THE SUM OF DIGITS FUNCTION OF CANONICAL NUMBER SYSTEMS: DISTRIBUTION IN RESIDUE CLASSES

MANFRED G. MADRITSCH

Abstract. In the present paper we investigate the sum of digits function for canonical number systems. We are interested in its re-partition in arithmetic progressions and similar results for sum sets. The original problem goes back to Gelfond, who proved the independence of the distribution of the digits and their sum of digits. The present paper extends results by Thuswaldner and Mauduit and Sárközy to this kind of numeration systems.

1. Introduction

Let $q \geq 2$ be a positive integer, then we define the sum-of-digits function s_q, which as its name indicates takes the digits of an expansion and sums them up, *i.e.*,

$$s_q(z) = \sum_{h=0}^{\ell} a_h \quad \text{for} \quad z = \sum_{h=0}^{\ell} a_h q^h.$$

This function has been studied from different aspects. In the present paper we are interested in its re-partition in arithmetic progressions. One of the first results in this direction is due to Gelfond [4], who could prove that the set

$$S_{h,m}(N) := \{z \leq N : s_q(z) \equiv h \bmod m\}$$

is equidistributed in residue classes mod s. A similar question for sum sets has been investigated by Mauduit and Sárközy [13]. In particular, they proved that for $\mathcal{A}, \mathcal{B} \subset \{1, \dots, N\}$ two sets and $N \in \mathbb{N}$, the estimate

$$\left| \#\left\{(a,b) \in \mathcal{A} \times \mathcal{B} : a + b \in S_{h,m}(2N)\right\} - \frac{|\mathcal{A}|\,|\mathcal{B}|}{m} \right| \ll N^{\theta}(|\mathcal{A}|\,|\mathcal{B}|)^{\frac{1}{2}}$$

holds, where $\theta < 1$ and the implied constant is absolute.

Both results have been generalized to number systems in number fields. To this end let K be a number field and $\mathbb{Z}_K$ be its ring of integers. Let $b \in \mathbb{Z}_K$ and $\mathcal{N} := \{0, 1, \dots, |\mathrm{N}(b)| - 1\}$. Then the pair $(b, \mathcal{N})$ is called a canonical number system in $\mathbb{Z}_K$ if each $z \in \mathbb{Z}_K$ admits a finite and unique representation of the form

$$z = \sum_{h=0}^{\ell} a_h b^h$$

with $a_h \in \mathcal{N}$ for $0 \leq h \leq \ell$ and $a_\ell \neq 0$ if $\ell \neq 0$. Furthermore we call b the base and $\mathcal{N}$ the set of digits.

A characterization for all possible bases together with an algorithm for determining bases was given by Kovács and Pethő [10]. Unfortunately this characterization depends on the structure of the ring of integers of the field. This algorithm was improved and simplified by Akyama nad Pethő in [3]. Explicit characterizations for some classes of number fields are give in a series of papers by Kátai, Kovács and Szabó [7–9] .

Date: July 6, 2012.

2010 *Mathematics Subject Classification.* 11R45 (11A63).

Key words and phrases. sum of digits, canonical number system, exponential sum.

Supported by the Austrian Research Foundation (FWF), Project S9603, that is part of the Austrian Research Network "Analytic Combinatorics and Probabilistic Number Theory".

Similarly to the definition above, we define the sum-of-digits function s_b in these number systems by

$$s_b(z) = \sum_{h=0}^{\ell} a_h \quad \text{for} \quad z = \sum_{h=0}^{\ell} a_h b^h.$$

In order to state the generalization of the two results from above we need a second ingredient – the estimation of the length of expansion. To this end we note that for the positive integers, we have that the length of expansion of z growths with the logarithm of z. Now let K be a number field of degree n. Since the digits are integers, we get an expansion for z and all its conjugates simultaneously, *i.e.*

$$z^{(i)} = \sum_{h=0}^{\ell} a_h (b^{(i)})^h.$$

Thus we also have to simultaneously bound the length of expansion in this case. This is established by the following

Lemma 1.1 ([11, Theorem]). *Let $\ell(z)$ be the length of the expansion of z to the base b. Then*

$$\left| \ell(z) - \max_{1\le i\le n} \frac{\log|z^{(i)}|}{\log|b^{(i)}|} \right| \le C.$$

Now we define the Minkowski-embedding $\phi(z)$ by

$$\phi(z) := (z^{(1)}, \dots, z^{(s)}, \Re z^{(s+1)}, \Im z^{(s+1)}, \dots, \Re z^{(s+t)}, \Im z^{(s+t)}),$$

where $z^{(1)}, \dots, z^{(s)}$ are the real and $z^{(s+1)}, \dots, z^{(s+t)}$ are the complex conjugates of $z \in K$. We define the set $C(N) \subset \mathbb{R}^n$ as generalization of the area of summation from above. In particular, let $C(N)$ consist of all vectors

$$(x_1, \dots, x_s, x_{s+1}, y_{s+1}, \dots, x_{s+t}, y_{s+t}) \in \mathbb{R}^n,$$

whose coordinates satisfy

$$\begin{aligned} |x_j| &\le \ell_j(N) && (1 \le j \le s),\\ x_{s+j}^2 + y_{s+j}^2 &\le \ell_{s+j}(N) && (1 \le j \le t), \end{aligned}$$

with

$$N^{\beta_1} < \ell_j(N) < N^{\beta_2}, \quad (1 \le j \le s+t)$$

for some $0 < \beta_1 \le \beta_2$. With help of this set we define

$$M(N) = \{z \in \mathbb{Z}_K : \phi(z) \in C(N)\}.$$

Now by writing

$$U_{r,m}(M(N)) = \{z \in M(N) : s_b(z) \equiv r \bmod m\}$$

we can state Thuswaldner's result describing the distribution of the sum-of-digits function in residue classes.

Theorem ([16, Theorem 3.1]). *Let K be a number field with ring of integers $\mathbb{Z}_K$. Let b be the base of a canonical number system in $\mathbb{Z}_K$ and write $p_b(x) = a_0 + \cdots + a_{n-1}x^{n-1} + x^n$ for the minimal polynomial of b. For an ideal $\mathfrak{s}$ of $\mathbb{Z}_K$ denote by $V_b(M(N))$ the number of elements of $U_{r,m}(M(N))$ that fulfill*

$$z \equiv a \bmod \mathfrak{s}.$$

Then, if $(p_b(1), m) = 1$,

$$V_b(M(N)) = \frac{|M(N)|}{m\mathrm{N}(\mathfrak{s})} + \mathcal{O}\left(|M(N)|^{\lambda}\right) \quad (\lambda < 1),$$

where λ does not depend on N, r, a and $\mathfrak{s}$.

Furthermore he also extended the result by Mauduit and Sárközy to number fields.

Theorem ([16, Theorem 4.1]). *Let K be a number field of degree n with ring of integers $\mathbb{Z}_K$. Let b be the base of a canonical number system in $\mathbb{Z}_K$ and $p_b(x)$ be the minimal polynomial of b. If $(p_b(1), m) = 1$, then*

$$\left| \#\left\{(a,b) \in \mathcal{A} \times \mathcal{B} : a + b \in U_{h,m}(2M(N))\right\} - \frac{|\mathcal{A}|\,|\mathcal{B}|}{m} \right| \ll M(N)^{\theta}(|\mathcal{A}|\,|\mathcal{B}|)^{\frac{1}{2}}$$

holds for any two sets $\mathcal{A}, \mathcal{B} \subset M(N)$. The implied constant is absolute and $\theta < 1$.

