_j^{e_j}) - p_j^{e_j}.
\]
Equation (3.2) yields
\[ \nu(d, a, q) = \prod_{j=1}^{r} (p_j^{e_j} + A(d, a, p_j^{e_j})) = q \prod_{j=1}^{r} \left( 1 + \frac{A(d, a, p_j^{e_j})}{p_j^{e_j}} \right) = q \sum_{S \subseteq \{1, \ldots, r\}} \frac{A(d, a, c_S)}{c_S}, \] (3.3)
where for each non-empty subset \( S \subseteq \{1, \ldots, r\} \) we let
\[ c_S = \prod_{j \in S} p_j^{e_j}, \quad A(d, a, c_S) = \prod_{j \in S} A(d, a, p_j^{e_j}), \]
and \( c_S = 1 \) for \( S = \emptyset \).

In the next lemma we will establish a bound for \( |A(d, a, c_S)| \). Following [KR99], for a prime \( p \) and \( a = (a_1, \ldots, a_{m-1}) \), we denote by \( r_{\text{eff}}(a, p) \) the number of distinct components of an element \( y = (y_1, \ldots, y_m) \) satisfying
\[ y_i - y_{i+1} = a_i \pmod{p}, \quad 1 \leq i \leq m-1. \] (3.4)
This number is well defined, independent of the particular solution. For \( 1 \leq i < j \leq m \), let
\[ \sigma_{ij}(a) = \sum_{k=i}^{j-1} a_k, \]
so that \( \sigma_{i+1}(a) = a_i, \sigma_{ij} = \sum_{k=i}^{j-1} \sigma_{k+1} \). Let \( D(a) = \prod_{1 \leq i \leq j \leq m} \sigma_{ij}(a) \). A solution of the system (3.4) has distinct components (that is, \( r_{\text{eff}}(a, p) = m \)) if and only if \( p \) does not divide \( D(a) \), since \( y_i - y_j = \sum_{k=i}^{j-1} (y_k - y_{k+1}) = \sum_{k=i}^{j-1} a_k = \sigma_{ij}(a) \).

**Lemma 3.3.** Let \( \tilde{q} \) be the squarefree part of \( q \). Assume that there exists \( \delta > 0 \) such that \( \tilde{q} \geq q^{1-\delta} \). Then, for every subset \( S \subset \{1, \ldots, r\} \), we have
\[ |A(d, a, c_S)| \ll_{m,d,\epsilon} c_S^{1/2+\epsilon}(c_S, D(a))^{1/2}q^{\delta m}. \]

**Proof.** First we consider the case of \( c = p \) prime with \( p \nmid d \). Applying the Riemann Hypothesis for curves over finite fields (see [W48] and [Sc76, Theorem 5A and Corollary 5B]) as in [KR99, Proposition 4], we obtain
\[ \nu(d, a, p) = d^{m-r_{\text{eff}}(a,p)}(p+B(a,p)), \quad \text{with } |B(a,p)| \ll_m p^{1/2}. \] (3.5)
We use estimate (3.5) for the primes \( p_j \) such that \( e_j = 1 \) and \( p_j \nmid d \). For the other primes, we use the trivial estimate
\[ |A(d, a, p_j^{e_j})| \leq p_j^{e_j m}. \] (3.6)
Note that since \( \tilde{q} \geq q^{1-\delta} \) it follows that
\[ \prod_{j \in S, e_j \geq 2} p_j^{e_j} \leq q^{2\delta m}. \] (3.7)
Multiplying the inequalities in (3.5) and (3.6), using (3.7), and recalling that \( \# S \ll m, d, \epsilon \), we obtain

\[
|A(d, a, c_S)| = \prod_{j \in S, e_j = 1, p_j \nmid d} |A(d, a, p_j)| \prod_{j \in S, e_j \geq 2 \text{ or } p_j \nmid d} |A(d, a, p_j^{e_j})| \\
\leq \prod_{j \in S, e_j = 1, p_j \nmid d} C_{m, d} p_j^{1/2} (p_j, D(a))^{1/2} \prod_{j \in S, e_j \geq 2} p_j^{e_j m} \prod_{e_j = 1, p_j \nmid d} p_j^{e_j m}.
\]

\[
\leq C_{m, d, \epsilon} c_S^{1/2 + \epsilon} (c_S, D(a))^{1/2} q^{2\delta_m},
\]

which concludes the proof of the lemma. \(\square\)

**Lemma 3.4.** For every \( c > 1 \),

\[
\sum_{a \pmod{c}} A(d, a, c) = 0.
\]

**Proof.** For every prime \( p \),

\[
\sum_{a \pmod{p}} \nu(d, a, p) = \sum_{x \pmod{p}} \sum_{a \pmod{p}} 1 = p^m. \tag{3.8}
\]

By definition of \( A(d, a, p) \),

\[
\sum_{a \pmod{p}} \nu(d, a, p) = \sum_{a \pmod{p}} (p + A(d, a, p)) = p^m + \sum_{a \pmod{p}} A(d, a, p). \tag{3.9}
\]

Combining (3.8) and (3.9) we obtain

\[
\sum_{a \pmod{p}} A(d, a, p) = 0.
\]

The result now follows from the multiplicativity of the above sums. \(\square\)

4. A CONVERGENCE THEOREM

The goal of this section is proving the following result.

**Theorem 4.1.** Let \( d \geq 2 \). Fix \( m \geq 2 \) and \( 0 < \delta_0 < \frac{1}{4m} \). There exists \( \delta = \delta(m, \delta_0) > 0 \) such that for every \( f \in C_c^\infty(R^{m-1}) \) one has

\[
R^{(m)} \left( N, d, \frac{b}{q}, f \right) \to \int_{R^{m-1}} f(x) \, dx
\]

uniformly for \( (b, q) = 1, q^{1-1/(2m)+\delta_0} \leq N \leq q^{1-\delta_0} \), as \( q \to \infty \) such that \( \bar{q} \geq q^{1-\delta} \).
Following [Z03, Section 4], we reduce the proof of Theorem 4.1 to a point count on a curve over a finite field. We then prove Theorem 4.1 using the results of Sections 2 and 3.

