The Thue-Morse and Rudin-Shapiro sequences at primes in principal number fields

Sary Drappeau, Gautier Hanna

THE THUE-MORSE AND RUDIN-SHAPIRO SEQUENCES AT PRIMES IN PRINCIPAL NUMBER FIELDS

S. DRAPPEAU AND G. HANNA

1. Introduction

1.1. **Digits and multiplicative structure.** The present work is concerned with the interaction between the additive, multiplicative, and numeration properties of numbers, which is a reccurrent motivating theme in analytic number theory. The recent years, a lot of progress has been made on our understanding of digits of multiplicatively constrained integers (*e.g.* primes): see [FM96b, FM96a, DT05, MR10, MR15, Han17, DMR09] for sum of digits of primes in residue classes, [HK08, Bou15, Swa19] for primes with restricted digits, or [MR09, DMR11, DM12, MR18, DMR19] for digits of polynomials. Here we are interested in two particular digital functions (defined in terms of digit expansion), the sum-of-digits function

$$s_q(n) := \sum_{0\le j<J} b_j \qquad \text{if } n = \sum_{0\le j<J} b_j q^j,\ b_j \in \{0,\dots,q-1\}.$$

and the Rudin-Shapiro sequence

$$r(n) := \sum_{0\le j<J-1} b_j b_{j+1} \qquad \text{if } n = \sum_{0\le j<J} b_j 2^j,\ b_j \in \{0,1\}.$$

Given a fixed integer m, the functions $n \mapsto s_q(n) \pmod m$ and $n \mapsto r(n) \pmod m$ are two particular instances of automatic sequences, and it is predicted by Sarnak's Möbius randomness conjecture [Sar12] (in one of its lowest complexity case) that they should not be correlated with integer factorization, in the precise sense that the Möbius function should have average zero along automatic sequences. For the sum-of-digit function, this expectation goes back to conjectures of Gel'fond [Gel68]. This question was solved, in a strong quantitative form, by Mauduit and Rivat [MR10] for the sum-of-digit case, then by the same authors [MR15] for the Rudin-Shapiro case; and finally the full Sarnak conjecture for automatic sequences was proved by Müllner [Mül17]. The arguments in [MR15] are one of the crucial inputs in [Mül17].

1.2. **Digits of integers in number fields.** Our aim is to take up the study [MR15] and explore the corresponding questions in number fields. Let $K/\mathbb{Q}$ be an algebraic extension, and $\mathcal{O}_K$ be its ring of integers. We endow $\mathcal{O}_K$ with a numeration structure, in the following way.

Definition 1. *Let $q \in \mathcal{O}_K \smallsetminus \{0\}$ and $\mathcal{D} \subset \mathcal{O}_K$ be a set of representatives of $\mathcal{O}_K/(q)$. We call the pair $(q,\mathcal{D})$ a* number system with the finiteness property *(FNS) if:*

- $0 \in \mathcal{D}$,
- *the Galois conjugates of q have moduli larger than* 1,
- *every $n \in \mathcal{O}_K$ has an expansion of the form $n = \sum_{0\le j<J} b_j q^j$, where $b_j \in \mathcal{D}$.*

Date: June 20, 2019.

We make a small account of works on these systems in Section 2.1 below; see also Section 3.1 of the survey [BBLT06] for a discussion in the broad context of numeration systems.

The smallest $J \in \mathbb{N}_{\geq 0}$ such that $b_j = 0$ for $j \geq J$ will be called the *length* of n. The simplest non-rational example is the case $K = \mathbb{Q}(i)$, $q = -1 + i$, and $\mathcal{D} = \{0, 1\}$; see [Knu81, p. 206]. We make an account of existing works on number systems relevant to our case in Section 2.1 below, and refer to [BBLT06] for more references on this topic.

Our aim is to show that this numeration structure does not correlate with the multiplicative structure of $\mathcal{O}_K$. We will assume, throughout, that $\mathcal{O}_K$ is principal, so that it is a unique factorization domain. We present our results in the representative cases of the generalized sum-of-digit and Rudin-Shapiro functions.

Define, for all $n \in \mathcal{O}_K$, the sum-of-digits function $s(n) = s_{q,\mathcal{D}}(n)$ as

$$s_{q,\mathcal{D}}(n) := \sum_{0 \leq j < J} b_j \qquad \text{if } n = \sum_{0 \leq j < J} b_j q^j,\ b_j \in \mathcal{D}. \tag{1.1}$$

Several aspects of this function have been studied in the past: asymptotic formula for the mean-value and fluctuations in its the constant term [GKP98, Thu98b], equidistribution modulo 1 [GL99], central limit theorems [GT00, Mad10], and equidistribution along squares [Mor10]. In the case $q = -1 + i$, $\mathcal{D} = \{0, 1\}$, we have $s_{q,\mathcal{D}}(n) \in \mathbb{N}$, and as a special case of [GL99, Theorem 11] we have that for any $\alpha \in \mathbb{R} \smallsetminus \mathbb{Q}$, the multi-sets

$$\{\alpha s_q(n),\ n \in \mathcal{O}_K \text{ of length } \leq J\}$$

become equidistributed modulo 1 as $J \to \infty$.

We are interested in this question when n is restricted to be prime in $\mathcal{O}_K$. In [DRS08, Mor12], this problem was addressed in the Gaussian integer setting $K = \mathbb{Q}(i)$, using the approach of [MR10]. The question of whether the same method holds for other number systems was left open; the case when K is imaginary quadratic has specific aspects, notably the fact that multiplication by a complex number is an isometry, which are implicitely at play in [Mor12]. We show that the expected statement in fact holds in full generality.

Theorem 1. *Suppose that $\mathcal{O}_K$ is a unique factorization domain, let $(q, \mathcal{D})$ be a number system with the finiteness property, and $\phi : K \to \mathbb{R}$ be a linear form. Then, as $J \to \infty$, the multi-sets*

$$\{\phi(s_q(p)),\ p \in \mathcal{O}_K \text{ prime of length } \leq J\} \tag{1.2}$$

becomes equidistributed modulo 1 if and only if $\phi(b) \in \mathbb{R} \smallsetminus \mathbb{Q}$ for some $b \in \mathcal{D}$.

Under the appropriate conditions, which are more involved, a similar equidistribution statement holds for linear maps $\phi : K \to \mathbb{R}^d$ where $d = [K : \mathbb{Q}]$. Note also that we have chosen, for simplicity, to control the size of p by its digital length.

We next turn to the Rudin-Shapiro sequence, which was introduced due to the extremal properties of its associated trigonometric polynomials [Rud59, Sha53]. We consider the multidimensional variants constructed in [BvH05]: we call $(q, \mathcal{D})$ a *binary* FNS if $\mathrm{card}(\mathcal{D}) = 2$. Binary NFS were characterized in [BvH06]. We define a function $r_{q,\mathcal{D}} : \mathcal{O}_K \to \mathbb{N}$ by

$$r_{q,\mathcal{D}}(n) := \sum_{0 \leq j < J-1} \mathbf{1}(b_j b_{j+1} \neq 0) \qquad \text{if } n = \sum_{0 \leq j < J} b_j q^j,\ b_j \in \mathcal{D}, \tag{1.3}$$

where $\mathbf{1}(n \neq 0)$ is 0 or 1 according to whether $n = 0$ or not.

We are interested in this sequence because it is a non-trivial and natural instance of a digital function which has much less useful analytic properties than $s_{q,\mathcal{D}}$: it is not

q-additive, and by analogy with the rational case, we do not expect its discrete Fourier transforms to have better than square-root cancellation in L^1 norm (as opposed to $s_{q,\mathcal{D}}$). The arguments in [MR15] were partly designed to work without these useful analytic properties.

In [DGL08], this function was considered in the general setting of "block-additive functions". There it was shown, using ergodic methods, that for any $\alpha \in \mathbb{R} \smallsetminus \mathbb{Q}$, the multi-sets

$$\{\alpha r_{q,\mathcal{D}}(n),\ n \in \mathcal{O}_K \text{ of length } \leq J\}$$

become equidistributed modulo 1 as $J \to \infty$[1].

We show that the corresponding statement holds for primes in full generality.

Theorem 2. *Suppose that K is a unique factorization domain, let $(q, \mathcal{D})$ be a binary FNS, and $\alpha \in \mathbb{R} \smallsetminus \mathbb{Q}$. Then, as $J \to \infty$, the multi-sets*

$$\{\alpha r_{q,\mathcal{D}}(p),\ p \in \mathcal{O}_K \text{ prime of length} \leq J\} \tag{1.4}$$

becomes equidistributed modulo 1.

As we mentioned in the introduction, in the recent work [Mül17] pertaining to the case $K = \mathbb{Q}$, the Sarnak conjecture over was fully solved for automatic sequences detecting integers given by their usual digital expansion. By combining the arguments of Sections 4.1–4.2 of [Mül17] with the work presented here, we expect that the Möbius function

$$\mu_K(n) = \begin{cases} (-1)^k & \text{if } n \text{ is, up to units, a product of } k \text{ distinct primes,} \\ 0 & \text{otherwise,} \end{cases}$$

is asymptotically orthogonal to the output of an automaton reading the digits of f in any FNS. Here, however, we choose to remain in the formalism of [MR15], having in mind only the sum-of-digits and the Rudin-Shapiro sequence. The input required to handle arbitrary automatic sequences does not substantially differ from [Mül17] and we believe it would obfuscate the "number field" aspects of our arguments. We also believe that by mixing the arguments of [MR18] with the ones presented here, one should be able to show that the multi-sets $\{\alpha r_{q,\mathcal{D}}(n^2), n \in \mathcal{O}_K \text{ of length} \leq J\}$ become equidistributed as $J \to \infty$ if $\alpha \notin \mathbb{Q}$.

Another interesting direction would be to restrict the sets (1.2), (1.4) to *rationals* that are prime in $\mathcal{O}_K$, which form a very sparse subset of all primes. The arguments presented here are, in their present form, not effective enough to address this question. Note however that partial results have been proved in [GKP98] for the average of the sum-of-digit function, without the primality condition.

1.3. **Overview.** The difficulties we encounter in Theorems 1 and 2 are of two kinds.

The first is related to point-counting on lattices, and the "skewing phenomenon". The multiplication by q, viewed as a map on the lattice $\mathcal{O}_K$, can be quite far from an isometry in general, depending on the relative moduli of Galois conjugates of q. This can induce an inefficiency in lattice-point counting estimates in large dilates $q^\nu \mathcal{O}_K$. The effect of this skewing will be counteracted by systematically using Dirichlet's theorem on the structure of the group of units.

[1]The authors [DGL08] work exclusively in the Knuth setting $(q, \mathcal{D}) = (-1 + i, \{0, 1\})$, but the statement above can be easily deduced from our arguments.

The second, more substantial difficulty is the harmonic analysis of the fundamental tile

$$\mathcal{F} = \{\sum_{j\geq 1} b_j q^{-j}, b_j \in \mathcal{D}\}.$$

By contrast with earlier works, the method of [MR15], which we take up here, makes a particularly extensive use of information on the Fourier transform $\widehat{\chi}_{\mathcal{F}}$ of the indicator function $\chi_{\mathcal{F}}$ of $\mathcal{F}$ (viewed as a subset of $\mathbb{R}^d$ through a choice of basis of $\mathcal{O}_K$). In the classical case $K = \mathbb{Q}$, the fundamental tile is an interval (see [MR15, Lemma 1]), so that we have explicit expressions and bounds for its Fourier transform. In the general case, and in fact already for the Knuth setting $K = \mathbb{Q}(i)$, $(q, \mathcal{D}) = (-1 + i, \{0, 1\})$, the fundamental tile has a non-trivial fractal boundary, known as the "twin-dragon" ([Man82, p. 66], [Knu81, p. 206]). The Fourier transform $\widehat{\chi}_{\mathcal{F}}$ does not decay uniformly enough for the method to naively go through[2]. To handle this, we rework the arguments of [MR15] so as to require as few information of the Fourier transform as possible: as we will show, the arguments of [MR15] can be recast so that the only essential input is an L^2 bound on $\widehat{\chi}_{\mathcal{F}}$, which we will obtain easily from Parseval's identity.