2. Definitions and Results

The objective of this paper are generalisations of Thuswaldner's results to number systems in quotient rings of the ring of polynomials over the integers. To formulate our results we have to introduce the relevant notions. The following definition describes number systems in this ring.

Definition 2.1. Let $p \in \mathbb{Z}[X]$ be monic of degree n and let $\mathcal{N}$ be a subset of $\mathbb{Z}$. The pair $(p, \mathcal{N})$ is called a number system if for every $z \in \mathbb{Z}[X] \setminus \{0\}$ there exist unique $\ell \in \mathbb{N}$ and $a_h \in \mathcal{N}, h = 0, \ldots, \ell; a_\ell \neq 0$ such that

$$z \equiv \sum_{h=0}^{\ell} a_h(z) X^h \pmod{p}. \tag{2.1}$$

In this case a_h are called the digits and $\ell = \ell(a)$ is called the length of the representation.

This concept was introduced in [14] and was studied among others in [1,2,10,11]. It was proved in [2], that $\mathcal{N}$ must be a complete residue system modulo $p(0)$ including 0 and the zeroes of p are lying outside or on the unit circle. However, following the argument of the proof of Theorem 6.1 of [14], which dealt with the case p square free, one can prove that non of the zeroes of p are lying on the unit circle.

If p is irreducible then we may replace X by one of the roots β of p. Then we are in the case of $\mathbb{Z}[X]/(p) \cong \mathbb{Z}[\beta]$ being an integral domain in an algebraic number field (*cf.* Section 1). Then we may also denote the number system by the pair $(\beta, \mathcal{N})$ instead of $(p, \mathcal{N})$. For example, let $q \geq 2$ be a positive integer, then $(p, \mathcal{N})$ with $p = X - q$ gives a number system in $\mathbb{Z}$, which corresponds to the number systems $(q, \mathcal{N})$. Furthermore for n a positive integer and $p = X^2 + 2n\,X + (n^2 + 1)$ we get number systems in $\mathbb{Z}[i]$.

Now we want to return to these more general number systems and consider the sum-of-digits function s_p in $(p, \mathcal{N})$. We define

$$s_p(z) \equiv \sum_{h=0}^{\ell} a_h \quad \text{for} \quad z \equiv \sum_{h=0}^{\ell} a_h(z) X^h \pmod{p}.$$

As above we need an estimation for the length of expansion in order to find good bounds for the area of summations. Therefore we will define an embedding of the ring $\mathbb{Z}[X]/(p)$ in $\mathbb{R}^n$. To this end we fix a number system $(p, \mathcal{N})$ and factor p by

$$p := \prod_{i=1}^{t} p_i^{m_i}$$

with $p_i \in \mathbb{Z}[X]$ irreducible and $\deg p_i = n_i$. Then we define by

$$\mathcal{R} := \mathbb{Z}[X]/(p) = \bigoplus_{i=1}^{t} \mathcal{R}_i \quad \text{with} \quad \mathcal{R}_i = \mathbb{Z}[X]/\left(p_i^{m_i}\right)$$

for $i = 1, \ldots, t$ the $\mathbb{Z}$-module under consideration and in the same manner by

$$K := \mathbb{Q}[X]/(p) = \bigoplus_{i=1}^{t} K_i \quad \text{with} \quad K_i = \mathbb{Q}[X]/\left(p_i^{m_i}\right)$$

for $i = 1, \ldots, t$ the corresponding vector space. Finally we denote by $\overline{K}$ the completion of K according to the usual Euclidean distance.

In order to properly state our result we need a bounded area whose measure increases with T tending to infinity. We start with the projections to the parts $\mathcal{R}_i$. Let $\pi_i : \mathcal{R} \to \mathcal{R}_i$ be the canonical projections. Noting that

$$\mathcal{R}_i = \mathbb{Z}[X]/(p_i^{m_i}) \cong (\mathbb{Z}[X]/(p_i))^{m_i}$$

we define π_{ij} to be the canonical projections for $i = 1, \dots, t$ and $j = 1, \dots, m_i$. We have for every $z_i \in \mathcal{R}_i$ the unique representation

$$z_i = \sum_{j=1}^{m_i} a_{ij} p_i^{j-1} = \sum_{j=1}^{m_i} \sum_{k=1}^{n_i} a_{ijk} X^{k-1} p_i^{j-1}$$

with $a_{ij} \in \mathbb{Z}[X]$ and $a_{ijk} \in \mathbb{Z}$, respectively. We clearly have

$$\pi_{ij}(z) = \sum_{k=1}^{n_i} a_{i1k} X^{k-1} \quad \text{for} \quad j = 1, \dots, m_i.$$

Since we will often consider a fixed $z \in \mathcal{R}$ or a fixed ideal $\mathfrak{q}$ of $\mathcal{R}$ we shorten notation by setting $z_i := \pi_i(z)$, $z_{ij} := \pi_{ij}(z)$, $\mathfrak{q}_i := \pi_i(\mathfrak{q})$ and $\mathfrak{q}_{ij} := \pi_{ij}(\mathfrak{q})$ for the corresponding projections, respectively. Finally we note that $\pi := (\pi_1, \dots, \pi_t) = (\pi_{11}, \dots, \pi_{tm_t})$ is an isomorphism by the Chinese Remainder Theorem.

Now we want to use these projections in order to bound the area under considerations. To this end we denote by β_{ik} the roots of p_i for $i = 1, \dots, t$ and $k = 1, \dots, n_i$. We may assume that these roots are ordered such that for (s_i, t_i) being the index of p_i (*i.e.*, s_i being the number of real roots and t_i being the number of pairs of complex roots, respectively) we have that $\beta_{i1}, \dots, \beta_{is_i}$ are the real roots and $(\beta_{i,s_i+1}, \beta_{i,s_i+t_i+1}), \dots, (\beta_{i,s_i+t_i}, \beta_{i,s_i+2t_i})$ are the pairs of complex roots of p_i.

In the same manner as in the paragraph above we split vectors in $\mathbb{R}^n$ up into its components according to the parts $\mathcal{R}_i$ and $\mathcal{R}_{ij}$. In particular, for fixed $\mathbf{x} \in \mathbb{R}^n$ we write

$$\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_t) = (\mathbf{x}_{11}, \dots, \mathbf{x}_{tm_t}) = (x_{111}, \dots, x_{tm_tn_t}),$$

where $\mathbf{x}_i \in \mathbb{R}^{m_i n_i}$, $\mathbf{x}_{ij} \in \mathbb{R}^{n_i}$ and $x \in \mathbb{R}$, respectively.