By approximating \( f \) from above and below by step functions, it is enough to prove the statement for the characteristic function of a compact set with piecewise smooth boundary \( I \subseteq \mathbb{R}^{m-1} \). Given \( b \) and \( q \) as in the hypotheses, we thus want to show, for \( q \rightarrow \infty \), that

\[
NR^{(m)}(N, d, b/q, I) \rightarrow \text{vol}(I),
\]

where \( NR^{(m)}(N, d, b/q, I) \) is the number of \( m \)-tuples \((x_1, \ldots, x_m)\) with distinct components \( x_1, \ldots, x_m \) in \( \{1, \ldots, N\} \) such that

\[
N\left(\left\{ \frac{bx_1^d}{q} \right\} - \left\{ \frac{bx_2^d}{q} \right\}, \ldots, \left\{ \frac{bx_{m-1}^d}{q} \right\} - \left\{ \frac{bx_m^d}{q} \right\} \right) \in I.
\]

We can write \( R^{(m)}(N, d, b/q, I) \) in the form

\[
R^{(m)}(N, d, b/q, I) = \frac{1}{N} \sum_{a \in sI}^* \nu(N, d, a, q),
\]

where \( s = q/N \) is the dilate factor and

\[
\nu(N, d, a, q) = \#\{1 \leq x_i \leq N : bx_i^d - bx_{i+1}^d = a_i \pmod q, 1 \leq i \leq m-1\}.
\]

Here the star in (4.2) denotes summation over the vectors \( a \) for which the partial sums \( A_i = \sum_{k \geq i} a_k \) are all distinct and non-zero, a condition which comes from the requirement that the \( m \)-tuples \((x_1, \ldots, x_m)\) to be counted in \( R^{(m)}(N, d, b/q, I) \) have distinct components.

**Lemma 4.2.** We have

\[
R^{(m)}(N, d, b/q, I) = \frac{1}{Nq^m} \sum_{a \in sI} \sum_{r \pmod q} \sum_{y \in C(d, a\bar{b}, q)} e \left( \frac{-r \cdot y}{q} \right) \prod_{i=1}^m \sum_{1 \leq x_i \leq N} e \left( \frac{r_i x_i}{q} \right),
\]

where \( q \) are assumed to lie in the interval \( \left[-\frac{q}{2}, \frac{q}{2}\right] \).

To prove (4.1), we first consider the contribution of \( r = 0 \) on the right side of (4.3). We obtain the term

\[
\mathcal{M} = \frac{N^{m-1}}{q^m} \sum_{a \in sI}^* \nu(d, a, q),
\]

where \( \mathcal{M} \) is the sum of the contributions of \( r = 0 \).
where \( \nu(d, a, q) \) is the quantity defined in (3.1). We let

\[
\mathcal{E} = R(m)(N, d, b/q, I) - \mathcal{M}.
\]

(4.5)

Theorem 4.1 follows from the two lemmas below.

**Lemma 4.3.** As \( q \to \infty \), we have \( \mathcal{M} = \text{vol}(I) + o(1) \).

**Lemma 4.4.** As \( q \to \infty \), we have \( \mathcal{E} = o(1) \).

**Proof of Lemma 4.3.** By (3.3) we can rewrite \( \mathcal{M} \) as

\[
\mathcal{M} = \frac{N^{m-1}}{q^{m-1}} \sum_{S \subseteq \{1, \ldots, r\}} \frac{1}{c_S} \sum_{a \in sI} A(d, a, c_S).
\]

Recall that by definition \( c_S = 1 \) when \( S = \emptyset \). The contribution of \( S = \emptyset \) is therefore

\[
\left( \frac{N}{q} \right)^{m-1} \sum_{a \in sI} 1 = \frac{1}{s^{m-1}} \# \{(sI)^* \cap \mathbb{Z}^{m-1}\} = \text{vol}(I) + O\left(\frac{1}{s}\right),
\]

where \((sI)^*\) is the set of vectors \( a \in sI \) with all the partial sums \( A_i \) distinct and non-zero.

For the remaining divisors \( c_S \) of \( q \) we distinguish two cases. Let \( \mathfrak{A} \) be the set of all subsets \( S \subseteq \{1, \ldots, r\} \) for which \( c_S > s_1 \), and let \( \mathfrak{B} \) be the set of all \( S \subseteq \{1, \ldots, r\} \) for which \( 1 < c_S < s_1 \). Here \( s_1 \) is a parameter that will be chosen later. By Lemma 3.3,

\[
\frac{1}{s^{m-1}} \sum_{S \in \mathfrak{A}} \frac{1}{c_S} \sum_{a \in sI} A(d, a, c_S) \ll_{m, d, \varepsilon, t} \frac{1}{s^{m-1}} \sum_{S \in \mathfrak{A}} \frac{1}{c_S^{1/2+\varepsilon}} \sum_{a \in sI} (c_S, D(a))^{1/2} q^{2\delta m}
\]

\[
= \frac{1}{s^{m-1}} \sum_{S \in \mathfrak{A}} c_S^{-1/2} q^{2\delta m} \sum_{t \mid c_S} t^{1/2} \# \{a \in sI: (c_S, D(a)) = t\}
\]

\[
\leq \frac{1}{s^{m-1}} \sum_{S \in \mathfrak{A}} c_S^{-1/2} q^{2\delta m} \sum_{t \mid c_S} t^{1/2} \#(J(t)),
\]

where \( J(t) = \{a \in sI: t \mid D(a)\} \). One can easily see that

\[
\#(J(t)) \ll_{m, d, \varepsilon, t} t^{\epsilon} s^{m-1} \left(\frac{1}{t} + \frac{1}{s}\right).
\]

(4.7)

Equations (4.6) and (4.7) yield

\[
\frac{1}{s^{m-1}} \sum_{S \in \mathfrak{A}} \frac{1}{c_S} \sum_{a \in sI} A(d, a, c_S) \ll_{m, d, \varepsilon, t} \sum_{S \in \mathfrak{A}} c_S^{-1/2} \sum_{t \mid c_S} q^{2\delta m} t^{1/2+\varepsilon} \left(\frac{1}{t} + \frac{1}{s}\right) = \sigma_1 + \sigma_2,
\]

where

\[
\sigma_1 = \sum_{S \in \mathfrak{A}} c_S^{-1/2} \sum_{t \mid c_S} q^{2\delta m} t^{-1/2+\varepsilon} \leq q^{2\delta m} s_1^{-1/2} \# \{ (c_S, t): t \mid c_S \mid q \} \leq q^{2\delta m+2\varepsilon} s_1^{-1/2},
\]

(4.8)
\[
\sigma_2 = \sum_{S \in \mathfrak{S}} c_S^{\varepsilon-1/2} \sum_{t \mid c_S} q^{2\delta m} t^{1/2+\varepsilon} \frac{1}{s} \leq \frac{1}{s} \sum_{c_S \mid q} \sum_{t \mid c_S} q^{2\delta m} (t c_S)^{\varepsilon} \left( \frac{t}{c_S} \right)^{1/2} \leq \frac{1}{s} q^{4\varepsilon+2\delta m}. \tag{4.9}
\]

Equation (4.9) shows that \( \sigma_2 = o(1) \) as \( q \to \infty \) for \( \delta \) small enough in terms of \( m \). Letting \( s_1 = \sqrt{s} \), we see from (4.8) that
\[
\sigma_1 \leq s^{\varepsilon/2-1/4} q^{2(\delta m+\varepsilon)}. \tag{4.10}
\]

Since \( s = q/N \geq q^{\delta_0} \), the inequality (4.10) implies that \( \sigma_1 = o(1) \) as \( q \to \infty \) for \( \delta \) small enough in terms of \( m \) and \( \delta_0 \).