2. Setting

2.1. **Number field.** Let K be a number field, with its trace map denoted $\langle x\rangle = \mathrm{Tr}(x) = \mathrm{Tr}_{K/\mathbb{Q}}(x)$. We denote $\mathcal{O}^\vee$ the dual of $\mathcal{O}$ for the scalar product $(x, y) \mapsto \mathrm{Tr}(xy)$. It is a fractional ideal, and the different ideal $D_K := (\mathcal{O}^\vee)^{-1} \subset \mathcal{O}$ is of norm equal to the discrimant of K [Nar04, Chapter 4.1].

Given an base $q \in \mathcal{O}$, all of whose conjugates have moduli greater than 1, and a set of digits $\mathcal{D}$, assume that any element of $n \in \mathcal{O}$ has a unique base q expansion

$$n = \sum_{j=0}^{r} b_j q^j, \qquad r \in \mathbb{N}, b_j \in \mathcal{D}.$$

On the other hand, when the ring $\mathcal{O}$ is principal, n also possesses a factorisation $n = p_1 \cdots p_\ell$ as a product of prime elements, which is also unique up to order and multiplication by units.

Let $(\omega_1, \ldots, \omega_d)$ be a $\mathbb{Z}$-basis of $\mathcal{O}$, and $(\omega_1^\vee, \ldots, \omega_d^\vee)$ its dual basis $\mathcal{O}^\vee$. For any $(x_j)_{1\leq j\leq d}$, $(y_j)_{1\leq j\leq d} \in \mathbb{R}^d$, denote

$$\iota(x_1, \ldots, x_d) = \sum_{j=1}^{d} x_j \omega_j, \qquad \iota^\vee(y_1, \ldots, y_d) = \sum_{j=1}^{d} y_j \omega_j^\vee.$$

Note that $K = \iota(\mathbb{Q}^d) = \iota^\vee(\mathbb{Q}^d)$, and

$$\mathcal{O} = \iota(\mathbb{Z}^d), \qquad \mathcal{O}^\vee = \iota^\vee(\mathbb{Z}^d). \tag{2.1}$$

We fix a norm $\|\cdot\|$ on $\mathbb{R}^n$, and when $x \in K$, we use the notation $\|x\|$ to mean $\|\iota^{-1}(x)\|$.

We pick a base $q \in \mathcal{O}_K$ and assume that all conjugates of q have modulus > 1. Let $\mathcal{D}$ be a set of representatives of $\mathcal{O}_K/(q)$ containing 0. Borrowing the terminology of [PT18], we call such a pair $(q, \mathcal{D})$ a number system. If every $n \in \mathcal{O}_K$ has a finite expression

$$n = \sum_{j=0}^{r} b_j q^j$$

[2]The analysis of the rates of decay of functions such as $\widehat{\chi}_{\mathcal{F}}$ is in fact an important object of study in wavelet theory; see the references in Section 3.2.2.

with $b_j \in \mathcal{D}$ and $r \geq 0$, then we say that $(q, \mathcal{D})$ has the finitess property. Note that such an expansion, if it exists, is unique. We use the abbreviation FNS to designate a number system with the finiteness property.

Given a pair $(q, \mathcal{D})$, Kovács and Pethő [KP91] have shown that the question of whether $(q, \mathcal{D})$ is a FNS can be decided algorithmically in finite time (they also characterize completely such number systems in positive characteristics). Gröchenig and Haas [GH94, Theorem 2.2] have shown that it corresponds exactly to a certain explicit matrix having spectral radius < 1 (which is equivalent to the existence of cycles in a certain directed graph, which we will mention below in Section 3.2.1). The FNS are characterized for $d = 1$ in Theorem 2.3 of [GH94]; in the same paper, the authors characterize the numbers q which can arise as the bases of FNS for the field $K = \mathbb{Q}(i)$.

If $(q, \mathcal{D})$ is a number system with $\mathcal{D} = \{0, \dots, N(q) - 1\}$, the pair $(q, \mathcal{D})$ is called a *canonical number system* (CNS). The fields K which admit a CNS with the finitess property have been characterized in [Kov81]: they are exactly those fields for which $\mathcal{O}$ has a primitive element. Many works have been devoted to deciding whether a given pair $(q, \mathcal{D})$ is a CNS with the finiteness property. The problem was completely solved in the quadratic case $d = 2$ by Kátai and Szabó [KS75] and Kátai and Kovács [KK80, KK81]. For $d \geq 3$, only partial results are known; Akiyama and Pethő [AP02] construct an algorithm which determines whether $(q, \mathcal{D})$ is a CNS with the finiteness property using only the coefficients of the minimal polynomial of q. Other partial results have been proved for $d = 3$ [ABP03] and $d = 4$ [BHP06].

Returning to general number systems, Germán and Kovács [GK07] proved that any q having all its conjugates of moduli $< 1/2$ admits a set of digits $\mathcal{D}$ for which $(q, \mathcal{D})$ is a FNS.

From now on, we assume that $(q, \mathcal{D})$ has the finiteness property.

Let $\mathcal{F}$ be the fundamental tile

$$\mathcal{F} = \Big\{ \sum_{j=1}^{r} b_j q^{-j}, r \geq 1, b_j \in \mathcal{D} \Big\}. \tag{2.2}$$

We will state in Section 3.2.2 below the basic properties of $\mathcal{F}$; for now, let us simply mention that there exist $R_{\mathcal{F}}^-, R_{\mathcal{F}}^+ > 0$ (depending on $(q, \mathcal{D})$ and $\|\cdot\|$) such that

$$\{x \in K, \|x\| \leq R_{\mathcal{F}}^-\} \subset \mathcal{F} \subset \{x \in K, \|x\| \leq R_{\mathcal{F}}^+\}. \tag{2.3}$$

In particular, since all the conjugates of q have moduli > 1, for some $\Lambda \in \mathbb{N}$ there holds

$$(\mathcal{F} + \mathcal{F}) \cup (-\mathcal{F}) \cup (\mathcal{F} \cdot \mathcal{F}) \subset q^{\Lambda} \mathcal{F}. \tag{2.4}$$

For any integer $\kappa \geq 0$, we define

$$\mathcal{N}_\kappa := \Big\{ \sum_{j=0}^{\kappa-1} b_j q^j, b_j \in \mathcal{D} \Big\}.$$

2.2. **Hypotheses on f and $(q, \mathcal{D})$.** We work with the formalism introduced in [MR15], which assumes two hypotheses of different nature on f.

Definition 2. *We say that f satisfies the* Carry property *if there exists a number $\eta_1 > 0$ such that for any $\kappa, \lambda, \rho \in \mathbb{N}$ with $\rho \leq \lambda$, the number of $v \in \mathcal{N}_\lambda$ such that*

$$f(u_1 + u_2 + vq^\kappa)\overline{f(u_1 + vq^\kappa)} \neq f_{\kappa+\rho}(u_1 + u_2 + vq^\kappa)\overline{f_{\kappa+\rho}(u_1 + vq^\kappa)} \tag{2.5}$$

for some $(u_1, u_2) \in \mathcal{N}_\kappa^2$, is bounded by $O(N(q)^{\lambda - \eta_1 \rho})$.

Definition 3. *We say that f satisfies the* Fourier property *if there exist a non-decreasing function $\gamma : \mathbb{N} \to \mathbb{R}_+$, and $c > 0$, such that uniformly for $\lambda \in \mathbb{N}$, $\kappa \leq c\lambda$ and $t \in K$,*

$$\sum_{v \in \mathcal{N}_\lambda} f(vq^\kappa) \mathrm{e}^{2\pi i \langle tv \rangle} \ll N(q)^{\lambda - \gamma(\lambda)}. \tag{2.6}$$

As is noted in [MR15, eq. (26)], if (2.6) holds then we always have

$$\gamma(\lambda) \leq \lambda/2. \tag{2.7}$$

We define the following two "distortion" parameters on the number system:

$$\Theta := \max_{\pi \in G_K} \frac{d \log |q^\pi|}{\log N(q)} \geq 1, \tag{2.8}$$

$$\theta := \min_{\pi \in G_K} \frac{d \log |q^\pi|}{\log N(q)} > 0. \tag{2.9}$$

Note that the inequality in (2.8) is obvious, and that the inequality in (2.9) follows from the assumption, made in Section 2.1, that the Galois conjugates of q have moduli > 1.

As a consequence of (2.9), the multiplication matrix associated to q^{-1} has spectral radius at most $N(q)^{-\theta} < 1$ (it is asymptotically contractant). We will use repeatedly the Gelfand inequality in the form

$$\|q^\lambda\| \ll \lambda^{d-1} N(q)^{\Theta\lambda}, \qquad \|q^{-\lambda}\| \ll \lambda^{d-1} N(q)^{-\theta\lambda}, \tag{2.10}$$

for $\lambda \in \mathbb{N}_{>0}$, see [Wir98, Lemma 2.3].

2.3. **Main result.** Our main result is the proof of the following statement, which shows that the analogue of [MR15] holds in number fields in the most general formulation.

Theorem 3. *Assume that $\mathcal{O}_K$ is principal, $(q, \mathcal{D})$ is a FNS, and $f : \mathcal{O}_K \to \mathbb{C}$ has the Carry and Fourier properties with the above notations, and $c \geq 20\Theta\theta^{-1}$. There exist $C, \delta, \eta_2 > 0$, with $\delta \asymp \eta_1\eta_2 d^{-1} \min\{\eta_1\eta_2, \theta\}$, such that for all $\lambda \in \mathbb{N}_{>0}$, we have*

$$\sum_{\substack{p \in \mathcal{N}_\lambda \\ p \text{ prime}}} f(p) \ll_{K,q,\mathcal{D}} \lambda^C N(q)^{\lambda - \delta\gamma(\frac{\lambda}{100\Theta\theta^{-1}})}. \tag{2.11}$$

The constant η_2 is a natural parameter associated the addition automaton of the NFS $(q, \mathcal{D})$; in particular it depends only on $(q, \mathcal{D})$. It is formally introduced below in Lemma 8. In Appendix A below, we study the asymptotic behaviour of this constant in infinite families of canonical number systems $q = -m + x$, $m \in \mathbb{N}$, $m \to \infty$.

2.4. **Plan of the paper.** After compiling technical lemmas in Section 3, we state and prove our type I and II estimates in Sections 4 and 5. We then prove Theorem 3 in Section 6, and deduce Theorems 1 and 2 in Section 7. Appendix A is concerned with a subsidiary result on asymptotic behaviour of carry constants.

2.5. **Notations.** In the sequel, we abbreviate

$$Q := N(q),$$

$$\mathrm{e}(z) := \mathrm{e}^{2\pi i z}.$$

It will also be useful to denote, for $\lambda \in \mathbb{N}$ and $t \in K$,

$$\mathrm{e}_\lambda(t) = \mathrm{e}\Big(\Big\langle \frac{t}{q^\lambda} \Big\rangle\Big). \tag{2.12}$$

We recall the definitions (2.3), and we let further

$$R_{\mathcal{F}}^{*} = \sup_{x\in\mathcal{F}} \prod_{\pi\in G_K} (1+|x^{\pi}|). \tag{2.13}$$

3. Lemmas

On many occasions, we will use the following simple bounds on norms of products.

Lemma 1.

(1) For all $x, y \in K$, $\|xy\| \ll \|x\|\|y\|$,
(2) For all $x \in K \smallsetminus \{0\}$, $\|x^{-1}\| \ll N(x)^{-1}\|x\|^{d-1}$.

Proof. The first part is obvious. The second part follows from $N(x) = \prod_{\pi\in G_K} x^{\pi}$. Indeed, writing $x = \sum_{i=1}^{d} x_i\omega_i$ with $x_i \in \mathbb{Q}$, then for any $k \in \{1,\dots,d\}$, we have

$$\begin{aligned}\left\langle \omega_k^{\vee} x^{-1}\right\rangle &= N(x)^{-1}\left\langle \omega_k^{\vee} \sum_{(i_\pi)_{\pi\neq \mathrm{id}}} \prod_{\pi\neq\mathrm{id}} x_{i_\pi}\omega_{i_\pi}\right\rangle \\ &= N(x)^{-1} \sum_{(i_\pi)_{\pi\neq\mathrm{id}}} \Big(\prod_{\pi\neq\mathrm{id}} x_{i_\pi}\Big)\left\langle \omega_k^{\vee}\prod_{\pi\neq\mathrm{id}}\omega_{i_\pi}\right\rangle \\ &\ll N(x)^{-1}\|x\|^{d-1}.\end{aligned}$$

□

We also state now an upper-bound for the number of units in a certain angle.