In the next step we embed $\overline{K}$ in $\mathbb{R}^n$. In view of the structure of $\mathcal{R}$ it is more convenient to start at the bottom level with $\mathcal{R}_{ij}$ and define by ϕ_{ij} its embedding as

$$\phi_{ij} : \begin{cases} \pi_{ij}(\overline{K}) & \to & \mathbb{R}^{n_i}, \\ z_{ij} & \mapsto & (z_{ij}(\beta_{i1}), \dots, z_{ij}(\beta_{in_i})). \end{cases}$$

Now we go one step back and define for $z_i \in \mathcal{R}_i$ the embedding ϕ_i by

$$\phi_i : \begin{cases} \pi_i(\overline{K}) & \to & \mathbb{R}^{m_i n_i}, \\ z_i & \mapsto & (z_{i1}(\beta_{i1}), \dots, z_{i1}(\beta_{in_i}), z_{i2}(\beta_{i1}), \dots, z_{im_i}(\beta_{in_i})) \end{cases}$$

Finally we define the embedding ϕ by

$$\phi : \begin{cases} \overline{K} & \to & \mathbb{R}^n, \\ z & \mapsto & (z_{11}(\beta_{11}), \dots, z_{1m_i}(\beta_{1n_1}), z_{21}(\beta_{21}), \dots, z_{t,m_t}(\beta_{t,n_t})). \end{cases}$$

We note that

$$\phi(z) = (\phi_1 \circ \pi_1(z), \dots, \phi_t \circ \pi_t(z)) = (\phi_{11} \circ \pi_{11}(z), \dots, \phi_{t,m_t} \circ \pi_{t,m_t}(z)).$$

Remark 2.1. This embedding is motivated by the one used by Thuswaldner in [16]. We want to note that we could have use an other one as for example the following (as was used in [12])

$$\psi : \begin{cases} \overline{K} & \to & \mathbb{R}^n, \\ a_1 + a_2 X + \cdots + a_n X^{n-1} & \mapsto & (a_1, \dots, a_n). \end{cases}$$

However, there exists an invertible matrix M such that

$$M^{-1} \phi(z) M = \psi(z)$$

and therefore these embeddings are equivalent.

We want to use lattice theory in $\mathbb{R}^n$ therefore we define the bounded area $\mathcal{S}(T) \subset \mathbb{R}^n$ and use our projections and embeddings to gain the "bounded area" in $\mathcal{R}$. Again because of the structure of $\mathcal{R}$ it is more convenient to start at the bottom level with the set $\mathcal{S}_{ij}(T)$ bounding the area for $\mathcal{R}_{ij}$. Thus for $i = 1, \dots, t$ and $j = 1, \dots, m_i$ let $\mathcal{S}_{ij}(T)$ be the set of points $\mathbf{x} \in \mathbb{R}^{n_i}$ such that

$$|x_k| \le l_{ijk}(T),$$
$$x_k^2 + x_{k+1}^2 \le l_{ijk}(T)^2.$$

with

$$T^{\beta_1} < l_{ijk} < T^{\beta_2} \quad (1 \le k \le n_i). \tag{2.2}$$

Then $\mathcal{S}(T)$ is defined by

$$\mathcal{S}(T) := \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x}_{ij} \in \mathcal{S}_{ij}(T) \text{ for } i = 1, \dots, t,\ j = 1, \dots, m_i\}.$$

Finally we define the set $\mathcal{R}(T) \subset \mathcal{R}$ as those elements whose embedding lies in $\mathcal{S}(T)$, *i.e.*

$$\mathcal{R}(T) := \{g \in \mathcal{R} : \phi(g) \in \mathcal{S}(T)\}. \tag{2.3}$$

Since we concentrate on the set of elements whose sum of digits is in a certain residue class, we write for short

$$\mathcal{U}_{h,m}(\mathcal{R}(T)) := \{z \in \mathcal{R}(T) : s_p(z) \equiv h \bmod m\}.$$

Now we are able to state our main result.

Theorem 2.2. *Let $(p, \mathcal{N})$ be a number system. For an ideal $\mathfrak{s}$ of $\mathcal{R}$ denote by $\mathcal{V}_p(\mathcal{R}(T))$ the number of elements of $\mathcal{U}_{h,m}(\mathcal{R}(T))$ that fulfill*

$$z \equiv a \mod \mathfrak{s}.$$

Then, if $(p(1), m) = 1$,

$$\mathcal{V}_p(\mathcal{R}(T)) = \frac{|\mathcal{U}_{h,m}(\mathcal{R}(T))|}{m\mathrm{N}(\mathfrak{s})} + \mathcal{O}\left(|\mathcal{U}_{h,m}(\mathcal{R}(T))|^{\lambda}\right), \quad (\lambda < 1),$$

where λ does not depend on T, h, a, and $\mathfrak{s}$.

Note that $\mathcal{V}_p$ depends on $\mathfrak{s}$ but not on the choice of the residue class $a \bmod \mathfrak{s}$.

Theorem 2.3. *Let $(p, \mathcal{N})$ be a number system. If $(p(1), m) = 1$, then for any two subsets $\mathcal{A}, \mathcal{B} \subset \mathcal{R}(T)$ we have that*

$$\left| |\{(x, y) \in \mathcal{A} \times \mathcal{B} : x + y \in \mathcal{U}_{h,m}(\mathcal{R}(T))\}| - \frac{|\mathcal{A}|\,|\mathcal{B}|}{m} \right| \ll |\mathcal{R}(\mathcal{T})|^{\mu} \left(|\mathcal{A}|\,|\mathcal{B}|\right)^{\frac{1}{2}}$$

where the implied constant is absolute and $\mu < 1$.

3. Preliminaries

In this section we will use our choice of the embedding and connect the number system $(p, \mathcal{N})$ with a matrix number system. This method is standard in that area and we mainly follow Thuswaldner [16] and Madritsch and Pethő [12].

We note that if $(p, \mathcal{N})$ is a number system then X is an integral power base of $\overline{K}$, *i.e.*, $\{1, X, \dots, X^{n-1}\}$ is an $\mathbb{R}$-basis for $\overline{K}$. Then we get that

$$\phi_{ij}(X \cdot z_{ij}) = B_{ij}\phi_{ij}(z_{ij}) \quad \text{with} \quad B_{ij} = \begin{pmatrix} \beta_{i1} & \cdots & \cdots \\ \dots & \ddots & \dots \\ \cdots & \cdots & \beta_{i,n_i} \end{pmatrix}. \tag{3.1}$$

Now we extend this definition and get

$$\phi_i(X \cdot z_i) = B_i\phi_i(z_i) \quad \text{with} \quad B_i = \begin{pmatrix} B_{i1} & \cdots & \cdots \\ \dots & \ddots & \dots \\ \cdots & \cdots & B_{i,m_i} \end{pmatrix}$$

and

$$\phi(X \cdot z) = B\phi(z) \quad \text{with} \quad B = \begin{pmatrix} B_1 & \cdots & \cdots \\ \cdots & \ddots & \cdots \\ \cdots & \cdots & B_t \end{pmatrix}.$$

We note that B is a block diagonal matrix, which is the motivation of splitting the ring $\mathcal{R}$ into the subrings $\mathcal{R}_{ij}$.

Since X is invertible we get that B is invertible and extend the definition of ϕ by setting for an integer h

$$\phi(X^h \cdot z) := B^h \phi(z). \tag{3.2}$$

After we have defined the embedding ϕ and the action of X in $\mathbb{R}^n$ we take a closer look at the canonical number system $(p, \mathcal{N})$. To this end we define the fundamental domain by

$$\mathcal{F} := \left\{ z \in K \middle| z = \sum_{h \geq 1} a_h X^{-h}, a_h \in \mathcal{N} \right\}.$$

Similarly we define by $\mathcal{G} := \phi(\mathcal{F})$ the embedding of the fundamental domain in $\mathbb{R}^n$.

Following Gröchenig and Haas [5] we get that $(B, \phi(\mathcal{N}))$ is a matrix number system and, moreover, a so called *just touching covering system.*

Proposition 3.1 (*cf.* [5])**.** *Let $(p, \mathcal{N})$ be a number system and let λ denote the n-dimensional Lebesgue measure. Then we have*

(1) *$\mathcal{G}$ is compact.*
(2) *$\bigcup_{g \in \mathbb{Z}^n} (\mathcal{G} + g) = \mathbb{R}^n$.*
(3) *$\lambda((\mathcal{G} + g_1) \cap (\mathcal{G} + g_2)) = 0$ for every $g_1, g_2 \in \mathbb{Z}^n$ with $g_1 \neq g_2$.*
(4) *$\lambda(\mathcal{G}) > 0$.*

The following proposition relates the cardinality of $\mathcal{R}(T)$ with the Lebesgue measure of $\mathcal{S}(T)$. Moreover we get estimates for the boarder of $S(T)$ which are of interest for the estimation of the exponential sums in the following section.