We now consider the divisors \( c_S \) of \( q \) such that \( 1 < c_S < s_1 = \sqrt{s} \). Recall that we denote by \((sI)^*\) the set of vectors \( a \in sI \) such that all the partial sums \( A_i \) are distinct and non-zero. We divide the region \((sI)^*\) into integer cubes of side \( c_S \) of the form \( y + c_S B \), where \( y \in c_S \mathbb{Z}^{m-1} \) and \( B = \{ 0 \leq x_i < 1 \} \) is the unit cube in \( \mathbb{R}^{m-1} \). We call a cube \( c_S\text{-interior} \) if it is entirely contained in \((sI)^*\). By the Lipschitz principle (see [D51]) it follows that the number \( n_{c_S} \) of \( c_S\text{-interior} \) cubes is given by
\[
n_{c_S} = \text{vol} \left( \frac{s}{c_S} \right) + O_I \left( \left( \frac{s}{c_S} \right)^{m-2} \right) = \left( \frac{s}{c_S} \right)^{m-1} \text{vol}(I) + O_{I} \left( \left( \frac{s}{c_S} \right)^{m-2} \right).
\]

We say that a point \( a \in sI \cap \mathbb{Z}^{m-1} \) is \( c_S\text{-interior} \) if it is contained in a \( c_S\text{-interior} \) cube, and is \( c_S\text{-boundary} \) otherwise. Each interior cube contains \( c_S^{m-1} \) \( c_S\text{-interior} \) points, so the total number of \( c_S\text{-interior} \) points is
\[
c_S^{m-1} n_{c_S} = s^{m-1} \text{vol}(I) + O(c_S s^{m-2}). \tag{4.11}
\]

The total number of points of \( sI \cap \mathbb{Z}^{m-1} \) is \( s^{m-1} \text{vol}(I) + O(s^{m-2}) \). Subtracting the number of \( c_S\text{-interior} \) points given by (4.11), we obtain that the number of \( c_S\text{-boundary} \) points is \( O(c_S s^{m-2}) \).

For every divisor \( c_S \) of \( q \), with \( S \in \mathfrak{B} \), we write
\[
\sum_{a \in sI}^* A(d, a, c_S) = \sum_{a \in c_S\text{-boundary}}^* A(d, a, c_S) + \sum_{a \in c_S\text{-interior}}^* A(d, a, c_S).
\]

Since the sum over each \( c_S\text{-interior} \) cube is just a sum over \((\mathbb{Z}/c_S \mathbb{Z})^{m-1}\), Lemma 3.4 implies
\[
\sum_{a \in sI}^* A(d, a, c_S) = \sum_{a \in c_S\text{-boundary}}^* A(d, a, c_S).
\]

By Lemma 3.3 and the fact that the number of \( c_S\text{-boundary} \) points is \( O(c_S s^{m-2}) \) we obtain
\[
\frac{1}{s^{m-1}} \sum_{S \in \mathcal{B}} \left( \sum_{c \in S}^* A(d, a, c_S) \right) \sum_{a \in \mathcal{I}} A(d, a, c_S) = \frac{1}{s^{m-1}} \sum_{S \in \mathcal{B}} \sum_{c \in S}^* A(d, a, c_S) \sum_{a \in \mathcal{I}}^* A(d, a, c_S)
\]

\[
\ll_{d, m, \varepsilon} s^{m-1} \sum_{S \in \mathcal{B}} c_S \sum_{a \in \mathcal{I}} A(d, a, c_S) \ll_{\varepsilon} s^{2+\varepsilon} s^{m-2} q^{2\delta m} = \frac{1}{s} \sum_{S \in \mathcal{B}} s^{1+\varepsilon} q^{4\delta m}
\]

which is \(o(1)\) as \(q \to \infty\) for \(\delta\) small enough in terms of \(m\) and \(\delta_0\). This concludes the proof of Lemma 4.3.

\[\square\]

**Proof of Lemma 4.4.** By (4.3), (4.4) and (4.5),

\[
\mathcal{E} = \frac{1}{N q^m} \sum_{a \in \mathcal{I}}^* \sum_{r \pmod{q}} \sum_{y \in \mathcal{C}(d, a, b, q)} e\left( -\frac{r \cdot y}{q} \right) \prod_{i=1}^{m} \sum_{1 \leq x_i \leq N} e\left( \frac{r_i x_i}{q} \right)
\]

\[
\ll_{\varepsilon} q^{2\delta m} \frac{1}{s} \sum_{s^1 \{c_S \mid q\} \ll s^{-1/2+\varepsilon/2} q^{\varepsilon+2\delta m} \leq q^{-\delta_0/2+\varepsilon}\delta_0/2+\varepsilon+2\delta m},
\]

(4.12)

We start by observing that, if \(q = \prod_{j} p_j^{k_j}\) is the decomposition of \(q\) into primes, then (see [Z03] for details)

\[
\sum_{y \in \mathcal{C}(d, a, b, q)} e\left( -\frac{r \cdot y}{q} \right) = \prod_{j} \sum_{y \in \mathcal{C}(d, a, b, p_j^{k_j})} e\left( -\frac{b_j r \cdot y}{p_j^{k_j}} \right),
\]

(4.13)

where the \(b_j\) are given by

\[
b_j = \prod_{i \neq j} p_i^{-k_i} (\text{mod } p_j^{k_j}).
\]

We use the trivial bound

\[
\left| \sum_{y \in \mathcal{C}(d, a, b, p_j^{k_j})} e\left( -\frac{b_j r \cdot y}{p_j^{k_j}} \right) \right| \leq p_j^{m k_j}
\]

for the factors on the right side of (4.13) for which \(k_j \geq 2\). Since \(\tilde{q} \leq q^{1-\delta}\), we obtain

\[
\left| \prod_{k_j \geq 2} \sum_{y \in \mathcal{C}(d, a, b, p_j^{k_j})} e\left( -\frac{b_j r \cdot y}{p_j^{k_j}} \right) \right| \leq \prod_{k_j \geq 2} p_j^{m k_j} \leq q^{2\delta m}.
\]

(4.14)
We consider those primes $p_j$ for which $k_j = 1$. For such primes $p_j$ which divide $d$, we have the trivial bound
\[
\prod_{k_j=1}^{\text{prime divisors of } d} \sum_{y \in C(d,ab,p_j)} e\left(-\frac{b_j r \cdot y}{p_j}\right) \leq d^m. \tag{4.15}
\]

Next, for primes $p_j \mid d$, we use the Bombieri-Weil inequality [B66, Theorem 6], which gives
\[
\left| \sum_{y \in C(d,ab,p_j)} e\left(-\frac{b_j r \cdot y}{p_j}\right) \right| \leq m \frac{p_j^{1/2}}{d} \tag{4.16}
\]
provided that the partial sums $A_i$ are distinct mod $p_j$. We can apply (4.16) only if $y \cdot r$ is not constant on any component of the curve $C(d,ab,p_j)$. Note that Proposition 2.1 guarantees that every curve $C(d,ab,p_j)$ is irreducible. In the next paragraph we prove that if $y \cdot r$ is constant on a curve $C(d,ab,p_j)$ then $r = 0$, which is never the case for the terms considered in Lemma 4.4 (see (4.12)).