Lemma 2. *For all $x \in K^*$, we have*

$$\operatorname{card}\left\{\varepsilon\in\mathcal{O}^*, \|\varepsilon/x\|\le 1\right\} \ll (\log(2+N(x)))^{d-1},$$

where the implicit constant may depend on K and $\|\cdot\|$.

Proof. Shifting by a suitable unit, we may assume that $|x^{\pi}| \asymp N(x)^{1/d}$ for all $\pi \in G_K$. The condition $\|\varepsilon/x\| \le 1$ then implies $|\varepsilon^{\pi}| \ll N(x)^{1/d}$. Since $\varepsilon \in \mathcal{O}^*$, we also deduce $|\varepsilon^{\pi}| \gg N(x)^{1-1/d}$. Let $(\varepsilon_1,\dots,\varepsilon_r)$ be a $\mathbb{Z}$-basis of the free part of $\mathcal{O}^*$ [Neu99, Theorem I.7.3] (where $r \le d-1$). We are then reduced to counting the number of tuples $(n_1,\dots,n_r) \in \mathbb{Z}^r$ such that

$$\sum_{j=1}^{r} n_j \log|\varepsilon_j^{\pi}| = O(\log(2+N(x)))$$

for all $\pi \in G_K$. Inverting this condition by using a subset of embeddings of size r as in [MV07, p.55], we find that there are at most $O(\log(2+N(x))^r)$ solutions, whence the claimed bound. □

3.1. Additive characters and van der Corput's inequality.

3.1.1. *Orthogonality.* We recall the following orthogonality relations.

Lemma 3. *For all $q \in \mathcal{O}_K \smallsetminus \{0\}$ and $\xi \in \mathcal{O}^{\vee}$, we have*

$$\frac{1}{Q}\sum_{n\in\mathcal{O}/q} \mathrm{e}(\left\langle q^{-1}n\xi\right\rangle) = \begin{cases} 1 & \text{if } \xi \in q\mathcal{O}^{\vee},\\ 0 & \text{otherwise,}\end{cases}$$

and similarly, for all $n \in \mathcal{O}_K$,

$$\frac{1}{Q}\sum_{\xi\in\mathcal{O}^{\vee}/q} \mathrm{e}(\left\langle q^{-1}\xi n\right\rangle) = \begin{cases} 1 & \text{if } n \in q\mathcal{O}_K,\\ 0 & \text{otherwise.}\end{cases}$$

3.1.2. *Counting additive characters.* In Section 4 below, we will require properties of additive characters in $\mathcal{O}$, which we quote from [Hux68, p. 179]. We recall that given an integral ideal $\mathfrak{m}$ and an additive character $\sigma \pmod{\mathfrak{m}}$, we say that σ is a *proper* additive character modulo $\mathfrak{m}$ if σ is not periodic $\mathfrak{n}$ for any integral ideal $\mathfrak{n} \supsetneq \mathfrak{m}$.

We will mainly work with additive characters of the form $n \mapsto \mathrm{e}(\langle nk/m \rangle)$, for $m \in \mathcal{O}$, $k \in \mathcal{O}^\vee/m$ and $m \neq 0$. In this context, given an additive character σ, let us denote

$$(k, m) \sim \sigma \quad \iff \quad \forall n \in \mathcal{O}, \sigma(n) = \mathrm{e}(\langle nk/m \rangle).$$

Note that for any such k and m, there is a unique pair $(\mathfrak{m}, \sigma)$, where $\mathfrak{m}$ containing m, and a unique proper additive character $\sigma \pmod{\mathfrak{m}}$, such that $(k, m) \sim \sigma$.

Lemma 4. *Let $\mu \in \mathbb{N}$, and $\sigma \pmod{\mathfrak{m}}$ be a proper additive character. Then*

$$\sum_{\substack{m \in \mathcal{N}_\mu \\ k \in \mathcal{O}^\vee/m \\ (k,m) \sim \sigma}} \frac{1}{N(m)} \ll \frac{\mu^d}{N(\mathfrak{m})}.$$

The implicit constant may depend on $(q, \mathcal{D})$.

Proof. For any m on the left-hand side, there can be at most one $k \in \mathcal{O}^\vee/m$ for which $(k, m) \sim \sigma$. Moreover, since σ is proper, this can only happen if $\mathfrak{m} \mid m$. Therefore, the quantity on the left-hand side is at most $\sum_{m \in \mathcal{N}_\mu \cap \mathfrak{m}} \frac{1}{N(m)}$. We sort this sum according the principal ideal $\mathfrak{a} = (m)$. First note that $N(m) \leq R_{\mathcal{F}}^* Q^\mu$ (we recall the definition (2.13)). Then

$$\sum_{m \in \mathcal{N}_\mu \cap \mathfrak{m}} \frac{1}{N(m)} \leq \sum_{\substack{\mathfrak{a} \text{ principal} \\ \mathfrak{m} \mid \mathfrak{a} \\ N(\mathfrak{a}) \leq R_{\mathcal{F}}^* Q^\mu}} \frac{1}{N(\mathfrak{a})} \sum_{\substack{m \in \mathcal{N}_\mu \\ (m) = \mathfrak{a}}} 1.$$

For all $\mathfrak{a}$ in the first sum, we pick a generator $u \in \mathcal{O}$ such that $|u^\pi| \asymp N(\mathfrak{a})^{1/d}$ for all field imbedding $\pi \in G_K$. Then the second sum is

$$\sum_{\substack{m \in \mathcal{N}_\mu \\ (m) = \mathfrak{a}}} 1 = \sum_{\substack{\varepsilon \in \mathcal{O}^* \\ \varepsilon u \in \mathcal{N}_\mu}} 1 \ll \mu^{d-1}$$

by Lemma 2, and so

$$\sum_{\substack{\mathfrak{a} \text{ principal} \\ \mathfrak{m} \mid \mathfrak{a} \\ N(\mathfrak{a}) \leq R_{\mathcal{F}}^* Q^\mu}} \frac{1}{N(\mathfrak{a})} \sum_{\substack{m \in \mathcal{N}_\mu \\ (m) = \mathfrak{a}}} 1 \ll \mu^{d-1} \sum_{\substack{\mathfrak{a} \text{ ideal} \\ \mathfrak{m} \mid \mathfrak{a} \\ N(\mathfrak{a}) \leq R_{\mathcal{F}}^* Q^\mu}} \frac{1}{N(\mathfrak{a})} \ll \frac{\mu^d}{N(\mathfrak{m})}$$

as claimed. □

3.1.3. *Van der Corput's inequality.* For all $\rho \in \mathbb{N}$, we define the set

$$\Delta_\rho = \mathcal{N}_\rho - \mathcal{N}_\rho = \{m - n, (m, n) \in \mathcal{N}_\rho^2\}. \tag{3.1}$$

Lemma 5. *Let $\rho, \kappa, \nu \in \mathbb{N}$ with $\rho + \kappa \leq \nu$, and $(z_n)_{n \in \mathcal{O}}$ be complex numbers satisfying $z_n = 0$ when $n \notin \mathcal{N}_\nu$. There exists an even function $w_\rho : \mathcal{O} \to \mathbb{N}$, such that $|w_\rho(r)| \ll Q^\rho$ uniformly in $r \in \mathcal{O}$, and*

$$\Big| \sum_n z_n \Big|^2 \ll Q^{\nu - 2\rho} \sum_{r \in \Delta_\rho} w_\rho(r) \sum_n z_{n + q^\kappa r} \overline{z_n}.$$

Proof. By following the proof of [MR09, Lemma 17], we find

$$\Big|\sum_n z_n\Big|^2 \le \operatorname{card}\Big(\bigcup_{r\in\mathcal{N}_\rho}(\mathcal{N}_\nu - q^\kappa r)\Big)Q^{-2\rho}\sum_{r\in\Delta_\rho} w_\rho(r)\sum_n z_{n+q^\kappa r}\overline{z_n},$$

where $w_\rho(r) = \operatorname{card}\{(r_1,r_2)\in\mathcal{N}_\rho^2, r = r_1 - r_2\}$. The claimed bound follows by our hypothesis $\nu \ge \kappa+\rho$, which implies that the sets $q^{-\nu}(\mathcal{N}_\nu - q^\kappa r)$ are uniformly bounded for $r\in\mathcal{N}_\rho$. □

3.1.4. *Majorants of the fundamental tile.* Since most of our sums over lattices will be estimated by Poisson summation, it will be convenient to work with smooth majorant functions having a compactly supported Fourier transform.

Lemma 6. *For any bounded set $B\subset\mathbb{R}^d$, there exists a function $V:\mathbb{R}^d\to\mathbb{R}_+$ in the Schwartz class, depending on B, satisfying the following:*

(1) for all $x\in\mathbb{R}^d$, if $x\in B$, then $V(x)\ge 1$,
(2) the Fourier transform $\widehat{V}(\xi) = \int_{\mathbb{R}_d} V(x)\mathrm{e}(\langle\xi,x\rangle)\mathrm{d}x$ vanishes unless $\|\xi\|_\infty\le 1$.

Proof. We take $V(x) = \alpha\prod_{j=1}^d \widehat{f}(\beta x_j)$, where f is given as in Theorem A.3 of [Swa19] for some small enough $\beta>0$ and large enough α depending on B. □

3.1.5. *The large sieve inequality.* The following is a multidimensional version of the large sieve inequality, and corresponds to Theorem 2 of [Hux68]. The main difference lies in the scaling of the set of points: when dealing with ideals (rather than arbitrary lattices), we can avoid the "skewing" phenomenon refered to above. We refer to [Mon78] for history and additional references on the large sieve.

Lemma 7. *Let $\alpha\in K^*$, $X\in[1,\infty)$ and $(c(n))_{n\in\mathcal{O}}$ be complex numbers. Then*

$$\sum_{\substack{\mathfrak{m}\ ideal\\ 0<N(\mathfrak{m})\le X}}\sum_{\substack{\sigma\ (\mathrm{mod}\ \mathfrak{m})\\ proper}}\Big|\sum_{\substack{n\in\mathcal{O}\\ \|n/\alpha\|\le 1}} c(n)\sigma(n)\Big|^2 \ll_K (N(\alpha)+X^2)\sum_{\substack{n\in\mathcal{O}\\ \|n/\alpha\|\le 1}}|c(n)|^2,$$

where in the sum on the left-hand side, σ runs over proper additive characters (mod $\mathfrak{m}$).

Proof. Let $\varepsilon\in\mathcal{O}^*$ be such that $|(\varepsilon\alpha)^\pi|\asymp N(\alpha)^{1/d}$, and denote $\alpha' = \varepsilon\alpha$. For any $\mathfrak{m}$, the map $\sigma\mapsto(a\mapsto\sigma(\varepsilon^{-1}a))$ is a permutation of the proper additive characters (mod $\mathfrak{m}$). Therefore, we have

$$\sum_{\substack{\mathfrak{m}\ \text{ideal}\\ 0<N(\mathfrak{m})\le X}}\sum_{\substack{\sigma\ (\mathrm{mod}\ \mathfrak{m})\\ \text{proper}}}\Big|\sum_{\substack{n\in\mathcal{O}\\ \|n/\alpha\|\le 1}} c(n)\sigma(n)\Big|^2 = \sum_{\substack{\mathfrak{m}\ \text{ideal}\\ 0<N(\mathfrak{m})\le X}}\sum_{\substack{\sigma\ (\mathrm{mod}\ \mathfrak{m})\\ \text{proper}}}\Big|\sum_{\substack{n\in\mathcal{O}\\ \|n/\alpha'\|\le 1}} c'(n)\sigma(n)\Big|^2$$

with $c'(n) = c(\varepsilon^{-1}n)$. The condition $\|n/\alpha'\|\le 1$ implies $\|n\|\ll\|\alpha'\|\ll N(\alpha)^{1/d}$, and so Theorem 2 of [Hux68] can be applied with $N_j\ll N(\alpha)^{1/d}$, which yields the claimed result. □

3.2. **Numeration.**

3.2.1. *Carry propagation.* Let $r_{\nu,\mu}(n)$ be the integer formed with the digits of n of indices $\{\nu,\dots,\mu-1\}$, so that if $n=\sum_{j\ge 0} n_j q^j$, then $r_{\nu,\mu}(n) = \sum_{0\le j<\mu-\nu} n_{\nu+j}q^j$. We write $r_{\nu,\infty}(n) = \lim_{\mu\to\infty} r_{\nu,\mu}(n)$. We wish to quantify the fact that propagation of a carry is an exponentially rare event. This has been studied in particular in [GL99, MTT01]. In fact the following lemma can be seen as an arithmetic restatement of a weaker version of [MTT01, Proposition 4.1].