Proposition 3.2. *Let β_1 and β_2 be as in* (2.2) *and set $\alpha = \beta_1/n\beta_2$. Furthermore let* $\mathrm{Vol}(\Lambda)$ *be the volume of the fundamental domain of the lattice Λ. Then the following assertions hold*

(1) $|\mathcal{R}(T)| = \frac{1}{\mathrm{Vol}(\Lambda)} \lambda(\mathcal{S}(T)) + \mathcal{O}\left(\lambda(\mathcal{S}(\mathcal{T}))^{1-\alpha}\right)$.
(2) $\lambda(\partial \mathcal{S}(T)) \ll |\mathcal{R}(T)|^{1-\alpha}$.
(3) $|2\mathcal{R}(T)| = 2^n |\mathcal{R}(T)| + \mathcal{O}\,|\mathcal{R}(T)|^{1-\alpha}$.

Proof. As we remarked above our choice of the embedding ϕ was motivated by the embedding used in the paper of Thuswaldner [16]. Since the matrix B is a block diagonal matrix we may apply Proposition 2.2 of [16] for each B_i in order to gain the result. □

4. Exponential sums

The main idea is to relax the restriction to residue classes by the usage of exponential sums. In this section we want to estimate all the exponential sums occurring in the proofs of Theorem 2.2 and Theorem 2.3. But before we start, we need some tools originating from linear algebra. Since $\mathcal{R}$ is obviously a free $\mathbb{Z}$-module of rank n, let $\lambda : \mathcal{R} \to \mathcal{R}$ be a linear mapping and $\{z_1, \dots, z_n\}$ be any basis of $\mathcal{R}$. Then

$$\lambda(z_j) = \sum_{i=1}^{n} a_{ij} z_i \quad (j = 1, \dots, n)$$

with $a_{ij} \in \mathbb{Z}$. The matrix $M(\lambda) = (a_{ij})$ is called the matrix of λ with respect to the basis $\{z_1, \dots, z_n\}$. For an element $r \in \mathcal{R}$ we define by $\lambda_r : \mathcal{R} \to \mathcal{R}$ the mapping of multiplication by r; that is $\lambda_r(z) = rz$ for every $z \in \mathcal{R}$. Then we define the norm $\mathrm{N}(r)$ and the trace $\mathrm{Tr}(r)$ of an element $r \in \mathcal{R}$ as the determinant and the trace of $M(\lambda_r)$, respectively, *i.e.*,

$$\mathrm{N}(r) := \det(M(\lambda_r)), \quad \mathrm{Tr}(r) := \mathrm{Tr}(M(\lambda_r)).$$

Note that these are unique despite of the used basis $\{z_1, \dots, z_n\}$. Similarly we define by Tr_i and Tr_{ij} the corresponding traces for $\mathcal{R}_i$ and $\mathcal{R}_{ij}$. We can canonically extend these notions to K and $\overline{K}$ by everywhere replacing $\mathbb{Z}$ by $\mathbb{Q}$ and $\mathbb{R}$, respectively.

Now we need a final ingredient. In particular, since the exponential sums will extend over the traces of elements we have to take the representants in the right ideal for the separation of the residue classes. In the classical case this is established by the usage of the different. Since in our case we have that $\mathcal{R}_{ij}$ are not necessarily the ring of integers, we have to generalize this concept. To this end for $M \subset K$ a $\mathbb{Z}$-module we denote by M^* the complementary set of M with respect to $\mathbb{Z}$, *i.e.*,

$$M^* := \{x \in K : \mathrm{Tr}(x \cdot M) \subset \mathbb{Z}\}.$$

If we take M to be equal to the ring of integers of a number field $\mathbf{K}$ we get that the complementary set is the inverse of the different $M^* = \mathfrak{d}^{-1}$ of this set. In our case we are not interested in the ring of integers, but in the order $\mathcal{R}$. We can show by similar means as for the different that $\mathcal{R}^*$ is a fractional ideal of K (*cf.* Chapter 13, (**H**) and (**I**) of [15]). In order to express the similarity of the different $\mathfrak{d}^{-1}$ and $\mathcal{R}^*$ we write for short

$$\mathfrak{r}^{-1} := \mathcal{R}^* = \{x \in K : \mathrm{Tr}(x \cdot \mathcal{O}) \subset \mathbb{Z}\}.$$

Finally we denote for $\mathfrak{q}$ an ideal of $\mathcal{R}$ by $\mathrm{R}(\mathfrak{q})$ a complete set of residues modulo $\mathfrak{r}^{-1}$. Similarly we denote by $\mathrm{R}(\mathfrak{q}_{ij})$ a complete set of the projection modulo $\mathfrak{r}_{ij}^{-1} := \pi_{ij}(\mathfrak{r}^{-1})$.

After this definitions we are now able to state the corresponding lemma of Hua, which will help us dropping the requirement, that the variable of summation lies in a certain residue class.

Lemma 4.1. *Let $\mathfrak{q}$ be an ideal of $\mathcal{R}$. Then we have for $z \in \mathcal{R}$ that*

$$\sum_{\xi \bmod \mathfrak{r}^{-1}} e(\mathrm{Tr}(\xi z)) = \begin{cases} |\mathrm{R}(\mathfrak{q})| & \text{if } z \in \mathfrak{q} \\ 0 & \text{otherwise,} \end{cases}$$

where ξ runs over a complete set of residues of $\mathfrak{q}\mathfrak{r}^{-1}$ mod $\mathfrak{r}^{-1}$.

Proof. First we assume that $\mathfrak{q} \mid z$. Then $\xi z \in \mathfrak{r}^{-1}$, $\mathrm{Tr}(\xi z) \in \mathbb{Z}$ and $e(\mathrm{Tr}(\xi z)) = 1$ for all ξ. Thus we have the first conclusion.

For the second conclusion we rewrite the sum. Noting that

$$\mathrm{Tr}(z) = \sum_{i=1}^{t} \mathrm{Tr}_i(z_i) = \sum_{i=1}^{t} \sum_{j=1}^{m_i} \mathrm{Tr}_{ij}(z_{ij})$$

where the traces denote the traces of the corresponding parts. Our choice of ϕ yields for the sum that

$$\sum_{\xi \in \mathrm{R}(\mathfrak{q})} e(\mathrm{Tr}(\xi z)) = \prod_{i=1}^{t} \prod_{j=1}^{m_i} \sum_{\xi \in \mathrm{R}(\pi_{ij}(\mathfrak{q}))} e(\mathrm{Tr}_{ij}(\xi z_{ij})).$$