Let $k = \overline{\mathbb{Z}}_{p_j}$ denote the algebraic closure of the field $\mathbb{Z}_{p_j} = \mathbb{Z}/p_j\mathbb{Z}$. Then, in the function field $k(Y_1,\ldots,Y_m)$ of the curve $C(d,ab,p_j)$, $Y_1$ is a variable and $Y_2,\ldots,Y_m$ are algebraic functions such that
\[
Y_i^d = Y_1^d - (a_1 + \cdots + a_{i-1})b \quad \text{for } 2 \leq i \leq m.
\]

Recall that the key step in the proof of Proposition 2.1 was to show the irreducibility of some polynomials (there denoted by $f$) over some quotient fields (see (2.6)). The same exact argument shows, for every $i \in \{2,\ldots,m\}$, that the polynomial
\[
x^d - (Y_1^d - (a_1 + \cdots + a_{i-1})b)
\]
is irreducible in the ring $k(Y_1,\ldots,Y_{i-1})[x]$. It follows that
\[
[k(Y_1,\ldots,Y_m) : k(Y_1)] = d^{m-1}. \tag{4.18}
\]

Assume now by contradiction that $y \cdot r = c$, with $c \in k$ and $r \neq 0$. Let $j_0 \in \{1,\ldots,m\}$ be such that $r_{j_0} \neq 0$. Then $Y_{j_0}$ belongs to $k(Y_1,\ldots,Y_{j_0-1},Y_{j_0+1},\ldots,Y_m)$, and therefore
\[
k(Y_1,\ldots,Y_m) = k(Y_1,\ldots,Y_{j_0-1},Y_{j_0+1},\ldots,Y_m). \tag{4.19}
\]

Applying again the irreducibility of the polynomials in (4.17) we obtain
\[
[k(Y_1,\ldots,Y_{j_0-1},Y_{j_0+1},\ldots,Y_m) : k(Y_1)] = d^{m-2},
\]
which, together with (4.19), contradicts (4.18). We thus conclude that for the primes $p_j \mid d$ such that the sums $A_i$ are distinct mod $p_j$, the inequality (4.16) holds true.

Now, in general, for each pair of $a$ and $p_j$, we have a partition $\mathcal{P} = \{V_1,\ldots,V_L\}$ of the set $V = \{1,2,\ldots,m\}$ where $A_{i_1} = A_{i_2} \pmod{p_j}$ if and only if $i_1, i_2 \in V_{\ell'}$ for some $1 \leq \ell' \leq \ell$. 


Using this partition, for each \( r \) we write \( r \cdot y \) as
\[
 r \cdot y = \sum_{\ell' = 1}^{\ell} \sum_{i \in V_{\ell'}} r_i y_i.
\]
By the definition of \( P \), if \( 1 \leq i_1 \neq i_2 \leq m \) belong to the same set, then the equation
\[
 x_{i_1}^d - x_{i_2}^d = 0 \pmod{p_j} \tag{4.20}
\]
is one of the equations defining the curve \( C(d, \overline{a}b, p_j) \).

Let \( \gamma_j = (d, p_j - 1) \). Since \( \gamma_j \mid (p_j - 1) \), there exists a \( \gamma_j \)-th primitive root of unity mod \( p_j \), say \( \alpha_j \). Then equation (4.20) gives
\[
 x_{i_2} = \alpha_j^t x_{i_1}, \quad 0 \leq t \leq \gamma_j - 1. \tag{4.21}
\]
Replacing (4.20) by (4.21), we can regard \( C(d, \overline{a}b, p_j) \) as the union of \( \gamma_j \) curves. Repeating this process for all such pairs \( i_1 \) and \( i_2 \), we see that \( C(d, \overline{a}b, p_j) \) is a union of \( \gamma_j \) curves. Note that we can apply (4.16) provided that \( r \cdot y \) is nonconstant along any of these curves. The exception occurs when there exists a function \( \theta : V \to \{1, \alpha_j, \ldots, \alpha_{\gamma_j - 1}\} \) such that for any \( 1 \leq \ell' \leq \ell \), we have
\[
 \sum_{i \in V_{\ell'}} \theta(i) r_i = 0 \pmod{p_j}. \tag{4.22}
\]
In this case, we use the following trivial bound instead of (4.16):
\[
 \left| \sum_{y \in C(d, \overline{a}b, p_j)} e\left( - \frac{b_j r \cdot y}{p_j} \right) \right| \ll_{m, d} p_j. \tag{4.23}
\]
For fixed \( a \) and \( r \), we denote by \( D(a, r) \) the product of the prime factors \( p_j \) of \( q \) for which \( k_j = 1 \) and (4.22) holds for some \( \theta \). By (4.13), (4.14), (4.15), (4.16), and (4.23), we obtain
\[
 \sum_{y \in C(d, \overline{a}b, q)} e\left( - \frac{r \cdot y}{q} \right) \ll_{\delta, m, d} q^{2\delta m + 1/2} D(a, r)^{1/2} c_{m, d}^{\omega(q)} \tag{4.24}
\]
where \( \omega(q) \) is the number of prime divisors of \( q \), and \( c_{m, d} \) is a constant depending on \( m \) and \( d \). Since \( q \to \infty \), we can assume \( c_{m, d}^{\omega(q)} \leq q^{\delta m} \). Hence, putting (4.24) into (4.12) yields the following:
\[
 E \ll_{\delta, m, d} \frac{q^{1/2 + 3\delta m - m}}{N} \sum_{r \pmod{q} \atop r \neq 0} \prod_{i=1}^{m} \min \left\{ N, \frac{q}{|r_i|} \right\} \sum_{a \in sI} D(a, r)^{1/2} \]
\[
 \ll q^{1/2 + 3\delta m} \sum_{r \pmod{q} \atop r \neq 0} \prod_{i=1}^{m} \min \left\{ \frac{1}{s}, \frac{1}{|r_i|} \right\} \sum_{D \mid q} D^{1/2} N(D),
\]
where \( N(D) := \#\{a \in (sI)^* : D(a, r) = D\} \). If we let \( \rho(r, D) \) be the proportion of integer vectors \( a \) in \((sI)^*\) such that \( D(a, r) = D \), then

\[
N(D) \sim \rho(r, D)s^{m-1}\text{vol}(I).
\]