Lemma 8. *There exists $\eta_2 = \eta_2(q, \mathcal{D}) \in (0, 1]$, such that for all integers $0 \leq \rho \leq \nu \leq \mu$, we have*

$$\operatorname{card}\{m \in \mathcal{N}_\mu, \exists n \in \mathcal{N}_{\nu-\rho}, r_{\nu,\infty}(m+n) \neq r_{\nu,\infty}(m)\} \ll Q^{\mu-\eta_2\rho}. \tag{3.2}$$

However, in [MTT01] and with their notations, the authors work under the assumption that a certain graph $\widetilde{G}(S)$ is primitive. Since we are only interested in the upper-bound (3.2), we do not need this assumption here. What is required is that, from any vertex, there is a path leading to an absorbing state; the possibility of the matrix of the graph $\widetilde{G}(S)$ having multiple dominant eigenvalues does not affect us. In [ST02], the primitivity of $\widetilde{G}(S)$ is proved, however in the more specific case of canonical number systems. For these reasons we include a self-contained proof of Lemma 8.

Proof. We have assumed that $0 \in \mathcal{D}$, and that every element in $\mathcal{O}$ has a base q expansion. Let $\mathcal{B} = \mathcal{D} - \mathcal{D}$, and define a sequence of sets by

$$\mathcal{B}_0 = \{0\}, \qquad \mathcal{B}_{j+1} = \mathcal{B} + q\mathcal{B}_j$$

for all $j \geq 0$. Note that $\mathcal{B}_j = \mathcal{B} + q\mathcal{B} + \cdots q^{j-1}\mathcal{B}$ for $j \geq 1$, so that this sequence is increasing. Since $\mathcal{D} \subset \mathcal{B}$, we have $\mathcal{N}_j \subset \mathcal{B}_j$. Moreover, for all $j > 0$ and all $n \in \mathcal{B}_j$, there exist $a \in \mathcal{D}$ and $m \in \mathcal{B}_{j-1}$ such that $n + a \in qm + \mathcal{D}$.

Next we let $\{0\} \subset \mathcal{B}_{st} \subset \mathcal{O}$ be the smallest set such that $\mathcal{B}_{st} + \mathcal{D} + \mathcal{D} \subset \mathcal{D} + q\mathcal{B}_{st}$; the existence of $\mathcal{B}_{st}$ is ensured by boundedness of $\{\sum_{j=1}^{r}(n_{j,1}+n_{j,2}-n_{j,3})q^{-j}, r \geq 1, n_{j,k} \in \mathcal{D}\}$. The set $\mathcal{B}_{st}$ is our initial set of carries. We define a Markov chain on the set of states $\mathcal{B}_{st}$ by setting, for every $n \in \mathcal{B}_{st}$ and digit $a \in \mathcal{D}$, an edge

$$n \xrightarrow{a} m \qquad \Longleftrightarrow \qquad n + a \in qm + \mathcal{D},$$

each digit $a \in \mathcal{D}$ being chosen with equal probability. Note that by construction, we do have $m \in \mathcal{B}_{st}$. The main point is that 0 is an absorbing state for this chain. Therefore, a random walk on $\mathcal{B}_{st}$ of length $\rho \in \mathbb{N}$, starting at any given vertex, has probability $O(c^\rho)$ of not ending at 0, for some $c \in (0, 1)$.

Let $m = \sum_{j=0}^{\mu-1} m_j q^j$, with $m_j \in \mathcal{D}$. Suppose that there is an $n \in \mathcal{N}_{\nu-\rho}$ such that $(m+n)_{[\nu,\infty]} \neq (m)_{[\nu,\infty]}$. Consider the sequences of carries $(b_j)_{j\geq -1}$ in the addition $m + n$. More precisely, if we let $n = \sum_{j\geq 0} n_j q^j$ with $n_j = 0$ if $j \geq \nu - \rho$, then $b_{-1} = 0$ and for all $j \geq 0$, b_j is the unique element of $\mathcal{O}$ such that $b_{j-1} + m_j + n_j \in \mathcal{D} + qb_j$. By construction, we have $b_j \in \mathcal{B}_{st}$ for all $j \geq -1$. For all $j \geq \nu$, the recurrence relation reads, with our above notations,

$$b_{j-1} \xrightarrow{m_j} b_j.$$

Our hypothesis on m and n implies that $b_\nu \neq 0$. Therefore, the tuple $(m_j)_{\nu-\rho<j\leq\nu}$ describes a walk on $\mathcal{B}_{st}$ of length at least ρ, not ending at 0. The number of such tuples is at most $O(c^\rho)$, and so the number of possibilities for m is at most $O(Q^{\mu-\eta_2\rho})$ with $\eta_2 = -(\log c)/\log Q > 0$ □

Remark. We will call any admissible constant η_2 in Lemma 8 a *carry constant*. When $K = \mathbb{Q}(i)$, we may choose

$$\eta_2 = \begin{cases} 0.238186\ldots, & (q, \mathcal{D}) = (-1+i, \{0, 1\}), \\ 0.195636\ldots, & (q, \mathcal{D}) = (-2+i, \{0, 1, 2, 3, 4\}), \\ 0.053205\ldots, & (q, \mathcal{D}) = (-2+i, \{0, -2i, 2, 3, 4\}). \end{cases}$$

These values were obtained by approximating the spectral radius of the adjacency matrix associated with the graph on $\mathcal{B}_{st}$ considered above (with the absorbing state removed).

3.2.2. *Harmonic analysis of the fundamental tile.* In this section we study some harmonic analytic properties of the indicator function of the fundamental tile defined in (2.2). For this purpose we will study the closure of this tile in $\mathbb{R}^d$,

$$\mathscr{F} = \overline{\iota^{-1}(\mathcal{F})} \subset \mathbb{R}^d$$

In our context the set $\mathscr{F}$ plays the rôle of the unit interval $[0,1]$ in [MR15]. For example, when $d=1$, $q<-1$ and $\mathcal{D}=\{0,\dots,|q|-1\}$, we have explicitly

$$\mathscr{F} = \Big[\frac{q}{q^2-1}, \frac{1}{q^2-1}\Big].$$

In general however, the set $\mathscr{F}$ is of a more complicated nature, and is a main object of study in the theory of self-similar tilings of $\mathbb{R}^n$ (see [LW96]).

Here, we have assumed that $(q,\mathcal{D})$ is a FNS; we refer to Proposition 2.1 of [MTT01] for general properties of $\mathscr{F}$. In particular, $\mathscr{F}$ is compact, measurable with Lebesgue measure $\mathrm{meas}(\mathscr{F})=1$; by Theorem 1 of [Vin95], $\mathscr{F}$ contains an open neighborhood of the origin; and finally

$$\mathrm{meas}(\mathscr{F} \cap (\mathscr{F}+a)) = 0 \qquad (a \in \mathbb{Z}^d \smallsetminus \{0\}).$$

Remark.

— When $d=1$, the set $\mathscr{F}$ needs not be an interval, as the example $q=-3$, $\mathcal{D}=\{0,2,7\}$ shows. The pair $(q,\mathcal{D})$ is a FNS (see [GH94, Th. 2.3]) but the boundary $\partial\mathscr{F}$ has Hausdorff dimension $0.8798\cdots = \log\lambda/\log 3$, where λ is the real root of X^3-X^2-2X-6.

— When $d\geq 2$, the set $\mathscr{F}$ needs not be connected, as the case

$$K=\mathbb{Q}(i), \quad q=3, \quad \mathcal{D}=\{0,i,2i,1,1+i,1+2i,2,2+i,5+5i\}$$

shows (see [LW96, Figure 2.1]). In this case, an admissible carry constant is $\eta_2 = 1-\log\lambda/\log 9 = 0.237701\ldots$, where λ is the largest real root of $X^4-4X^3-8X^2+4X+3$.

The set $\mathscr{F}$ has been studied in a variety of cases:

(1) For CNS and $d=2$, in [Gil86] for $K=\mathbb{Q}(i)$, and in [Thu98a, Thu01] for all quadratic fields.
(2) For CNS and arbitrary d, under a generic condition on the minimal polynomial of q, the upper-box dimension of $\partial\mathscr{F}$ is obtained in [ST02].
(3) For general FNS, Keesling [Kee99] has shown that the Hausdorff dimension $\dim_H(\partial\mathscr{F})$ is always strictly less than d, and that it can be arbitrarily close to d. Note that $\dim_H(\partial\mathscr{F})\geq d-1$, and that equality is achieved in the case $q=-2$, $\mathcal{D}=\{\sum_{i\in I}\omega_i, I\subset\{1,\dots,d\}\}$, for which $\mathscr{F}=[0,1]^d$. Upper and lower bounds on $\dim_H(\partial\mathscr{F})$ in terms of the carry constant η_2 are obtained in [MTT01]; the bounds coincide when $\Theta=\theta=1$.

In the present work, we will require some information of the decay of the Fourier transform of the characteristic function of $\mathscr{F}$. This is ultimately due to the fact that the information we will use of the function f concerns its correlation with additive characters (2.6) and its behaviour with respect to the digital expansion (2.5).

For $x,\xi\in\mathbb{R}^d$, let

$$\chi(x)=\mathbf{1}_{x\in\mathscr{F}}, \qquad \widehat{\chi}(\xi)=\int_{\mathscr{F}} \mathrm{e}(-\langle x,\xi\rangle)\mathrm{d}x.$$

For $\lambda \in \mathbb{N}_{>0}$, define

$$\psi_\lambda(x) := \sum_{k\in\mathbb{Z}^d} \chi(q^\lambda(x+k)),$$

where q is viewed as a linear map of $\mathbb{R}^d$ by $qx = \iota^{-1}(q\iota(x))$ for all $x \in \mathbb{R}^d$. The function ψ_λ is $\mathbb{Z}^d$-periodic, and its Fourier coefficients are

$$\widehat{\psi}_\lambda(\xi) = Q^{-\lambda}\widehat{\chi}(\widetilde{q}^{-\lambda}\xi) \qquad (\xi \in \mathbb{Z}^d),$$

where $\widetilde{q}$ is the adjoint of q.

The less regular $\partial\mathscr{F}$ is, the more slowly the function $\widehat{\chi}$ decays: for instance, in the case $K = \mathbb{Q}(i)$, $q = -1+i$, $\mathcal{D} = \{0,1\}$, it is shown by Cohen and Daubechies [CD93, eq. (5.3)] that $\widehat{\chi}(\xi) \ll \|\xi\|^{-1/2}$ for all $\xi \in \mathbb{R}^d$, the exponent $1/2$ being in fact optimal. This and related questions are known in wavelet theory as the regularity problem of self-refinable functions; see in particular [CD96, PW08]. Here we are largely able to avoid this question altogether. We essentially require two informations: a truncated Fourier expansion of ψ_λ, and an estimate for L^2 norms.

In the context of distribution of q-additive functions, this difficulty has been encountered in [GT00] in the case $K = \mathbb{Q}(i)$, and [Mad10] for general K (see [Ste02] for related earlier computations in the context of Parry expansions). To truncate the Fourier series of ψ_λ, one wishes to smooth out the function $\widehat{\chi}$. In the above-mentioned works, this is done by convolving with the characteristic function of a hypercube (Urysohn approximation), however, it is technically convenient to use smooth, compactly supported majorants, so that sums over lattices can be estimated more easily by Poisson summation.