Since $\mathcal{R}_{ij}$ is an order in a number field the last sum now resembles the original one in Theorem 3 of Hua [6] and we may follow the proof there. If $\mathfrak{q} \nmid z$, then there exists i and j such that $\mathfrak{q}_{ij} \nmid z_{ij}$. For this i and j there exists a $\xi_0 \in (\mathfrak{q}_{ij}\mathfrak{r}_{ij})^{-1}$ for which $\xi_0 z_{ij} \notin \mathfrak{r}_{ij}^{-1}$. In fact, if for all $\xi_0 \in (\mathfrak{q}_{ij}\mathfrak{r}_{ij})^{-1}$ we have that $\xi_0 z_{ij} \in \mathfrak{r}_{ij}^{-1}$, then

$$\mathfrak{r}_{ij}^{-1} \mid (\mathfrak{q}_{ij}\mathfrak{r}_{ij})^{-1} z_{ij}$$

and consequently $\mathfrak{q}_{ij} \mid z_{ij}$ contradicting our hypothesis. By the definition of the complementary set $\mathfrak{r}_{ij}^{-1} = \mathcal{R}_{ij}^*$ there is an integer y such that $e(\mathrm{Tr}_{ij}(y\xi_0 z_{ij})) \neq 1$. Since $y\xi_0 \in (\mathfrak{q}_{ij}\mathfrak{r}_{ij})^{-1}$, we get that

$$\sum_{\xi \in \mathrm{R}(\mathfrak{q}_{ij})} e(\mathrm{Tr}_{ij}(\xi z_{ij})) = \sum_{\xi \in \mathrm{R}(\mathfrak{q}_{ij})} e(\mathrm{Tr}_{ij}((\xi + y\xi_0) z_{ij})) = e(\mathrm{Tr}_{ij}(y\xi_0 z_{ij})) \sum_{\xi \in \mathrm{R}(\mathfrak{q}_{ij})} e(\mathrm{Tr}_{ij}(\xi z_{ij}))$$

and the second conclusion follows. □

The main idea is to apply the lemma above for the residue class of the elements and the corresponding version in the integers for the residue class of the additive function. To this end we will have to treat sums of the form

$$S(T,\xi,\ell) := \sum_{z\in\mathcal{R}(T)} e\left(\operatorname{Tr}(\xi z)+\frac{\ell}{m}f(z)\right), \tag{4.1}$$

where ξ goes over all residue classes modulo $\mathfrak{s}$ and ℓ over all modulo m. In the following two lemmas we will distinguish the cases of $m\nmid\ell$ and $m\mid\ell$. For the first one we will use the following

Lemma 4.2. *Assume that the same conditions hold as in the statement of Theorem 2.2. For any $\xi\in K$ we have, if $(p(1),m)=1$ and $m\nmid\ell$,*

$$S(T,\xi,\ell)\ll|\mathcal{R}(T)|^{\lambda}. \tag{4.2}$$

Proof. Without loss of generality we may suppose that $1\le\ell\le m-1$. Since the estimation depends on the sum of digits we will use an idea which goes back to Gelfond [4]. In particular, we will consider all those elements having a bounded length of expansion and cover the set $\mathcal{R}(T)$ by its translates. To this end we define the set of all elements of $\mathcal{R}$ having length at most k by

$$\mathcal{L}_{k-1} := \left\{ z\in\mathcal{R} : z=\sum_{h=0}^{k-1} a_h X^h, a\in\mathcal{N}\right\}.$$

Now we focus on the sum for $z\in\mathcal{L}_{k-1}$. To this end we note the definition of s_p to get

$$\sum_{z\in\mathcal{L}_{k-1}} e\left(\operatorname{Tr}(\xi z)+\frac{\ell}{m}s_p(z)\right) = \prod_{h=0}^{k-1}\sum_{a=0}^{|p(0)|-1} e\left(a\left(\operatorname{Tr}(\xi X^h)+\frac{\ell}{m}\right)\right). \tag{4.3}$$

Noting that the sum in the product is a geometric sum we get

$$\sum_{a=0}^{|p(0)|-1} e\left(a\left(\operatorname{Tr}(\xi X^h)+\frac{\ell}{m}\right)\right) = \frac{\sin\left(\pi\,|p(0)|\left(\operatorname{Tr}(\xi X^h)+\frac{\ell}{m}\right)\right)}{\sin\left(\pi\left(\operatorname{Tr}(\xi X^h)+\frac{\ell}{m}\right)\right)} \tag{4.4}$$

We fix h and set for short

$$\mu_r = \operatorname{Tr}(\xi X^{h+r})+\frac{\ell}{m}\quad(0\le r\le n).$$

Now we consider the $(n+1)$-fold product

$$Q = \left|\frac{\sin(\pi\,|p(0)|\,\mu_0)}{\sin(\pi\mu_0)}\cdots\frac{\sin(\pi\,|p(0)|\,\mu_n)}{\sin(\pi\mu_n)}\right|.$$

Writing $p=a_0+a_1X+\cdots+a_{n-1}X^{n-1}+a_nX^n$ we get

$$\begin{aligned}\sum_{r=0}^{n} a_r\mu_r &= \sum_{r=0}^{n} a_r\operatorname{Tr}(\xi X^{h+r})+\frac{\ell}{m}\sum_{r=0}^{n}a_r\\ &= \operatorname{Tr}(\xi X^h\,p)+\frac{\ell}{m}\sum_{r=0}^{n}a_r\\ &= \frac{\ell}{m}\sum_{r=0}^{n}a_r.\end{aligned}$$

Since $(p(1),m)=(\sum_{r=0}^{n}a_r,m)=1$ and $1\le\ell\le m-1$ we get that

$$\left\|\sum_{r=0}^{n}a_r\mu_r\right\| = \left\|\frac{\ell}{m}\sum_{r=0}^{n}a_r\right\| \ge \frac{1}{m}.$$

Thus there exists a $\rho\in\{0,\dots,n\}$ with

$$\|\mu_\rho\|\ge\frac{1}{(n+1)a_{max}m}, \tag{4.5}$$

where $a_{max}=\max_{0\le r\le n}a_r$.

We return to the sum in (4.3). The idea is to trivially estimate every factor in the product, except the one corresponding to ρ, where we apply (4.5). In particular, we note that the number of summands on the left of (4.4) is $|p(0)|$, which yields trivially for $r \neq \rho$

$$\left|\frac{\sin\left(\pi\left|p(0)\right|\mu_r\right)}{\sin\left(\pi\mu_r\right)}\right| \leq |p(0)|\,.$$

For the factor corresponding to ρ we use (4.5) to get

$$\left|\frac{\sin\left(\pi\left|p(0)\right|\mu_r\right)}{\sin\left(\pi\mu_r\right)}\right| \leq \left|\frac{\sin\left(\pi\left|p(0)\right|/((n+1)a_{max}m)\right)}{\sin\left(\pi/((n+1)a_{max}m)\right)}\right| < |p(0)|\,.$$

Thus we get for the $(n+1)$-fold product

$$Q \leq |p(0)|^n \left|\frac{\sin\left(\pi\left|p(0)\right|/((n+1)a_{max}m)\right)}{\sin\left(\pi/((n+1)a_{max}m)\right)}\right| = |p(0)|^{\lambda_2(n+1)}$$

where

$$\lambda_2 = \log\left(|p(0)|\left|\frac{\sin\left(\pi\left|p(0)\right|/((n+1)a_{max}m)\right)}{\sin\left(\pi/((n+1)a_{max}m)\right)}\right|\right)\left((n+1)\log|p(0)|\right)^{-1} < 1.$$

Plugging this into (4.3) yields

$$\left|\sum_{z\in\mathcal{L}_{k-1}} e\left(\mathrm{Tr}(\xi z)+\frac{\ell}{m}s_p(z)\right)\right| \leq |p(0)|^{k\lambda_2+n}\,. \tag{4.6}$$

The idea now is to tessellate the set $\mathcal{R}(T)$ by translates of $\mathcal{L}_{k-1}$. To this end we note that for $z\in\mathcal{L}_{k-1}$ and $a\in X^k\mathcal{R}$ we have by the additivity of the trace and the sum of digits function, that

$$e\left(\mathrm{Tr}(\xi(z+a))+\frac{\ell}{m}s_p(z+a)\right) = e\left(\mathrm{Tr}(\xi a)+\frac{\ell}{m}s_p(a)\right)e\left(\mathrm{Tr}(\xi z)+\frac{\ell}{m}s_p(z)\right).$$