Thus, it follows that

\[
\mathcal{E} \ll_{\delta, m, d, I} q^{-1/2+3\delta} s^m \sum_{D|\tilde{q}} D^{1/2} \sum_{\substack{r \pmod{q} \atop r \neq 0}} \rho(r, D) \prod_{i=1}^m \min \left\{ \frac{1}{s}, \frac{1}{|r_i|} \right\}.
\]  \quad (4.25)

In order to prove Lemma 4.4, we show the following:

\[
D^{1/2} \sum_{\substack{r \pmod{q} \atop r \neq 0}} \rho(r, D) \prod_{i=1}^m \min \left\{ \frac{1}{s}, \frac{1}{|r_i|} \right\} \ll_{\delta_0, m, d, I} q^{1/2-\delta_0} s^{-m}.
\]  \quad (4.26)

Note that the number of divisors \( D \) of \( \tilde{q} \) is \( \ll q^\epsilon \). Thus, for \( \delta \) small enough in terms of \( m \) and \( \delta_0 \), (4.26) implies

\[
\mathcal{E} \ll_{\delta, \delta_0, m, d, I} q^{-\delta_0/2},
\]

which completes the proof of the lemma.

Now, for a nonempty subset \( \mathcal{L} \) of \( V = \{1, 2, \ldots, m\} \), we let \( \sum(\mathcal{L}) \) denote the sum on the left-hand side of (4.26) over the vectors \( r \pmod{q} \) such that \( r_i \neq 0 \) if and only if \( i \in \mathcal{L} \). There are \( 2^m - 1 \) such subsums \( \sum(\mathcal{L}) \), and therefore it suffices to show, for each \( \mathcal{L} \), that

\[
\sum(\mathcal{L}) \ll_{m, \delta_0, d, I} D^{-1/2} q^{1/2-\delta_0} s^{-m}.
\]  \quad (4.27)

For convenience, we can assume that \( \mathcal{L} = \{1, 2, \ldots, L\} \) for some \( 1 \leq L \leq m \). It follows that

\[
\sum(\mathcal{L}) = \sum_{0 < |r_1|, \ldots, |r_L| \leq q/2} \rho(r, D) \prod_{i=1}^m \min \left\{ \frac{1}{s}, \frac{1}{|r_i|} \right\}
\leq \frac{1}{s^{m-L}} \sum_{0 < |r_1|, \ldots, |r_L| \leq q/2} \rho(r, D) \prod_{i=1}^L \frac{1}{|r_i|}.
\]

We consider a \( L \)-tuple \( \mathcal{D} = (D_1, \ldots, D_L) \) with \( D_i | D \), \( 1 \leq i \leq L \), and set

\[
\mathcal{M}(\mathcal{D}) := \max\{\rho(r, D) : 0 < |r_i| \leq q/2, (r_i, D) = D_i\}.
\]

Observe that

\[
\sum_{0 < |r_1|, \ldots, |r_L| \leq q/2} \rho(r, D) \prod_{i=1}^L \frac{1}{|r_i|} \leq \frac{\mathcal{M}(\mathcal{D})}{D_1 \cdots D_L} \sum_{0 < |e_i| \leq q/(2D_i)} \prod_{i=1}^L \frac{1}{|e_i|} \ll \frac{\mathcal{M}(\mathcal{D})(\log q)^L}{D_1 \cdots D_L}.
\]
Note that the number of such $L$-tuples $\mathcal{D}$ is $\ll q^\epsilon$. Thus, (4.27) holds if we can show that for each $r$ with $(r_i, D) = D_i$,

$$\rho(r, D) \ll m, \delta_0, d, l \ D^{-1/2}q^{1/2-\delta_0-2\epsilon} \ s^{-L} \ \prod_{i=1}^{L} D_i.$$  

(4.28)

Obviously, (4.28) is true if the right-hand side of (4.28) is strictly bigger than 1. We therefore assume that $D_1, \ldots, D_L$ satisfy

$$\prod_{i=1}^{L} D_i \leq D^{1/2}s^Lq^{-1/2+\delta_0+2\epsilon}.$$  

Also, since $s \leq q^{1/(2m)-\delta_0}$, we have

$$\prod_{i=1}^{L} D_i \leq D^{1/2}q^{L/(2m)-1/2+(1-L)\delta_0+2\epsilon} \leq D^{1/2}q^{-\delta_0/2}.$$  

(4.29)

The following pages contain the proof of (4.28), thus completing the proof of Lemma 4.4.

Proof of (4.28). For a prime divisor $p_j$ of $D$, we let $m_j$ be the number of components $r_i = 0 \pmod{p_j}$. Then it can be easily seen that

$$\prod_{i=1}^{L} D_i = \prod_{p_j | D} p_j^{m_j}.$$  

(4.30)

Consider a vector $a$ which contributes to $\rho(r, D)$ and the corresponding partition $\mathcal{P}(a, p_j)$. Recall that such $a$ satisfies (4.22). Since $r_i = 0$ for $L < i \leq m$, we can view $\mathcal{P}(a, p_j)$ as a partition of $\{1, \ldots, L\}$. Note that if $r_i \neq 0 \pmod{p_j}$, then the subset $V_{\ell}$ containing the index $i$ has more than one element. Thus, there are at most $\left[ \frac{L-m_j}{2} \right]$ such subsets $V_{\ell}$. Now, in each $V_{\ell}$, we choose the largest index $i(\ell')$ for which $r_{i(\ell')} \neq 0 \pmod{p_j}$. Then, we see that $V_{\ell}$ produces the following independent congruences:

$$A_i - A_{i(\ell')} = 0 \pmod{p_j}, \quad i \in V_{\ell} \setminus \{i(\ell')\}.$$  

Since each of the $L-m_j$ indices $i \neq i(\ell')$ with $r_i \neq 0 \pmod{p_j}$ corresponds to exactly one of these independent congruences, the number of such congruences, say $\tilde{m}_j$, satisfies

$$\tilde{m}_j \geq L - m_j - \left[ \frac{L-m_j}{2} \right].$$  

(4.31)

We put together all these congruences for all the prime divisors $p_j$ of $D$. Note that $m_j = 0$ for some $p_j$, since otherwise (4.30) implies that $D$ divides $\prod_{i=1}^{L} D_i$, which contradicts (4.29). Thus, every index $i \in \{1, \ldots, L\}$ appears in the congruences. Also, the vectors $a$ which satisfy all these congruences lie on a lattice whose fundamental parallelepiped has volume $\prod_{p_j | D} p_j^{\tilde{m}_j}$.

We remark that all the vectors $a$ which contribute to $\rho(r, D)$ are placed on several lattices. The number of such lattices is $\ll \epsilon q^\epsilon$, and therefore we can consider only one fixed lattice.
In the following, we count the vectors $\mathbf{a}$ in $\rho(\mathbf{r}, D)$ that satisfy a fixed set of congruences described above.