Lemma 9. *Let $\lambda, \tau \in \mathbb{N}_{>0}$. There exist complex numbers $(a_{\lambda,\tau}(\xi))_{\xi\in\mathbb{Z}^d}$ and $(b_{\lambda,\tau}(\xi))_{\xi\in\mathbb{Z}^d}$ satisfying the following.*

(i) For all fixed $A \geq 0$, we have

$$|a_{\lambda,\tau}(\xi)| \ll_A Q^{-\lambda}(1+\|\widetilde{q}^{-\lambda-\tau}\xi\|)^{-A}, \qquad |b_{\lambda,\tau}(\xi)| \ll_A Q^{-\lambda-\eta_2\tau}(1+\|\widetilde{q}^{-\lambda-\tau}\xi\|)^{-A}. \tag{3.3}$$

(ii) The functions $A_{\lambda,\tau}(x)$ and $B_{\lambda,\tau}(x)$ defined by

$$A_{\lambda,\tau}(x) = \sum_{\xi\in\mathbb{Z}^d} a_{\lambda,\tau}(\xi)\mathrm{e}(\langle\xi,x\rangle), \qquad B_{\lambda,\tau}(x) = \sum_{\xi\in\mathbb{Z}^d} b_{\lambda,\tau}(\xi)\mathrm{e}(\langle\xi,x\rangle)$$

satisfy

$$|\psi_\lambda(x) - A_{\lambda,\tau}(x)| \leq B_{\lambda,\tau}(x).$$

(iii) For all $\kappa \in \{0,\dots,\lambda\}$ and $\xi_0 \in \mathbb{Z}^d$, we have

$$\sum_{\xi\in\mathbb{Z}^d} |a_{\lambda,\tau}(\xi_0+\widetilde{q}^\kappa\xi)|^2 \ll Q^{-\lambda-\kappa}, \tag{3.4}$$

$$\sum_{\xi\in\mathbb{Z}^d} |b_{\lambda,\tau}(\xi_0+\widetilde{q}^\kappa\xi)|^2 \ll Q^{-\lambda-\kappa-\eta_2\tau}. \tag{3.5}$$

Proof. Let $\phi : \mathbb{R}^d \to [0,1]$ be a smooth function satisfying

$$\mathbf{1}_{\|x\|\leq 1/2} \leq \phi(x) \leq \mathbf{1}_{\|x\|\leq 2}, \qquad \int_{\mathbb{R}^d} \phi(x)\mathrm{d}x = 1,$$

where $\|x\|$ is the euclidean norm. Define $\phi_\tau := Q^\tau\phi(q^\tau x)$. Define

$$\chi_\tau := \chi * \phi_\tau, \tag{3.6}$$

and let $V_1 = \partial\mathscr{F} + q^{-\tau}B(0,2)$ and $V_2 = \partial\mathscr{F} + q^{-\tau}B(0,2) + q^{-\tau}B(0,2)$. Note that $V_1 \subset V_2$, and

$$\{x \in \mathbb{R}^d : \ \chi(x) \neq \chi_\tau(x)\} \subset V_1.$$

We focus first on V_2. Let $\rho \in \mathbb{N}$ be such that $B(0,2) \subset q^\rho \mathscr{F}$. Each number $x \in q^\tau V_2$ can be decomposed uniquely as $x = m + y$ where $m \in \mathbb{Z}^d$ and $y \in \mathscr{F}$. Note that $m \in q^{\max(\rho,\tau)+2\Lambda}\mathscr{F}$, so that certainly $\iota(m) \in \mathcal{N}_{\tau+\rho+2\Lambda}$. The condition $m+y \in \partial(q^\tau\mathscr{F})$ implies the existence of $z_+, z_- \in q^{\rho+2\Lambda}\mathscr{F}$ such that $m + y - z_+ \in \mathbb{Z}^d \cap q^\tau\mathscr{F}$ and $m + y - z_- \in \mathbb{Z}^d \smallsetminus q^\tau\mathscr{F}$. Therefore, there exist $n_+, n_- \in \mathbb{Z}^d \cap q^{\rho+4\Lambda}\mathscr{F}$ such that $m + n_+ \in q^\tau\mathscr{F}$ and $m + n_- \notin q^\tau\mathscr{F}$. By Lemma 8 the number of such m is at most $\ll Q^{(1-\eta_2)\tau}$, and therefore

$$\mathrm{meas}(V_2) = Q^{-\tau} \sum_{m\in\mathbb{Z}^d} \int_{\mathscr{F}} \mathbf{1}(m + y \in q^\tau V_2)\mathrm{d}y \ll Q^{-\eta_2\tau}. \tag{3.7}$$

We now write

$$|\chi(x) - \chi_\tau(x)| \leq \mathbf{1}_{V_1}(x) \leq (\mathbf{1}_{V_2} * \phi_\tau)(x).$$

Define now the smooth, $\mathbb{Z}^d$-periodic functions

$$A_{\lambda,\tau}(x) = \sum_{k\in\mathbb{Z}^d} \chi_\tau(q^\lambda(x+k)), \qquad B_{\lambda,\tau}(x) = \sum_{k\in\mathbb{Z}^d} (\mathbf{1}_{V_2} * \phi_\tau)(q^\lambda(x+k)).$$

We have $B_{\lambda,\tau}(x) \ll 1$. Let $a_{\lambda,\tau}(\xi)$ and $b_{\lambda,\tau}(\xi)$ be the coefficients in the Fourier expansions of $A_{\lambda,\tau}(x)$ and $B_{\lambda,\tau}(x)$, respectively. We have

$$a_{\lambda,\tau}(\xi) = Q^{-\lambda}\widehat{\chi}(\widetilde{q}^{-\lambda}\xi)\widehat{\phi}(\widetilde{q}^{-\lambda-\tau}\xi),$$

$$b_{\lambda,\tau}(\xi) = Q^{-\lambda}\widehat{\phi}(\widetilde{q}^{-\lambda-\tau}\xi)\int_{V_2} \mathrm{e}(\langle \widetilde{q}^{-\lambda}\xi, y\rangle)\mathrm{d}y.$$

By partial summation, we have the bound

$$\left|\widehat{\phi}(\xi)\right| \ll_A (1 + \|\xi\|)^{-A} \tag{3.8}$$

for any $A > 0$. By (3.7), we deduce parts (i) and (ii) as claimed.

For part (iii), let us consider the case of $b_{\lambda,\tau}$. By absolute convergence and orthogonality (Lemma 3), we have

$$\sum_{\xi\in\mathbb{Z}^d} |b_{\lambda,\tau}(\xi_0 + \widetilde{q}^\kappa\xi)|^2 = Q^{-\kappa} \sum_{\ell\in\mathbb{Z}^d/B^\kappa\mathbb{Z}^d} \mathrm{e}(-\langle \widetilde{q}^{-\kappa}\xi_0, \ell\rangle) \sum_{\xi\in\mathbb{Z}^d} |b_{\lambda,\tau}(\xi)|^2 \,\mathrm{e}(\langle \widetilde{q}^{-\kappa}\xi, \ell\rangle). \tag{3.9}$$

On the other hand, by Poisson summation, we have

$$\sum_{\xi\in\mathbb{Z}^d} |b_{\lambda,\tau}(\xi)|^2 \,\mathrm{e}(\langle \widetilde{q}^{-\lambda}\xi, \ell\rangle) = \int_{\mathbb{R}^d/\mathbb{Z}^d} B_{\lambda,\tau}(x + q^{-\lambda}\ell)B_{\lambda,\tau}(x)\mathrm{d}x.$$

Let $V_3 = V_2 + q^{-\tau}B(0,2)$; it is a bounded set. By construction, the support of $B_{\lambda,\tau}$ is included in $\mathbb{Z}^d + q^{-\lambda}V_3$. Therefore, for any given $x \in \mathbb{R}^d$, the integrand above vanishes unless there exists $k \in \mathbb{Z}^d$ such that

$$q^\kappa k + \ell \in q^{\kappa-\lambda}V_3,$$

and the latter is a bounded set since $\kappa \leq \lambda$, therefore, there are at most a bounded number of ℓ contributing to the sum on the right-hand side of (3.9). We deduce

$$\sum_{\xi\in\mathbb{Z}^d} |b_{\lambda,\tau}(\xi_0 + \widetilde{q}^\kappa\xi)|^2 \ll Q^{-\kappa-\lambda-\eta_2\tau}$$

by (3.7), and we obtain (3.5). The bound (3.4) is proved using identical argument in a simpler way; therefore we do reproduce the details. □

Remark. It is an important point in the proof that the smooth majorant ϕ is scaled down by powers of q, rather than *e.g.* homotheties (in which case the carry constant η_2 would be replaced by the upper-box dimension of $\partial\mathscr{F}$, which is less understood in general [MTT01, ST02]).

There would be much technical simplification to be gained, in our later arguments, by having an analogue of Vaaler's construction of band-limited majorants [Vaa85], as was used in [MR15]; our attempts were unsuccessful.

In the sequel, for $x \in K$ and $\xi \in \mathcal{O}^\vee$, we will denote

$$\psi_\lambda(x) = \psi_\lambda(\iota^\vee(x)), \qquad a_{\lambda,\tau}(\xi) = a_{\lambda,\tau}(\iota^\vee(\xi)) \tag{3.10}$$

and similarly for $b_{\lambda,\tau}$.

3.3. **Fourier estimates.** In this section, we prove an analogue of Lemma 10 of [MR15], concerning restricted L^2 estimates for the discrete Fourier transform of f.

3.3.1. *Fourier property over the middle digits.* The next lemma concerns a variant of the Fourier property (2.6), in which the sum is effectuated only over the middle digits. This additional flexibility comes at the price of a numerically smaller gain in the exponent.

Lemma 10. *Let $\alpha, \beta, \delta \in \mathbb{N}$ satisfy $\delta \leq \alpha+\beta$, and let $\lambda := \alpha+\beta+\delta$. For all f satifying the Fourier property, we have*

$$\frac{1}{Q^\beta} \sum_{u_1 \in \mathcal{N}_\beta} f_{\kappa+\lambda}(q^\kappa(u_0 + q^\alpha u_1 + q^{\alpha+\beta}u_2))\mathrm{e}(\langle u_1 t\rangle) \ll Q^{-\eta'\gamma(\lambda)+\alpha+\delta}$$

uniformly for $u_0 \in \mathcal{N}_\alpha$, $u_2 \in \mathcal{N}_\delta$, $t \in K$ and $\kappa \leq c\lambda$, where $\eta' = \eta_2(1+\eta_2)^{-1}$.

Proof. We recall the notation (2.12). By orthogonality, our sum is

$$\begin{aligned}&\frac{1}{Q^\beta} \sum_{u \in \mathcal{N}_\lambda} f(q^\kappa u)\mathrm{e}_\alpha(ut)\mathbf{1}_{u-u_0 \in q^\alpha\mathcal{O}}\mathbf{1}_{\frac{u}{q^{\alpha+\beta}} \in u_2+\mathcal{F}+q^\delta\mathcal{O}}\mathrm{e}_\kappa(-u_0 t)\mathrm{e}_{-\beta}(-u_2 t)\\ &= \mathrm{e}_\kappa(-u_0 t)\mathrm{e}_{-\beta}(-u_2 t) \sum_{\ell \in \mathcal{O}/q^\alpha} \mathrm{e}_\alpha(-u_0\ell) S\Big(\ell, \frac{t+\ell}{q^\alpha}\Big),\end{aligned}$$

where

$$S(\ell, t) = \frac{1}{Q^{\alpha+\beta}} \sum_{u \in \mathcal{N}_\lambda} f(q^\kappa u)\mathrm{e}(\langle ut\rangle)\psi_\delta\Big(\frac{u}{q^\lambda} - \frac{u_2}{q^\delta}\Big).$$

Let $\tau \in \mathbb{N}$, $\tau \leq \alpha+\beta$, be a parameter. At this point, we wish to apply Lemma 9, to replace ψ_δ by its smoothed version $A_{\sigma,\tau}$. The ensuing main term is

$$S_\tau(\ell, t) = \frac{1}{Q^{\alpha+\beta}} \sum_{u \in \mathcal{N}_\lambda} f(q^\kappa u)\mathrm{e}(\langle ut\rangle)A_{\delta,\tau}\Big(\frac{u}{q^\lambda} - \frac{u_2}{q^\delta}\Big),$$

where we recall the notation (3.10). We Fourier expand and use the Fourier property, getting

$$\begin{aligned}S_\tau(\ell, t) &= \sum_{\xi \in \mathcal{O}^\vee} a_{\delta,\tau}(\xi)\mathrm{e}_\delta(-\xi u_2)\frac{1}{Q^{\alpha+\beta}} \sum_{u \in \mathcal{N}_\lambda} f(q^\kappa u)\mathrm{e}_\lambda(u(\xi + tq^\lambda))\\ &\ll Q^{\delta-\gamma(\lambda)} \sum_{\xi \in \mathcal{O}^\vee} |a_{\delta,\tau}(\xi)|\\ &\ll Q^{-\gamma(\lambda)+\tau+\delta}.\end{aligned}$$