This implies for all $a\in X^k\mathcal{R}$

$$\begin{aligned}\left|\sum_{z\in\mathcal{L}_{k-1}+a} e\left(\mathrm{Tr}(\xi z)+\frac{\ell}{m}s_p(z)\right)\right| &= \left|\sum_{z\in\mathcal{L}_{k-1}} e\left(\mathrm{Tr}(\xi(z+a))+\frac{\ell}{m}s_p(z+a)\right)\right| \\ &= \left|\sum_{z\in\mathcal{L}_{k-1}} e\left(\mathrm{Tr}(\xi z)+\frac{\ell}{m}s_p(z)\right)\right| \\ &\leq |p(0)|^{k\lambda_2+n}\,.\end{aligned}$$

Now we count the number of sets $\mathcal{L}_{k-1}+a$ with $a\in X^k\mathcal{R}$, which lie completely in $\mathcal{R}(T)$ and those covering the border, respectively. In particular, we define the sets

$$\begin{aligned}X &:= \left\{a\in X^k\mathcal{R} : (\mathcal{L}_{k-1}+a)\subset\mathcal{R}(T)\right\},\\ Y &:= \left\{a\in X^k\mathcal{R} : (\mathcal{L}_{k-1}+a)\cap\mathcal{R}(T)\neq\emptyset \text{ and } (\mathcal{L}_{k-1}+a)\cap(\mathcal{R}\setminus\mathcal{R}(T))\neq\emptyset\right\}.\end{aligned}$$

Thus we get

$$\begin{aligned}\left|\sum_{z\in\mathcal{R}(T)} e\left(\mathrm{Tr}(\xi z)+\frac{\ell}{m}s_p(z)\right)\right| &\leq \left|\sum_{a\in X}\sum_{z\in\mathcal{L}_{k-1}+a} e\left(\mathrm{Tr}(\xi z)+\frac{\ell}{m}s_p(z)\right)\right| \\ &\quad + \left|\sum_{a\in Y}\sum_{z\in(\mathcal{L}_{k-1}+a)\cap\mathcal{R}(T)} e\left(\mathrm{Tr}(\xi z)+\frac{\ell}{m}s_p(z)\right)\right| \\ &\leq |X|\,|p(0)|^{k\lambda_2+n} + |Y|\,|\mathcal{L}_{k-1}|\,.\end{aligned}$$

Using Proposition 3.2 for the estimation of the number of elements in X yields

$$|X| \ll \frac{|\mathcal{R}(T)|}{\mathrm{Vol}(\Lambda)\,|p(0)|^k}.$$

The idea for the estimation of the elements in Y, which are the elements near the border is to shrink and increase $\mathcal{S}(T)$ a bit in order to cover the area near the border by its difference. Thus we define for $\delta > 0$, $i = 1, \dots, t$ and $j = 1, \dots, m_i$ the sets $\mathcal{S}_{ij}(T)^{\pm}$ by

$$|x_k| \le l_{ijk}(T) \pm \delta,$$
$$x_k^2 + x_{k+1}^2 \le l_{ijk}(T)^2 \pm \delta.$$

In the same manner as above $\mathcal{S}(T)^{\pm}$ is the product of the sets $\mathcal{S}_{ij}(T)^{\pm}$,*i.e.*,

$$\mathcal{S}(T)^{\pm} = \left\{ z \in \mathbb{R}^n : z_{ij} \in \mathcal{S}_{ij}^{\pm}(T) \right\}. \tag{4.7}$$

Since $\operatorname{diam}(\ell_{k-1} + a) \le |p(0)| \operatorname{diam}(\mathcal{G})$ we set $\delta = |p(0)| \operatorname{diam}(\mathcal{G})$. Thus as one easily checks

$$\lambda\left(\mathcal{S}(T)^{+} \setminus \mathcal{S}(T)^{-}\right) \ll |\mathcal{S}(T)|^{1-\alpha} |p(0)|^{k}.$$

It follows by Proposition 3.2 that $\lambda(\mathcal{L}_{k-1} + a) = |p(0)|^k \lambda(\mathcal{G})$ and therefore

$$|Y| \ll |\mathcal{R}(T)|^{1-\alpha}.$$

Putting the two estimates together yields

$$\left| \sum_{z \in \mathcal{R}(T)} e\left(\operatorname{Tr}(\xi z) + \frac{\ell}{m} s_p(z) \right) \right| \ll \frac{|\mathcal{R}(T)|}{\operatorname{Vol}(\Lambda) |p(0)|^k} |p(0)|^{k\lambda_2 + n} + |\mathcal{R}(T)|^{1-\alpha} |p(0)|^k.$$

Finally we set

$$k := \left\lfloor \frac{\alpha}{2} \log_{|p(0)|} \left(|\mathcal{R}(T)| \right) \right\rfloor,$$

which yields

$$\left| \sum_{z \in \mathcal{R}(T)} e\left(\operatorname{Tr}(\xi z) + \frac{\ell}{m} s_p(z) \right) \right| \ll |\mathcal{R}(T)|^{1-((1-\lambda_2)\frac{\alpha}{2})} + |\mathcal{R}(T)|^{1-\frac{\alpha}{2}}.$$

This proves the proposition for $\lambda = \max(1 - ((1-\lambda_2)\frac{\alpha}{2}), 1 - \frac{\alpha}{2})$.

□

For the second case we have an exponential sum in a number field which we treat by usual means.

Lemma 4.3. *Assume that the same conditions hold as in the statement of Theorem 2.2. Let* $\mathfrak{q}$ *be an ideal of* $\mathcal{R}$*. Then*

$$\sum_{\xi \not\equiv 0 \bmod \mathfrak{r}^{-1}} \sum_{z \in \mathcal{R}(T)} e\left(\operatorname{Tr}(\xi z) \right) \ll \mathrm{R}(\mathfrak{q}) |\mathcal{R}(T)|^{1-\alpha},$$

where $\alpha > 0$ *and* ξ *runs over a complete set of residues of* $\mathfrak{q}\mathfrak{r}^{-1} \bmod \mathfrak{r}^{-1}$ *not containing the element* $0 \bmod \mathfrak{r}^{-1}$.

Proof. Since the sum of digits function is missing here, we may use the structure of $\mathcal{R}$ and the projections π_{ij} in order to estimate this sum. Thus it suffices to focus on a single $\mathcal{R}_{ij}$ only. In particular, let $\mathfrak{r}_{ij} := \pi_{ij}(\mathfrak{r})$ then as ξ runs through a complete set of residues modulo $\mathfrak{r}^{-1}$, so does $\xi_{ij} := \pi_{ij}(\xi)$ for $\mathfrak{r}_{ij}^{-1}$. Thus it suffices to estimate

$$\sum_{\xi \not\equiv 0 \bmod \mathfrak{r}^{-1}} \sum_{z \in \mathcal{R}(T)} e\left(\operatorname{Tr}(\xi z) \right) = \prod_{i=1}^{t} \prod_{j=1}^{m_i} {\sum_{\xi_{ij} \bmod \mathfrak{r}_{ij}^{-1}}}' \sum_{z_{ij} \in \mathcal{R}_{ij}(T)} e\left(\operatorname{Tr}_{ij}(\xi_{ij} z_{ij}) \right)$$

where $\sum'$ denotes that we exclude the case where all $\xi_{ij} = 0$ which corresponds to $\xi \equiv 0 \bmod \mathfrak{r}^{-1}$.