It suffices to count the $m$-tuples $(A_1, \ldots, A_m)$ which satisfy the congruences, since $\mathbf{a}$ is uniquely determined by such a $m$-tuple. Recall that $A_m = 0$ by definition. Using the condition $\mathbf{a} \in (sI)^*$, we can bound the integers $A_{m-1}, \ldots, A_L$ by some positive constant, say $sc_I$. Hence there are at most $(sc_I)^{m-L}$ choices for $(A_{m-1}, \ldots, A_L)$. Now fix $A_{m-1}, \ldots, A_L$. We first consider the congruences that involve $A_{L-1} - A_L$ and put them together to obtain

$$A_{L-1} - A_L = 0 \pmod{d_{L-1}}$$

for some $d_{L-1} \mid D$. This gives at most $c_I([s/d_{L-1} + 1])$ possible values for $A_{L-1}$. Similarly, we consider the congruences involving $A_{L-2} - A_L$ and $A_{L-2} - A_{L-1}$. Putting them together yields one congruence

$$A_{L-2} = B_{L-2} \pmod{d_{L-2}},$$

where $d_{L-2}$ is some divisor of $D$, and $B_{L-2}$ (mod $d_{L-2}$) is an integer uniquely determined in terms of $A_{L-1}$ and $A_L$. This implies that for each value of $A_{L-1}$, there exist at most $c_I([s/d_{L-2} + 1])$ possible values for $A_{L-2}$. We repeat this argument for $A_{L-3}, \ldots, A_1$ in order. Here, we can see that

$$\prod_{i=1}^{L-1} d_i = \prod_{p_j \mid D} p_j^{m_j}. \quad (4.32)$$

It follows that the number of vectors $\mathbf{a}$ on the lattice is bounded by

$$s^{m-L} \prod_{i=1}^{L-1} \left( \left\lfloor \frac{s}{d_i} \right\rfloor + 1 \right) \ll s^{m-L} \prod_{i=1}^{L-1} \frac{\max\{s, d_i\}}{d_i} = s^{m-L+m_0} \prod_{i=1}^{L-1} \frac{1}{d_i},$$

where $m_0$ denotes the number of $d_i$'s less than $s$. This implies that

$$\rho(\mathbf{r}, D) \ll \frac{s^{m-L+m_0} d^c}{\#(sI)^* \prod_{d_i < s} d_i} \ll s^{1-L+m_0} d^c. \quad (4.33)$$

Hence (4.28) holds provided that we show the following:

$$D \ll q^{1-3\delta_0} s^{-2m_0-2} \left( \prod_{i=1}^{L} D_i^2 \right) \left( \prod_{d_i < s} d_i^2 \right). \quad (4.34)$$

Using $s \le q^{1/(2m) - \delta_0}$, we see that $s^{2m} \le q^{1-2m\delta_0} \le q^{1-4\delta_0}$. Therefore (4.33) follows from

$$D \ll q^{\delta_0} s^{2(m-1-m_0)} \left( \prod_{i=1}^{L} D_i^2 \right) \left( \prod_{d_i < s} d_i^2 \right). \quad (4.34)$$
It remains to prove (4.34). From (4.30), (4.32) and (4.31), we can deduce that

\[
\left( \prod_{i=1}^{L} D_i \right) \left( \prod_{d_i < s} d_i^2 \right) = \prod_{p_j \mid D} p_j^{m_j + 2 \tilde{m}_j} \geq \prod_{p_j \mid D} p_j^{m_j + (L - m_j)} = D^L. \tag{4.35}
\]

Thus, we get

\[
\left( \prod_{i=1}^{L} D_i \right) \left( \prod_{d_i < s} d_i^2 \right) = \left( \prod_{i=1}^{L} D_i \right) \left( \prod_{i=1}^{L-1} d_i^2 \right) \left( \prod_{d_i \geq s} d_i^2 \right)^{-1} \geq D^{L-2(L-1-m_0)} = D^{2m_0+2-L}.
\]

Note that if \(2m_0 + 2 > L\), then (4.34) is true. We thus assume \(2m_0 + 2 \leq L\). Since

\[
2(m - 1 - m_0) \geq 2m - L \geq L,
\]
equation (4.34) holds if we show

\[
D \ll s^L. \tag{4.36}
\]

From (4.35) and (4.29), we derive

\[
D^L \leq \left( \prod_{i=1}^{L} D_i \right) \left( \prod_{i=1}^{L-1} d_i^2 \right) \leq D^{1/2} q^{-\delta_0/2} \left( \prod_{i=1}^{L-1} d_i^2 \right),
\]

which implies that

\[
\prod_{i=1}^{L-1} d_i > D^{(L-1/2)/2}. \tag{4.37}
\]

On the other hand, we return to the aforementioned set of congruences of the form

\[
A_{i_1} - A_{i_2} = 0 \pmod{p_j}.
\]

Recall that we have \(\tilde{m}_j\) such congruences for each \(p_j\). For each fixed pair \((i_1, i_2)\), we combine all the congruences involving \(A_{i_1} - A_{i_2}\) to obtain one congruence

\[
A_{i_1} - A_{i_2} = 0 \pmod{d_{i_1,i_2}}. \tag{4.38}
\]

Note that this is just a different arrangement of the set of congruences above. In particular, we see that, by (4.32),

\[
\prod_{1 \leq i_1 < i_2 \leq L} d_{i_1,i_2} = \prod_{p_j \mid D} p_j^{\tilde{m}_j} = \prod_{i=1}^{L-1} d_i. \tag{4.39}
\]

It follows from (4.38) that \(\prod d_{i_1,i_2}\) divides

\[
\prod_{1 \leq i_1 < i_2 \leq L} (A_{i_1} - A_{i_2}).
\]

Since each \(A_i\) is bounded by \(sc_I\), we have

\[
\prod_{1 \leq i_1 < i_2 \leq L} (A_{i_1} - A_{i_2}) \ll_I s^{(L-1)/2}.
\]
Hence, by (4.37) and (4.39),
\[ D^{(L-1/2)/2} < \prod_{i=1}^{L-1} d_i \ll L^{(L-1)/2}. \tag{4.40} \]
From (4.40), we deduce that \( D \ll s^L \), which proves (4.36). The proof of Lemma 4.4 is therefore complete. \( \square \)

5. A necessary and sufficient condition

In this section we show that the obstruction to being Poissonian along a sequence for \( n^d \alpha \mod 1 \), \( d \geq 2 \), is the same as for \( n^2 \alpha \mod 1 \). This obstruction consists in the presence of large square factors in the denominators of good approximants. Theorem 1.1 is an easy consequence of the following result.