We justify the Fourier truncation (replacement of ψ_σ by $A_{\sigma,\tau}$) in a similar way to (3.7). Assuming δ is large enough in terms of q, by Lemma 9, we know that

$$\psi_\delta\Big(\frac{u}{q^\lambda}-\frac{u_2}{q^\delta}\Big)-A_{\delta,\tau}\Big(\frac{u}{q^\lambda}-\frac{u_2}{q^\delta}\Big)\ll \mathbf{1}\Big(\frac{u}{q^{\lambda-\delta}}-u_2\in\partial\mathcal{F}+B(0,2/H)+q^\delta\mathcal{O}\Big). \tag{3.11}$$

Let $\tau\in\mathbb{N}$ be the largest such that $B(0,2/H)\subset q^{-\tau}\mathcal{F}$; note that $\tau\geq O(1)+\frac{\log H}{2\Theta\log Q}$. By a reasoning similar to (3.7), we may find an element $n'\in\mathcal{N}_{\alpha+\beta-\tau+4\Lambda}$ such that $r_{\alpha+\beta,\infty}(u-q^{\alpha+\beta}u_2-q^\lambda k+n')\neq r_{\alpha+\beta,\infty}(u-q^{\alpha+\beta}u_2-q^\lambda k)$. Denoting $u'=u-q^{\alpha+\beta}u_2-q^\lambda k$, we deduce

$$\begin{aligned}|S(\ell,t)-S_\tau(\ell,t)|&\ll\frac{1}{Q^{\alpha+\beta}}\sum_{u\in\mathcal{N}_\lambda}\mathbf{1}\Big(\frac{u}{q^{\lambda-\delta}}-u_2\in\partial\mathcal{F}+B(0,2/H)+q^\delta\mathcal{O}\Big)\\&\ll\frac{1}{Q^{\alpha+\beta}}\sum_{k\in\mathcal{N}_{6\Lambda}}\operatorname{card}\{u'\in\mathcal{N}_{\lambda+3\Lambda},\exists n\in\mathcal{N}_{\alpha+\beta-\tau+4\Lambda},\\&\qquad\qquad r_{\alpha+\beta,\infty}(u')\neq r_{\alpha+\beta,\infty}(u'+n)\}\\&\ll Q^{\delta-\eta_2\tau}\end{aligned}$$

by Lemma 8. Using (2.7), we may optimize τ under the condition $\tau\leq\alpha+\beta$ and find

$$S(\ell,t)\ll Q^{-\eta'\gamma(\lambda)+\delta}$$

with $\eta'=\eta_2(1+\eta_2)^{-1}$, as claimed. □

3.3.2. *Incomplete L^2 bound on the Fourier transform.* The statements of this section depend of certain parameters which will be introduced later in Section 5. For now, we let μ,μ_0,μ_1 and μ_2 be natural numbers subject to

$$\mu_0<\mu_1<\mu<\mu_2.$$

We let $\sigma=\mu_2-\mu_0$, and define, for all $n\in\mathcal{O}$,

$$g(n)=f_{\mu_2}(q^{\mu_0}n)\overline{f_{\mu_1}}(q^{\mu_0}n). \tag{3.12}$$

We recall the definition of the discrete Fourier transform of g,

$$\widehat{g}(h):=\frac{1}{Q^\sigma}\sum_{u\in\mathcal{O}/q^\sigma}g(u)\mathrm{e}_\sigma(-uh). \tag{3.13}$$

Proposition 1. *With the above notation and hypotheses, for all $t\in K$ and $\lambda\in\mathbb{N}$, if $c^{-1}\mu_0\leq\lambda\leq\sigma$, then we have*

$$\sum_{\substack{h\in\mathcal{O}^\vee\\\|h/q^{\sigma-\lambda}\|\leq1}}|\widehat{g}(h+t)|^2\ll Q^{2(\mu_1-\mu_0)}(Q^{-\eta''\gamma(\lambda)}+Q^{-\eta_1(\sigma-\lambda)})$$

where $\eta''=2\eta_1\eta_2(2+\eta_1)^{-1}(1+\eta_2)^{-1}$.

Proof. The proof mirrors that of [MR15]: the point is that we may use the carry property to essentially factor $\widehat{g}(h+t)$ as a sum over $\mathcal{N}_\lambda$ times a sum over $\mathcal{N}_{\sigma-\lambda}$. Parseval's identity will be applied to the second factor, to recover the full h-sum, while the Fourier property on the first factor will allow for an extra saving. For each $h\in\mathcal{N}_{\sigma-\lambda}$, we write

$$\widehat{g}(t)=\frac{1}{Q^\sigma}\sum_{u\in\mathcal{N}_\lambda}\sum_{v\in\mathcal{N}_{\sigma-\lambda}}g(u+q^\lambda v)\mathrm{e}_\sigma(-ut)\mathrm{e}_{\sigma-\lambda}(-vt).$$

Here, we have by periodicity

$$g(u+q^\lambda v)=f(q^{\mu_0}(u+q^\lambda v))\overline{f_{\mu_1}(q^{\mu_0}u)}.$$

Let $\rho_3 \leq \sigma - \lambda$. By the carry property (2.5), we have

$$f(q^{\mu_0}(u+q^\lambda v)) = f_{\mu_0+\lambda+\rho_3}(q^{\mu_0}(u+q^\lambda v))f(q^{\mu_0+\lambda}v)\overline{f_{\mu_0+\lambda+\rho_3}(q^{\mu_0+\lambda}v)}$$

except when $u+q^\lambda v \in \mathcal{W}_{\rho_3}$, for some set $\mathcal{W}_{\rho_3}$ of cardinality at most $Q^{\sigma-\eta_1\rho_3}$. Therefore,

$$\widehat{g}(t) = G_1(t) + G_2(t),$$

$$\begin{aligned} G_1(t) &= \frac{1}{Q^\sigma}\sum_{u\in\mathcal{N}_\lambda}\sum_{v\in\mathcal{N}_{\sigma-\lambda}} f_{\mu_0+\lambda+\rho_3}(q^{\mu_0}(u+q^\lambda v))f(q^{\mu_0+\lambda}v)\times \\ &\qquad\qquad \times \overline{f_{\mu_0+\lambda+\rho_3}(q^{\mu_0+\lambda}v)f_{\mu_1}(q^{\mu_0}u)}\mathrm{e}_\sigma(-ut)\mathrm{e}_{\sigma-\lambda}(-vt), \\ G_2(t) &= \frac{1}{Q^\sigma}\sum_{w\in\mathcal{N}_\sigma} b(w)\mathrm{e}_\sigma(-wt), \end{aligned}$$

with $|b(w)| \leq 2$, supported on $\mathcal{W}_{\rho_3}$.

In the sum $G_1(t)$, we detect the congruence class $w = v \pmod{q^{\rho_3}}$ by orthogonality, and write

$$\begin{aligned} f_{\mu_0+\lambda+\rho_3}(q^{\mu_0+\lambda}v) &= f_{\mu_0+\lambda+\rho_3}(q^{\mu_0+\lambda}w), \\ f_{\mu_0+\lambda+\rho_3}(q^{\mu_0}(u+q^\lambda v)) &= f_{\mu_0+\lambda+\rho_3}(q^{\mu_0}(u+q^\lambda w)). \end{aligned}$$

We obtain

$$G_1(t) = \sum_{\ell\in\mathcal{O}^\vee/q^{\rho_3}} d_h(\ell)\frac{1}{Q^{\rho_3}}\sum_{w\in\mathcal{O}/q^{\rho_3}}\mathrm{e}_{\rho_3}(-\ell w)c_h(w),$$

where

$$d_t(\ell) = \frac{1}{Q^{\sigma-\lambda}}\sum_{v\in\mathcal{N}_{\sigma-\lambda}} f(q^{\mu_0+\lambda}v)\mathrm{e}_{\sigma-\lambda}(-vt)\mathrm{e}_{\rho_3}(v\ell),$$

$$c_h(w) = \frac{\overline{f_{\mu_0+\lambda+\rho_3}(q^{\mu_0+\lambda}w)}}{Q^\lambda}\sum_{u\in\mathcal{N}_\lambda} f_{\mu_0+\lambda+\rho_3}(q^{\mu_0}(u+q^\lambda w))\overline{f_{\mu_1}(q^{\mu_0}u)}\mathrm{e}_\sigma(-ut).$$

By splitting again $u = u_0 + q^{\mu_1-\mu_0}u_1$ with $u_0 \in \mathcal{N}_{\mu_1-\mu_0}$ and $u_1 \in \mathcal{N}_{\lambda-\mu_1+\mu_0}$, we get that under the additional assumption $\rho_3 \leq \lambda$,

$$\begin{aligned} |c_h(w)| &\leq \frac{1}{Q^{\mu_1-\mu_0}}\sum_{u_0\in\mathcal{N}_{\mu_1-\mu_0}}\Big|\sum_{u_1\in\mathcal{N}_{\lambda-\mu_1+\mu_0}} f(q^{\mu_0}(u_0+q^{\mu_1-\mu_0}u_1+q^\lambda w))\mathrm{e}_{\sigma-\mu_1+\mu_0}(-u_1t)\Big| \\ &\ll Q^{-\eta'\gamma(\lambda+\rho_3)+\mu_1-\mu_0+\rho_3} \end{aligned}$$

by Lemma 10. We can now sum over h. Using the Cauchy–Schwarz inequality and Parseval's equality as in [MR15], we get

$$\sum_{\substack{h\in\mathcal{O}^\vee\\ \|h/q^{\sigma-\rho}\|\leq 1}} |G_1(h+t)|^2 \leq \sup_{\substack{t'\in K\\ w\in\mathcal{O}/q^{\rho_3}}} |c_{t'}(w)|^2 \sup_{\ell\in\mathcal{O}^\vee/q^{\rho_3}} \sum_{\substack{h\in\mathcal{O}^\vee\\ \|h/q^{\sigma-\lambda}\|\leq 1}} |d_h(\ell)|^2.$$

We write

$$\sum_{\substack{h\in\mathcal{O}^\vee\\ \|h/q^{\sigma-\lambda}\|\leq 1}} |d_{h+t}(\ell)|^2 = \sum_{\alpha\in\mathcal{O}^\vee/q^{\sigma-\lambda}} |d_{\alpha+t}(\ell)|^2 \sum_{\substack{h\in\mathcal{O}^\vee\\ h-\alpha\in q^{\sigma-\lambda}\mathcal{O}^\vee\\ \|h/q^{\sigma-\lambda}\|\leq 1}} 1.$$

Note that the last sum is $O(1)$, and the remaining sum over α is again $O(1)$ by Parseval's identity. We deduce

$$\sum_{\substack{h\in\mathcal{O}^\vee\\ \|h/q^{\sigma-\rho}\|\leq 1}} |G_1(h+t)|^2 \ll Q^{-2\eta'\gamma(\lambda)+2(\mu_1-\mu_0+\rho_3)}.$$

On the other hand, by Parseval's equality and reasoning as above,

$$\sum_{\substack{h\in\mathcal{O}^\vee\\ \|h/q^{\sigma-\lambda}\|\le 1}}|G_2(h+t)|^2\le\sum_{\substack{h\in\mathcal{O}^\vee\\ \|h/q^{\sigma}\|\ll 1}}|G_2(h+t)|^2\ll\frac{1}{Q^\sigma}\sum_{w\in\mathcal{N}_\sigma}|b(w)|^2\ll Q^{-\eta_1\rho_3},$$

and by optimising ρ_3 (note that we always have $\eta'\gamma(\lambda)\le\lambda$ by (2.7)), the result follows. □

3.4. **Sums over lattices.** In this section, we estimate sums over lattices that will appear repeatedly later in our arguments. As we already mentioned an additional difficulty when $d>1$ is the possibility of the multiplication by q skewing the lattice $\mathcal{O}$ (see [Mad10, pp. 203–204]). This issue does not occur in $\mathcal{O}$ thanks to the additional structure of the unit group $\mathcal{O}^*$.