Throughout the rest of the proof we fix i and j such that $\xi_{ij} \not\equiv 0 \bmod \mathfrak{r}_{ij}^{-1}$. We drop the indices where possible, *i.e.*, we set $\mathcal{R} = \mathcal{R}_{ij}$, $\mathfrak{r} = \mathfrak{r}_{ij}$ and $\mathfrak{q} = \pi(\mathfrak{q}_{ij})$. Let $\beta := \beta_{i1}$ be a zero of p_i, then clearly $\mathcal{R} \cong \mathbb{Z}[\beta]$. Let $\mathbf{K} := \mathbb{Q}(\beta)$ be the corresponding algebraic number field an $\mathbf{Z_K}$ be its ring of integers. Then $\mathcal{R} \subset \mathbf{Z_K}$ is an order in $\mathbf{K}$ and $\mathfrak{r}^{-1} = \mathcal{R}^*$ (where the complement is with respect to $\mathbf{K}$). We denote by Tr the trace and by N the norm of an element of $\mathbf{K}$ over $\mathbb{Q}$, respectively.

Let R be a complete residue system $\bmod \mathfrak{q}$. As in the proof of Lemma 4.2 we want to tessellate the set $\mathcal{R}(T)$ by translates of R. To this end we again distinguish between those translates being totally inside and those covering the border. In particular, we define the sets,

$$X := \{a \in \mathfrak{q} : a + R \subset \mathcal{R}(T)\},$$
$$Y := \{a \in \mathfrak{q} : (a + R) \cap \mathcal{R}(T) \neq \emptyset \text{ and } (a + R) \cap (\mathcal{R} \setminus \mathcal{R}(T)) \neq \emptyset\}.$$

Then we may split up the sum under consideration as follows

$$\begin{aligned}\sum_{\xi\not\equiv 0 \bmod \mathfrak{r}^{-1}} \sum_{z\in\mathcal{R}(T)} e\left(\mathrm{Tr}(\xi z)\right) &= \sum_{\xi\not\equiv 0 \bmod \mathfrak{r}^{-1}} \sum_{a\in X} \sum_{z\in a+R} e\left(\mathrm{Tr}(\xi z)\right) \\ &\quad + \sum_{\xi\not\equiv 0 \bmod \mathfrak{r}^{-1}} \sum_{a\in Y} \sum_{z\in (a+R)\cap\mathcal{R}(T)} e\left(\mathrm{Tr}(\xi z)\right) \\ &=: R_1 + R_2.\end{aligned}$$

We start with the estimation of R_1. Because $\mathfrak{q}\mathfrak{r}(\mathfrak{q}\mathfrak{r})^{-1} = \mathbf{Z_K}$, there exists an $s \in \mathfrak{q}\mathfrak{r}$ with $s^{-1} \in (\mathfrak{q}\mathfrak{r})^{-1}$. Thus we have

$$\sum_{z\in a+R} e\left(\mathrm{Tr}(\xi z)\right) = \sum_{z\in a+R} e\left(\mathrm{Tr}\left(\frac{z}{s}\xi s\right)\right).$$

Since $s^{-1}z$ runs through a complete set of residues mod $\mathfrak{r}^{-1}$ in $(\mathfrak{q}\mathfrak{r})^{-1}$) and since $\xi s \notin \mathfrak{q}$ is an algebraic integer, we get by an application of Lemma 4.1 that

$$\sum_{z\in a+R} e\left(\mathrm{Tr}(\xi z)\right) = 0$$

and hence $R_1 = 0$.

For R_2 we get together with Lemma 4.1 that

$$\begin{aligned}\left|\sum_{a\in Y} \sum_{z\in (a+R)\cap\mathcal{R}(T)} \sum_{\xi\not\equiv 0 \bmod \mathfrak{r}^{-1}} e\left(\mathrm{Tr}(\xi z)\right)\right| &\leq \left|\sum_{a\in Y} \sum_{z\in (a+R)\cap\mathcal{R}(T)} \left(\sum_{\xi \bmod \mathfrak{r}^{-1}} e\left(\mathrm{Tr}(\xi z)\right) + \mathrm{R}(\mathfrak{q})\right)\right| \\ &\leq \left|\sum_{a\in Y} 2\mathrm{R}(\mathfrak{q})\right|.\end{aligned}$$

Now we want to use the same idea for counting the number of elements near the border, as in the proof of Lemma 4.2. To this end we recall the definition of $\mathcal{S}(T)^{\pm}$ in (4.7). Rephrasing the steps with $a + R$ instead of $\mathcal{L}_{k-1} + a$ yields $Y \ll |\mathcal{R}(T)|^{1-\alpha}$ and thus we get in the same manner as above that

$$R_2 \ll \mathrm{N}(\mathfrak{q})\,|\mathcal{R}(T)|^{1-\alpha}.$$

which proves the lemma. □

5. Proof of the Theorems 2.2 and 2.3

Proof of Theorem 2.2. Throughout this proof we fix the ideal $\mathfrak{s} \lhd \mathcal{R}$ and a system of residues ξ mod $\mathfrak{s}$. Since π is an isomorphism we get that

$$\pi(\mathfrak{s}) = (\mathfrak{s}_1, \ldots, \mathfrak{s}_t) = (\mathfrak{s}_{11}, \ldots, \mathfrak{s}_{t,m_t}),$$

where $\mathfrak{s}_i := \pi_i(\mathfrak{s})$ and $\mathfrak{s}_{ij} := \pi_{ij}(\mathfrak{s})$ for $i = 1, \ldots, t$ and $j = 1, \ldots, m_i$.

By an application of Lemma 4.1 we can rephrase $\mathcal{V}_p(\mathcal{R}(T))$ as follows

$$\begin{aligned}\#\mathcal{V}_p(\mathcal{R}(T)) &= \#\left\{z \in \mathcal{R} : z \equiv a \bmod \mathfrak{s} \text{ and } s_p(z) \equiv h \bmod m\right\}\\ &= \frac{1}{m}\sum_{w=0}^{m-1}\frac{1}{|\mathrm{R}(\mathfrak{s})|}\sum_{\xi \bmod \mathfrak{r}^{-1}}\sum_{z\in\mathcal{R}(T)} e\left(\mathrm{Tr}(\xi(z-a)) + w\frac{s_p(z)-h}{m}\right)\\ &= \frac{|\mathcal{R}(T)|}{m\,|\mathrm{R}(\mathfrak{s})|} + \frac{1}{m\,|\mathrm{R}(\mathfrak{s})|}\sum_{\xi\not\equiv 0 \bmod \mathfrak{r}^{-1}}\sum_{z\in\mathcal{R}(T)} e\left(\mathrm{Tr}(\xi(z-a))\right)\\ &\quad + \frac{1}{m\,|\mathrm{R}(\mathfrak{s})|}\sum_{\xi \bmod \mathfrak{r}^{-1}}\sum_{w=1}^{m-1}\sum_{z\in\mathcal{R}(T)} e\left(\mathrm{Tr}(\xi(z-a)) + w\frac{s_p(z)-h}{m}\right).\end{aligned}$$