**Theorem 5.1.** Let \( d \geq 2 \) be an integer, and let \( \alpha \) be an irrational number for which there are infinitely many rationals \( b_j/q_j \) satisfying
\[ |\alpha - b_j/q_j| < \frac{1}{q_j^{d+1}}. \tag{5.1} \]
Then the following are equivalent.

1. There exists a sequence \( N_j \to \infty \) with \( \log N_j/\log q_j \to 1 \) such that \( n^d \alpha \mod 1 \) is Poissonian along \( N_j \).
2. There exists a sequence \( N_j \to \infty \) with \( \log N_j/\log q_j \to 1 \) such that \( n^2 \alpha \mod 1 \) is Poissonian along \( N_j \).
3. Letting \( \tilde{q}_j \) denote the square free part of \( q_j \), we have
\[ \lim_{j \to \infty} \frac{\log \tilde{q}_j}{\log q_j} = 1. \]

Conditions (2) and (3) are equivalent by [Z03, Theorem 1]. Hence it is enough to prove that (1) is equivalent to (3). The implication (3) \( \implies \) (1) requires Theorem 4.1. The other direction follows the arguments in [Z03, Section 3], and requires the two following lemmas. The first is a divergency principle for \( m \)-correlations (see [RSZ01, Lemma 6]).

**Lemma 5.2.** Let \( q = uv^2 \) with \( v > q^\delta \) for some \( \delta > 0 \). Let \( \eta > 1 \), and suppose that \( \log N/\log q > \eta \). Let \( f \in \mathcal{C}_c^\infty(\mathbb{R}^{m-1}) \) be a non-negative test function which is non-vanishing at the origin. Then, for every integer \( b \) and every \( d \geq 2 \),
\[ R^{(m)}(N, d, b/q, f) \gg m, \delta \frac{1}{N} f(0) \left( \frac{Nv}{q} \right)^m. \]
Proof. By the definition of the \( m \)-level correlation,
\[
R^{(m)}(N, d, \frac{b}{q}, f) = \frac{1}{N} \sum_{1 \leq n_1, \ldots, n_m \leq N \atop n_j \text{ distinct}} f\left(\ldots, N\left\{ \frac{bn_j^d}{q} \right\}, \ldots \right).
\]

Since \( f \geq 0 \), it is enough to estimate the contribution of the terms \((n_1, \ldots, n_m)\), with \( n_j \) distinct, such that \( n_1, \ldots, n_m \) are all divisible by \( uv \). There are \( \gg_m [N/uv]^m [Nv/q]^m \) such \( m \)-tuples. If \( n = uvn' \), then, since \( q = uv^2 \),
\[
\left\{ \frac{bn_j^d}{q} \right\} = \{bu(n')^2(vn')^{d-2}\} = 0,
\]
and therefore
\[
R^{(m)}(N, d, \frac{b}{q}, f) \gg_m, \delta \frac{1}{N} f(0) \left( \frac{Nv}{q} \right)^m,
\]
as wanted. \( \square \)

The next lemma allows one to pass from the \( m \)-level correlation of a family of finite sequences to another family, which is close enough to the original one. Let \( \mathcal{N} = \{x_N(n): n \leq N\} \) and \( \mathcal{N}' = \{x'_N(n): n \leq N\} \) be two families of sequences in \([0, 1]\). We define for each \( N \) the scaled distance between the corresponding sequences to be
\[
\varepsilon_N(\mathcal{N}, \mathcal{N}') := N \max_{n \leq N} |x_N(n) - x'_N(n)|.
\]
Recall that the \( m \)-level correlation for the family \( \mathcal{N} \) is defined for every \( f \in C_c^\infty(\mathbb{R}^{m-1}) \) by
\[
R^{(m)}(N, \mathcal{N}, f) := \frac{1}{N} \sum_{1 \leq n_1, \ldots, n_m \leq N \atop n_j \text{ distinct}} F_N\left(x_N(n_1) - x_N(n_2), \ldots, x_N(n_{m-1}) - x_N(n_m)\right),
\]
where \( F_N(y) := \sum_{l \in \mathbb{Z}^m} f(\mathbf{1} + y) \).

Lemma 5.3. [RSZ01, Lemma 5] Assume that \( \mathcal{N}, \mathcal{N}' \subset [0, 1] \) are two families of sequences with \( \varepsilon_N(\mathcal{N}, \mathcal{N}') \to 0 \) as \( N \to \infty \). Then for every \( f \in C_c^\infty(\mathbb{R}^{m-1}) \),
\[
|R^{(m)}(N, \mathcal{N}, f) - R^{(m)}(N, \mathcal{N}', f)| \leq R^{(m)}(N, \mathcal{N}, f_+)\varepsilon_N(\mathcal{N}, \mathcal{N}')
\]
for \( N \) sufficiently large, with \( f_+ \in C_c^\infty(\mathbb{R}^{m-1}) \), a non-negative function depending only on \( f \).

Proof of Theorem 5.1. (1) \( \implies \) (3) We prove the contrapositive. Assume that (3) fails. Then there are infinitely many indices \( j \)'s and a \( \delta > 0 \) for which in the decomposition \( q_j = \tilde{q}_j v_j^2 \), with \( \tilde{q}_j \) square free, we have \( v_j > q_j^\delta \). Let \( N_j \to \infty \) be a sequence with \( \frac{\log N_j}{\log q_j} \to 1 \). For \( j \) large enough we have \( N_j \in [q_j^{1-\delta/2}, q_j^{1+\delta/2}] \). Consider the two families of sequences
\[
\mathcal{N} = \left\{ \{an^d\} : 1 \leq n \leq N_j \right\} \quad \text{and} \quad \mathcal{N}' = \left\{ \{bn^d/q_j\} : 1 \leq n \leq N_j \right\}.
\]
Let \( f \in C^\infty(\mathbb{R}^{m-1}) \) be a non-negative function that does not vanish at the origin. We want to argue that the \( m \)-level correlation \( R^{(m)}(N, \mathcal{N}, f) \) diverges as \( j \to \infty \) for \( m \) large enough. Since \( f \) is non-negative, we can restrict ourselves to considering the contribution of the \( m \)-tuples \( x = (x_1, \ldots, x_m) \in J^m \), where \( J = \left\{ 1, \ldots, \left\lfloor q_j^{1-\delta/2}\right\rfloor \right\} \subseteq \{1, \ldots, N_j\} \). On such \( x \), the scaled distance between \( \mathcal{N} \) and \( \mathcal{N}' \) is

\[
\varepsilon_{N_j}(\mathcal{N}, \mathcal{N}') = N_j \max_{n \in J} \left| n^d \alpha - \frac{n^d b_j}{q_j} \right| \leq q_j^{1+\delta/2} q_j^{d-\delta} \frac{1}{q_j^{\delta+1}} = q_j^{-\delta/2}.
\]

By Lemma 5.3, we can thus pass to the family \( \mathcal{N}' \). It is enough to prove that the contribution of the \( m \)-tuples \( x \in J^m \) to \( R^{(m)}(N, \mathcal{N}', f) \) makes it diverge for \( m \) large enough. By the definition of \( \mathcal{N}' \) and Lemma 5.2,

\[
R^{(m)}(N, \mathcal{N}', f) = R^{(m)}\left(N, d, \frac{b_j}{q_j}, f\right) \gg_{m, \delta} \frac{1}{N_j} f(0) \left( \frac{N_j v_j}{q_j} \right)^m \geq q_j^{(\delta/2)(m-1)}
\]

and therefore \( R^{(m)}(N, \mathcal{N}, f) \) diverges as \( j \to \infty \) while keeping \( m \) and \( \delta \) fixed, provided \( m > 1 + \frac{2}{\delta} \).