Lemma 11. *Let $\mathfrak{a}$ be a fractional ideal, and $R\ge 0$. Then*

$$\operatorname{card}\{h\in\mathfrak{a}\smallsetminus\{0\},\|h\|\le R\}\ll N(\mathfrak{a})^{-1}R^d.$$

Proof. As in the proof of Lemma 7, let $\mathfrak{c}\subset\mathcal{O}$ be an ideal in the same class as $\mathfrak{a}$, with $1\le N(\mathfrak{c})\ll 1$. Then $\mathfrak{a}\subset\mathfrak{c}^{-1}\mathfrak{a}=(u)$ for some $u\in K$ with $N(u)\asymp N(\mathfrak{a})$, and by multiplying by units we may impose $|u^\pi|\asymp N(u)^{1/d}$. Then

$$\begin{aligned}\operatorname{card}\{h\in\mathfrak{a},h\ne 0,\|h\|\le R\}&\le\operatorname{card}\{h\in\mathcal{O},h\ne 0\|uh\|\le R\}\\&\le\operatorname{card}\{h\in\mathcal{O},h\ne 0,\|h\|\le CRN(u)^{-1/d}\}\end{aligned}$$

for $C\ll 1$, since $\|uh\|\le R$ implies $\|h\|\ll\|u^{-1}\|\ll N(u)^{-1/d}$. The last cardinality is simple to evaluate, since the basis (ω_j) of $\mathcal{O}$ satisfies $\|\omega_j\|\ll 1$. □

Lemma 12. *Let $\mathfrak{t}$ be an integral ideal, $\alpha,\beta\in\mathfrak{t}^{-1}$ and $q\in\mathcal{O}$. Then*

$$\operatorname{card}\{n\in\mathcal{O}/q,\alpha n+\beta\in q\mathfrak{t}^{-1}\}\le N(\alpha\mathfrak{t}+(q)).$$

Proof. By homogeinizing, we have

$$\operatorname{card}\{n\in\mathcal{O}/q,\alpha n+\beta\in q\mathcal{O}^\vee\}\le\operatorname{card}\{n\in\mathcal{O}/q,n\alpha\in q\mathcal{O}^\vee\}.$$

Let $\alpha_0=\alpha\mathfrak{t}$ and $\mathfrak{d}=\alpha_0+(q)$. The condition $n\alpha\in q\mathfrak{t}^{-1}$ becomes $(q)\mid n\alpha_0$ and so $n\in I$, where $I=(q)\mathfrak{d}^{-1}$ is an integral ideal. But $|I/(q)|=|\mathcal{O}/\mathfrak{d}|=N(\mathfrak{d})$ as claimed. □

Lemma 13. *Let $s_1,s_2,q\in\mathcal{O}$ with $q\mid s_j$. Let $\mathfrak{t}$ be an integral ideal, and $\alpha,\beta\in\mathfrak{t}^{-1}$. Let $V_0:\mathbb{R}^d\to\mathbb{C}$ be in the Schwartz class, and define two functions on K by $V=V_0\circ\iota^{-1}$ and $\widehat{V}=\widehat{V_0}\circ(\iota^\vee)^{-1}$. Then*

$$\sum_{m\in\mathcal{O}}V\Big(\frac{m}{s_1}\Big)\Big|\sum_{n\in\mathcal{O}}V\Big(\frac{n}{s_2}\Big)\mathrm{e}\Big(\Big\langle\frac{n(\alpha m+\beta)}{q}\Big\rangle\Big)\Big|\ll\frac{N(s_1)N(s_2)}{N(q)}N(\alpha\mathfrak{t}+(q))N(\mathfrak{t}).$$

Proof. Note first that by the Poisson summation formula, for any $\eta\in K\smallsetminus\{0\}$ and $t\in K$,

$$\sum_{n\in\mathcal{O}}V\Big(\frac{n}{\eta}\Big)\mathrm{e}(\langle nt\rangle)=N(\eta)\sum_{\xi\in\mathcal{O}^\vee}\widehat{V}(\eta(\xi+t)).$$

Therefore, we have

$$\begin{aligned}
&\sum_{m\in\mathcal{O}} V\Big(\frac{m}{s_1}\Big)\Big|\sum_{n\in\mathcal{O}} V\Big(\frac{n}{s_2}\Big)\mathrm{e}\Big(\Big\langle\frac{n(\alpha m+\beta)}{q}\Big\rangle\Big)\Big| \\
&\le N(s_2)\sum_{m\in\mathcal{O}} V\Big(\frac{m}{s_1}\Big)\sum_{\xi\in\mathcal{O}^\vee}\Big|\widehat{V}\Big(s_2\Big(\frac{\alpha m+\beta}{q}+\xi\Big)\Big)\Big| \\
&\le N(s_2)\sum_{m\in\mathcal{O}} V\Big(\frac{m}{s_1}\Big)\sum_{\xi\in\mathfrak{t}^{-1}\mathcal{O}^\vee}\Big|\widehat{V}\Big(s_2\Big(\frac{\alpha m+\beta}{q}+\xi\Big)\Big)\Big| \\
&\le N(s_2)\sum_{m_0\in\mathcal{O}/q}\sum_{\xi\in\mathfrak{t}^{-1}\mathcal{O}^\vee}\Big|\widehat{V}\Big(s_2\Big(\frac{\alpha m_0+\beta}{q}+\xi\Big)\Big)\Big|\sum_{\substack{m\in\mathcal{O}\\ m\equiv m_0 \pmod q}} V\Big(\frac{m}{s_1}\Big).
\end{aligned}$$

Again by Poisson summation,

$$\begin{aligned}
\Big|\sum_{\substack{m\in\mathcal{O}\\ m\equiv m_0 \pmod q}} V\Big(\frac{m}{s_1}\Big)\Big| &= \frac{N(s_1)}{N(q)}\Big|\sum_{\omega\in\mathcal{O}^\vee}\widehat{V}\Big(\frac{s_1\omega}{q}\Big)\mathrm{e}\Big(\Big\langle\frac{-m_0\omega}{q}\Big\rangle\Big)\Big| \\
&\le \frac{N(s_1)}{N(q)}\sum_{\omega\in\mathcal{O}^\vee}\Big|\widehat{V}\Big(\frac{s_1\omega}{q}\Big)\Big| \\
&\ll_V \frac{N(s_1)}{N(q)}.
\end{aligned}$$

Next, by Lemma 12 with $\mathfrak{t}\leftarrow\mathfrak{t}D_K$ (where we recall that $D_K=(\mathcal{O}^\vee)^{-1}$ is the different ideal), for each $\gamma\in\mathfrak{t}^{-1}\mathcal{O}^\vee/q$, the number of $m_0\in\mathcal{O}/q$ such that $\alpha m_0+\beta\equiv\gamma \pmod{q\mathfrak{t}^{-1}\mathcal{O}^\vee}$ is at most $N(\alpha\mathfrak{t}D_k+(q))\ll_K N(\alpha\mathfrak{t}+(q))$. Therefore,

$$\begin{aligned}
\sum_{m_0\in\mathcal{O}/q}\sum_{\xi\in\mathfrak{t}^{-1}\mathcal{O}^\vee}\Big|\widehat{V}\Big(s_2\Big(\frac{\alpha m_0+\beta}{q}+\xi\Big)\Big)\Big| &\ll N(\alpha\mathfrak{t}+(q))\sum_{\xi\in\mathfrak{t}^{-1}\mathcal{O}^\vee}\sum_{\gamma\in\mathfrak{t}^{-1}\mathcal{O}^\vee/q}\Big|\widehat{V}\Big(s_2\Big(\frac{\gamma}{q}+\xi\Big)\Big)\Big| \\
&= N(\alpha\mathfrak{t}+(q))\sum_{\xi\in\mathfrak{t}^{-1}\mathcal{O}^\vee}\Big|\widehat{V}\Big(\frac{s_2\xi}{q}\Big)\Big| \\
&\ll N(\alpha\mathfrak{t}+(q))\sum_{\xi\in\mathfrak{t}^{-1}\mathcal{O}^\vee}\frac{1}{(1+\|\xi\|)^{d+1}}.
\end{aligned}$$

By Lemma 11 and partial summation, we obtain $\sum_{\xi\in\mathfrak{t}^{-1}\mathcal{O}^\vee}(1+\|\xi\|)^{-d-1}\ll N(\mathfrak{t})$, which concludes our proof. □

Lemma 14. *Let $R\ge 0$, $\mathfrak{t}$ be an integral ideal, and $q\in\mathcal{O}$. Then*

$$\sum_{\substack{h\in\mathfrak{t}^{-1}\mathcal{O}\\ 0<\|h\|\le R}} N(h\mathfrak{t}+(q))\ll\tau(q)R^dN(\mathfrak{t}),$$

where $\tau(q)$ is the number of integral ideal divisors of (q), and the implicit constant depends on K only.

Proof. In our sum, we sort according to the ideal $\mathfrak{d} = h\mathfrak{t}+(q)$ and use Lemma 11, getting

$$\begin{aligned}\sum_{\substack{h\in\mathfrak{t}^{-1}\mathcal{O}\\ 0<\|h\|\leq R}} N(h\mathfrak{t}+(q)) &\leq \sum_{\mathfrak{d}|q} N(\mathfrak{d}) \sum_{\substack{h\in\mathfrak{d}\mathfrak{t}^{-1}\mathcal{O}\\ 0<\|h\|\leq R}} 1\\ &\ll_K \sum_{\mathfrak{d}|q} R^d N(\mathfrak{t})\\ &\ll \tau(q) R^d N(\mathfrak{t}).\end{aligned}$$

□

Lemma 15. *Let $\mathfrak{t}$ be an integral ideal, $q \in \mathcal{O}$ and $R_0, R_1 \in \mathbb{R}_+$. Then*

$$\sum_{\substack{h_0,h_1\in\mathfrak{t}^{-1}\\ h_0+h_1\neq 0\\ \|h_j\|\leq R_j}} N((h_0+h_1)\mathfrak{t}+(q)) \ll \tau(q) N(\mathfrak{t}^2)(R_0+1)^d(R_0+R_1)^d.$$

Proof. Given a non-zero fractional ideal $\mathfrak{a} \subset \mathfrak{t}^{-1}$, we have

$$\sum_{\substack{h_0,h_1\in\mathfrak{t}^{-1}\\ \|h_j\|\leq R_j\\ 0\neq h_0+h_1\in\mathfrak{a}}} 1 \leq \sum_{\substack{h_0\in\mathfrak{t}^{-1}\\ \|h_0\|\leq R_0}} \sum_{\substack{h'\in\mathfrak{a}\smallsetminus\{0\}\\ \|h'\|\leq R_0+R_1}} 1 \ll N(\mathfrak{t}\mathfrak{a}^{-1})(1+R_0)^d(R_0+R_1)^d$$

By Lemma 11. The conclusion follows by setting $\mathfrak{a} = \mathfrak{d}\mathfrak{t}^{-1}$ and summing over $\mathfrak{d} \mid q$, against $N(\mathfrak{d}) = \det(\mathfrak{a})N(\mathfrak{t})$, similarly as in Lemma 14. □

4. Type I sums

The following estimate is a generalization of Proposition 1 of [MR15].

Proposition 2. *Let $f : \mathcal{O} \to \mathbb{C}$ satisfy the Carry and Fourier properties* (2.5)–(2.6). *Let $V_0 : \mathbb{R}^d \to \mathbb{C}$ be a smooth map, compactly supported inside $\mathbb{R}^d \smallsetminus \{0\}$. Let $V = V_0 \circ \iota^{-1} : K \to \mathbb{C}$, define $\widehat{V} = \widehat{V_0} \circ (\iota^\vee)^{-1}$ and*

$$\Sigma_V := \sum_{\xi\in\mathcal{O}^\vee} |\widehat{V}(\xi)|.$$

Then for $\mu \leq \frac{c}{c+2}\nu$, we have

$$S_I = \sum_{m\in\mathcal{N}_\mu} \Big| \sum_{n\in\mathcal{O}} V\Big(\frac{mn}{q^{\mu+\nu}}\Big) f(mn)\Big| \ll \Sigma_V \mu^{d+1} Q^{\mu+\nu-\frac{\eta_1}{1+\eta_1}\gamma(\nu-\mu)}. \tag{4.1}$$

The implied constant depends on $(q, \mathcal{D})$, and on the diameter of the support of V.