Now we estimate

$$\sum_{\xi\not\equiv 0 \bmod \mathfrak{r}^{-1}}\sum_{z\in\mathcal{R}(T)} e\left(\mathrm{Tr}(\xi(z-a))\right) \ll |\mathrm{R}(\mathfrak{s})|\,|\mathcal{R}(T)|^{1-\alpha}$$

with help of Lemma 4.3 and

$$\sum_{\xi \bmod \mathfrak{r}^{-1}}\sum_{w=1}^{m-1}\sum_{z\in\mathcal{R}(T)} e\left(\mathrm{Tr}(\xi(z-a)) + w\frac{s_p(z)-h}{m}\right) \ll |\mathcal{R}(T)|^{\lambda_1}$$

with help of Lemma 4.2 which proves the theorem. □

Proof of Theorem 2.3. Let $\mathfrak{q}$ be an ideal of $\mathcal{R}$ such that

$$\begin{aligned}\{x+y-z : x\in\mathcal{A},\mathcal{B}, z\in 2\mathcal{R}(T)\}\cap\mathfrak{q} &= \{0\},\\ \{x_1-x_2 : x_1,x_2\in\mathcal{A}\}\cap\mathfrak{q} &= \{0\},\\ \{y_1-y_2 : y_1,y_2\in\mathcal{B}\}\cap\mathfrak{q} &= \{0\}.\end{aligned} \tag{5.1}$$

Clearly $\mathfrak{q}$ depends on T but this will cause no problems in our proof. In order to simplify notation we define functions separating $x\in\mathcal{A}$, $y\in\mathcal{B}$ and $z\in 2\mathcal{R}(T)$, *i.e.*,

$$\begin{aligned}F(\xi) &:= \sum_{x\in\mathcal{A}} e(\mathrm{Tr}(\xi x)), & G(\xi) &:= \sum_{y\in\mathcal{B}} e(\mathrm{Tr}(\xi y)),\\ H_w(\xi, 2\mathcal{R}(T)) &:= \sum_{z\in 2\mathcal{R}(T)} e\left(\mathrm{Tr}(\xi z) + \frac{w}{m}s_p(z)\right), & I_w &:= \frac{1}{\mathrm{N}(\mathfrak{q})}\sum_{\xi} F(\xi)G(\xi)\overline{H_w(\xi, 2\mathcal{R}(T))},\end{aligned}$$

where $\sum_\xi$ runs over a complete set of residues $\bmod \mathfrak{r}^{-1}$ in $(\mathfrak{q}\mathfrak{r})^{-1}$. Now by an application of Lemma 4.1 we may write

$$m\cdot|\{(x,y)\in\mathcal{A}\times\mathcal{B} : x+y\in\mathcal{U}_{h,m}(2\mathcal{R}(T))\}| = \sum_{w=0}^{m-1} I_w$$

As in the proof of Theorem 2.2 we separate the term I_0 and get by noting the requirements on $\mathfrak{q}$ in (5.1) that

$$I_0 = \frac{1}{\mathrm{N}(\mathfrak{q})}\sum_{\xi}\sum_{x\in\mathcal{A}}\sum_{y\in\mathcal{B}}\sum_{z\in 2\mathcal{R}(T)} e(\mathrm{Tr}(\xi(x+y-z))) = \sum_{x\in\mathcal{A}}\sum_{y\in\mathcal{B}} 1 = |\mathcal{A}|\,|\mathcal{B}|.$$

Thus subtracting the main part and taking the modulus yields

$$\left|m\cdot|\{(x,y)\in\mathcal{A}\times\mathcal{B} : x+y\in\mathcal{U}_{h,m}(2\mathcal{R}(T))\}| - \frac{|\mathcal{A}|\,|\mathcal{B}|}{m}\right| = \left|\sum_{w=1}^{m-1} I_w\right| \le \sum_{w=1}^{m-1}|I_w|.$$

In order to estimate I_w for $1 \le w \le m-1$ we use Cauchy's inequality together with Lemma 4.2 to gain

$$\begin{aligned}
|I_w| &\le \frac{\max_{\eta\in K}(|H_w(\eta, 2\mathcal{R}(T))|)}{\mathrm{N}(\mathfrak{q})} \sum_{\xi} |F(\xi)|\,|G(\xi)| \\
&\le \frac{\gamma_1\,|2\mathcal{R}(T)|^{\lambda_1}}{\mathrm{N}(\mathfrak{q})} \left(\left(\sum_{\xi} |F(\xi)|^2\right)\left(\sum_{\xi} |G(\xi)|^2\right)\right)^{\frac{1}{2}} \\
&\le \frac{\gamma_1\,|2\mathcal{R}(T)|^{\lambda_1}}{\mathrm{N}(\mathfrak{q})} \left(\mathrm{N}(\mathfrak{q})^2\,|\mathcal{A}|\,|\mathcal{B}|\right)^{\frac{1}{2}} \\
&\ll \gamma_1\,|2\mathcal{R}(T)|^{\lambda_1} \left(|\mathcal{A}|\,|\mathcal{B}|\right)^{\frac{1}{2}}.
\end{aligned}$$

This proves Theorem 2.3. □

References

[1] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő, and J. M. Thuswaldner, *Generalized radix representations and dynamical systems. I*, Acta Math. Hungar. **108** (2005), no. 3, 207–238.

[2] S. Akiyama and H. Rao, *New criteria for canonical number systems*, Acta Arith. **111** (2004), no. 1, 5–25.

[3] Shigeki Akiyama and Attila Pethő, *On canonical number systems*, Theoret. Comput. Sci. **270** (2002), no. 1-2, 921–933.

[4] A. O. Gel′fond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith. **13** (1967/1968), 259–265.

[5] K. Gröchenig and A. Haas, *Self-similar lattice tilings*, J. Fourier Anal. Appl. **1** (1994), no. 2, 131–170.

[6] L.-K. Hua, *On exponential sums over an algebraic number field*, Canadian J. Math. **3** (1951), 44–51.

[7] I. Kátai and B. Kovács, *Kanonische Zahlensysteme in der Theorie der quadratischen algebraischen Zahlen*, Acta Sci. Math. (Szeged) **42** (1980), no. 1-2, 99–107.

[8] ———, *Canonical number systems in imaginary quadratic fields*, Acta Math. Acad. Sci. Hungar. **37** (1981), no. 1-3, 159–164.

[9] I. Kátai and J. Szabó, *Canonical number systems for complex integers*, Acta Sci. Math. (Szeged) **37** (1975), no. 3-4, 255–260.

[10] B. Kovács and A. Pethő, *Number systems in integral domains, especially in orders of algebraic number fields*, Acta Sci. Math. (Szeged) **55** (1991), no. 3-4, 287–299.

[11] ———, *On a representation of algebraic integers*, Studia Sci. Math. Hungar. **27** (1992), no. 1-2, 169–172.

[12] M. G. Madritsch and A. Pethő, *Asymptotic normality of additive functions on polynomial sequences in canonical number systems*, Journal of Number Theory **131** (2011), no. 9, 1553 – 1574.

[13] C. Mauduit and A. Sárközy, *On the arithmetic structure of sets characterized by sum of digits properties*, J. Number Theory **61** (1996), no. 1, 25–38.

[14] A. Pethő, *On a polynomial transformation and its application to the construction of a public key cryptosystem*, Computational number theory (Debrecen, 1989), de Gruyter, Berlin, 1991, pp. 31–43.

[15] P. Ribenboim, *Classical theory of algebraic numbers*, Universitext, Springer-Verlag, New York, 2001.

[16] J. M. Thuswaldner, *The sum of digits function in number fields: distribution in residue classes*, J. Number Theory **74** (1999), no. 1, 111–125.

(M. G. Madritsch) Department of Analysis and Computational Number Theory
Graz University of Technology
8010 Graz, Austria
E-mail address: madritsch@math.tugraz.at