(3) \( \implies \) (1) We construct the required sequence \( N_j \). For every integer \( k \geq 2 \) we define an integer \( j_k \) in the following way. Apply Theorem 4.1 for every \( m \in \{2, \ldots, k\} \) with \( \delta_0 = \frac{1}{8k} \). There exists \( \delta = \delta(k) > 0 \) such that for \( q \to \infty \) satisfying \( \tilde{q} \geq q^{1-\delta(k)} \) and for every residue \( b \mod q \) with \( (b, q) = 1 \), the \( m \)-level correlation for the sequence \( n^d b (\mod q), 1 \leq n \leq N \), where \( N = [q^{1-1/(4k)}] \), is Poissonian for every \( m \in \{2, \ldots, k\} \). We apply this to every pair \((b_j, q_j)\). By (3) there exists \( j_k \) such that, for every \( j \geq j_k \), we have \( \tilde{q}_j \geq q_j^{1-\delta(k)} \) and the \( m \)-level correlation for the sequence \( \{n^d b_j (\mod q_j), 1 \leq n \leq [q_j^{1-1/(4k)}]\} \), is Poissonian for \( m \in \{2, \ldots, k\} \). It follows from (5.1) and Lemma 5.3 that for \( j \geq j_k \) the \( m \)-level correlation for \( m \in \{2, \ldots, k\} \) for the sequence \( \{n^d \alpha\}, 1 \leq n \leq [q_j^{1-1/(4k)}] \), is Poissonian. With \( j_k \) defined as above, we now put \( N_j = [q_j^{1-1/(4k)}] \) for all those \( j \geq j_k \) such that \( j < j_{k+1} \). The sequence \( N_j \) thus defined has the required properties. \( \square \)

6. Acknowledgements

The authors are grateful to Bruce Berndt for useful comments and suggestions.

References

[AL94] W. W. Adams and P. Loustaunau, An introduction to Gröbner bases. Graduate Studies in Mathematics, 3. American Mathematical Society, Providence, RI, 1994.

[BT77] M. V. Berry and M. Tabor, Level clustering in the regular spectrum, Proc. Royal Soc. London A 356 (1977), 375–394.

[BZ00] F. P. Boca and A. Zaharescu, Pair correlation of values of rational functions (mod p). Duke Math. J. 105 (2000), no. 2, 267–307.

[B66] E. Bombieri, On exponential sums in finite fields. Amer. J. Math. 88 (1966), 71–105.
SPACINGS BETWEEN THE FRACTIONAL PARTS OF $n^d\alpha$

[CGI87] G. Casati, I. Guarneri, and F. M. Izrailev, Statistical properties of the quasi-energy spectrum of a simple integrable system, *Phys. Lett. A* **124** (1987), 263–266.

[D51] H. Davenport, On a principle of Lipschitz. *J. London Math. Soc.* **26** (1951), 179–183. Corrigendum: On a principle of Lipschitz. *J. London Math. Soc.* **26** (1964), 580.

[DZ19] A. Dunn and A. Zaharescu, The twisted second moment of modular half integral weight $L$-functions. Preprint. https://arxiv.org/abs/1903.03416.

[GTZ88] P. Gianni, B. Trager, and G. Zacharias, Gröbner bases and primary decomposition of polynomial ideals. Computational aspects of commutative algebra. *J. Symbolic Comput.* **6** (1988), no. 2-3, 149–167.

[K89] G. Karpilovsky, Topics in field theory. North-Holland Mathematics Studies, 155. Notas de Matemática [Mathematical Notes], 124. North-Holland Publishing Co., Amsterdam, 1989.

[KR99] P. Kurlberg, and Z. Rudnick, The distribution of spacings between quadratic residues. *Duke Math. J.* **100** (1999), no. 2, 211–242.

[PBG89] A. Pandey, O. Bohigas, and M. J. Giannoni, Level repulsion in the spectrum of two-dimensional harmonic oscillators, *J. Phys. A* **22** (1989), 4083–4088.

[RS98] Z. Rudnick and P. Sarnak, The pair correlation function of fractional parts of polynomials. *Comm. Math. Phys.* **194** (1998), no. 1, 61–70.

[RSZ01] Z. Rudnick, P. Sarnak, and A. Zaharescu, The distribution of spacings between the fractional parts of $n^2\alpha$. *Invent. Math.* **145** (2001), no. 1, 37–57.

[Sc76] W. M. Schmidt, Equations over finite fields. An elementary approach. Lecture Notes in Mathematics, Vol. 536. Springer-Verlag, Berlin-New York, 1976.

[Sh12] I. E. Shparlinski, Modular hyperbolas. *Jpn. J. Math.* **7** (2012), no. 2, 235–294.

[Só58] V. Sós, On the distribution mod 1 of the sequence $n\alpha$, *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* **1** (1958), 127–134.

[St98] M. Stillman, Gröbner Bases: a Tutorial. Available at www3.risc.jku.at.

[Sz59] S. Swierczkowski, On succesive settings of an arc on the circumference of a circle, *Fund. Math.* **46** (1959), 187–189.

[W48] A. Weil, Sur les Courbes Algébriques et les Variétés qui s’en Déduisent, Hermann. Paris 1948.

[Z03] A. Zaharescu, Correlation of fractional parts of $n^2\alpha$. *Forum Math.* **15** (2003), no. 1, 1–21.


M.F.: DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, 1409 WEST GREEN STREET, URBANA, IL 61801, USA

E-mail address: fassina2@illinois.edu

S.K.: AORC, SUNGKYUNKWAN UNIVERSITY, 2066 SEOBU-RO, SUWON 16419, KOREA

E-mail address: ssunny8079@hanmail.net

A.Z.: DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN 1409 WEST GREEN STREET, URBANA, IL 61801, USA AND SIMON STOILLOW INSTITUTE OF MATHEMATICS OF THE ROMANIAN ACADEMY, P.O. BOX 1-764, RO-014700 BUCHAREST, ROMANIA

E-mail address: zaharesc@illinois.edu