Remark.

— The same bound holds, with the same proof, for the more general quantity

$$\sum_{m\in\mathcal{N}_\mu} \max_{a\in\mathcal{O}/m} \Big| \sum_{n\in\mathcal{O}} V\Big(\frac{mn+a}{q^{\mu+\nu}}\Big) f(mn+a)\Big|. \tag{4.2}$$

— The bounds (4.1) and (4.2) can be viewed as a statement on cancellations of $f(n)$ on average over arithmetic progressions $n \equiv 0 \pmod m$; this is an analogue of the Bombieri-Vinogradov theorem in the context of multiplicative number theory. Bounds of the type (4.1) go back to work of Fouvry and Mauduit [FM96b]. The quality of the bound (4.1) can be measured by the exponent of distribution, which is the maximum asymptotically allowable value for the ratio $\frac{\mu}{\mu+\nu}$. As in [MR15], we have $\vartheta = \frac{c}{2(c+1)}$, independently of γ, and this value on the exponent is precisely

the analogue of the Bombieri-Vinogradov theorem if c can be picked arbitrarily large; in both cases, the limitation arises from the large sieve inequality.

— Obtaining an exponent of distribution greater than $1/2$ is a challenging question in general. In the sum-of-digits case $f(n) = (-1)^{s_q(n)}$, such a result was obtained in [FM96b] with a value $\vartheta \geq 0.55711$ (and a slightly larger exponent for $q = 2$). This has been improved to $\vartheta \geq 2/3$ in [MS17]; a proof of the value $\vartheta = 1$ has recently been announced by Spiegelhofer [Spi18].

Proof. First note that replacing ν by $\nu + C$, for some C depending on $(q, \mathcal{D})$ and V, and rescaling V accordingly, we may assume that $V(x) \neq 0 \implies x \in \mathcal{F}$. For any $\ell \in \mathbb{N}_{\mu+\nu}$, we have

$$V\Big(\frac{\ell}{q^{\mu+\nu}}\Big) = \sum_{\substack{u\in\mathcal{O}\\ q^{\mu+\nu}|u-\ell}} V\Big(\frac{u}{q^{\mu+\nu}}\Big)$$

by our hypothesis on the support of V. Then

$$\begin{aligned}
S_I &= \sum_{m\in\mathcal{N}_\mu} \Big| \sum_{n\in\mathcal{O}} V\Big(\frac{mn}{q^{\mu+\nu}}\Big) f(mn)\Big| \\
&= \sum_{m\in\mathcal{N}_\mu} \frac{1}{N(m)} \Big| \sum_{k\in\mathcal{O}^\vee/m} \sum_{\ell\in\mathcal{N}_{\mu+\nu}} \mathrm{e}\Big(\Big\langle \frac{k\ell}{m}\Big\rangle\Big) V\Big(\frac{\ell}{q^{\mu+\nu}}\Big) f(\ell)\Big| \\
&= \sum_{m\in\mathcal{N}_\mu} \frac{1}{N(m)Q^{\mu+\nu}} \Big| \sum_{k\in\mathcal{O}^\vee/m} \sum_{h\in\mathcal{O}^\vee/q^{\mu+\nu}} \sum_{\ell\in\mathcal{N}_{\mu+\nu}} \mathrm{e}\Big(\Big\langle \frac{k\ell}{m}\Big\rangle\Big) \mathrm{e}_{\mu+\nu}(-h\ell) f(\ell) \times \\
&\qquad\qquad \times \sum_{u\in\mathcal{O}} V\Big(\frac{u}{q^{\mu+\nu}}\Big) \mathrm{e}_{\mu+\nu}(hu)\Big|.
\end{aligned}$$

The Poisson formula yields

$$\sum_{u\in\mathcal{O}} V\Big(\frac{u}{q^{\mu+\nu}}\Big) \mathrm{e}_{\mu+\nu}(hu) = Q^{\mu+\nu} \sum_{v\in\mathcal{O}^\vee} \widehat{V}(h - q^{\mu+\nu}v),$$

and so

$$\sum_{h\in\mathcal{O}^\vee/q^{\mu+\nu}} \Big| \sum_{u\in\mathcal{O}} V\Big(\frac{u}{q^{\mu+\nu}}\Big) \mathrm{e}_{\mu+\nu}(hu)\Big| \leq Q^{\mu+\nu} \sum_{v\in\mathcal{O}^\vee} |\widehat{V}(v)| \ll \Sigma_V Q^{\mu+\nu}.$$

Therefore,

$$S_I \ll \Sigma_V Q^{\mu+\nu} \sup_{t\in K} \sum_{m\in\mathcal{N}_\mu} \frac{1}{N(m)} \sum_{k\in\mathcal{O}^\vee/m} \Big|\widehat{f}_{\mu+\nu}\Big(t - \frac{k}{m} q^{\mu+\nu}\Big)\Big|,$$

where

$$\widehat{f}_\lambda(t) = \frac{1}{Q^\lambda} \sum_{\ell\in\mathcal{N}_\ell} f(\ell) \mathrm{e}_\lambda(-t\ell).$$

Now, by computations identical to [MR15, pp. 2606-2607], we write

$$\widehat{f}_{\mu+\nu}(t) = G_{\kappa,1}(t) + G_{\kappa,2}(t), \tag{4.3}$$

where

$$\begin{aligned}
G_{\kappa,1}(t) = \sum_{h\in\mathcal{O}^\vee/q^{\rho_1}} &\Big(\frac{1}{Q^\kappa} \sum_{u\in\mathcal{N}_\kappa} c_{\kappa,\rho_1}(u,h) \mathrm{e}_{\mu+\nu}(-ut)\Big) \\
&\times \Big(\frac{1}{Q^{\mu+\nu-\kappa}} \sum_{v\in\mathcal{N}_{\mu+\nu-\kappa}} f(vq^\kappa) \mathrm{e}_{\mu+\nu-\kappa}(-tv) \mathrm{e}_{\rho_1}(hv)\Big),
\end{aligned}$$

$$c_{\kappa,\rho_1}(u,h)=\frac{1}{Q^{\rho_1}}\sum_{w\in\mathcal{N}_{\rho_1}} f_{\kappa+\rho_1}(u+wq^\kappa)\overline{f_{\kappa+\rho_1}(wq^\kappa)}\mathrm{e}_{\rho_1}(-hw),$$

and

$$G_{\kappa,2}(t)=\frac{1}{Q^{\mu+\nu}}\sum_{(u,v)\in\mathcal{N}_\kappa\times\mathcal{N}_{\mu+\nu-\kappa}} f(vq^\kappa)\mathrm{e}_{\mu+\nu}(-(u+vq^k)t)$$
$$\times\Big(f(u+vq^\kappa)\overline{f(vq^\kappa)}-f_{\kappa+\rho_1}(u+vq^\kappa)\overline{f_{\kappa+\rho_1}(vq^\kappa)}\Big).$$

By the carry property (2.5), we have $f(u+vq^\kappa)\overline{f(vq^\kappa)}=f_{\kappa+\rho_1}(u+vq^\kappa)\overline{f_{\kappa+\rho_1}(vq^\kappa)}$ unless (u,v) belongs to a subset $\mathcal{W}_{\kappa,\rho_1}\mathcal{N}_\kappa\times\mathcal{N}_{\mu+\nu-\kappa}$ of size at most

$$|\mathcal{W}_{\kappa,\rho_1}|\ll Q^{\mu+\nu-\eta_1\rho_1}.$$

If κ satisfies $(c+1)\kappa\le c(\mu+\nu)$, then we have

$$G_{\kappa,1}(t)\ll Q^{-\gamma(\mu+\nu-\kappa)}\sum_{h\in\mathcal{O}^\vee/q^{\rho_1}}\frac{1}{Q^\kappa}\Big|\sum_{u\in\mathcal{N}_\kappa}c_{\kappa,\rho_1}(u,h)\mathrm{e}_{\mu+\nu}(-ut)\Big| \tag{4.4}$$

uniformly.

For all $m\in\mathcal{N}_\mu$ and $k\in\mathcal{O}^\vee/m$, there is a unique ideal $\mathfrak{m}$ dividing m, and proper additive character $\sigma \pmod{\mathfrak{m}}$ such that $\sigma(\xi)=\mathrm{e}(\langle\xi k/m\rangle)$ for all $\xi\in\mathcal{O}$; we write $(k,m)\sim\sigma$. Note that we have $N(\mathfrak{m})\ll Q^\mu$. We rearrange our sum as

$$\sum_{m\in\mathcal{N}_\mu}\frac{1}{N(m)}\sum_{k\in\mathcal{O}^\vee/m}\Big|\widehat{f}_{\mu+\nu}\Big(t-\frac{k}{m}q^{\mu+\nu}\Big)\Big|$$
$$=\sum_{\substack{\mathfrak{m}\text{ ideal}\\ N(\mathfrak{m})\ll Q^\mu}}\sum_{\sigma \pmod{\mathfrak{m}}^*}\sum_{m\in\mathcal{N}_\mu}\frac{1}{N(m)}\sum_{\substack{k\in\mathcal{O}^\vee/m\\(m,k)\sim\sigma}}\Big|\widehat{f}_{\mu+\nu}\Big(t-\frac{k}{m}q^{\mu+\nu}\Big)\Big|.$$

For each $\mathfrak{m}$ in this sum, we apply the decomposition (4.3) with the unique integer $\kappa_{\mathfrak{m}}$ for which $Q^{\kappa_{\mathfrak{m}}-1}<N(\mathfrak{m})^2\le Q^{\kappa_{\mathfrak{m}}}$. Hence $0\le\kappa_{\mathfrak{m}}\le 2\mu+C$ where $C=1+\Big\lfloor\frac{2\log R^*_{\mathcal{F}}}{\log 2}\Big\rfloor$. Call $S_{I,1}$, resp. $S_{I,2}$ the contribution of $G_{\kappa,1}$, resp. $G_{\kappa,2}$. The inequality (4.4) holds if we assume $\mu\le\frac{c}{c+2}\nu-C\frac{c+1}{c+2}$. We obtain, using Cauchy–Schwarz,

$$S_{I,1}\ll\Sigma_V Q^{\mu+\nu+\rho_1/2}\sup_{t\in K}\sum_{\kappa=0}^{2\mu+C}\frac{(T_1(\kappa)T_2(\kappa))^{1/2}}{Q^{\kappa+\gamma(\mu+\nu-\kappa)}},$$

where

$$T_1(\kappa):=\sum_{h\in\mathcal{O}^\vee/q^{\rho_1}}\sum_{Q^{(\kappa-1)/2}<N(\mathfrak{m})\le Q^{\kappa/2}}\sum_{\sigma \pmod{\mathfrak{m}}^*}\Big|\sum_{u\in\mathcal{N}_\kappa}c_{\kappa,\rho_1}(u,h)\mathrm{e}_{\mu+\nu}(-ut)\sigma(u)\Big|^2.$$

$$T_2(\kappa):=\sum_{Q^{(\kappa-1)/2}<N(\mathfrak{m})\le Q^{\kappa/2}}\sum_{\sigma \pmod{\mathfrak{m}}^*}\Big(\sum_{m\in\mathcal{N}_\mu}\sum_{\substack{k\in\mathcal{O}^\vee/m\\(m,k)\sim\sigma}}\frac{1}{N(m)}\Big)^2.$$

Using Lemma 4, we get $T_2(\kappa)\ll\mu^{2d}$. On the other hand, by Lemma 7, we have

$$T_1(\kappa)\ll\kappa^{d(d-1)}\sum_{h\in\mathcal{O}^\vee/q^{\rho_1}}Q^\kappa\sum_{u\in\mathcal{N}_\kappa}|c_{\kappa,\rho_1}(u,h)|^2=\kappa^{d(d-1)}Q^{2\kappa},$$

and we conclude

$$S_{I,1}\ll\mu^{d^2}\Sigma_V Q^{\mu+\nu+\rho_1/2-\gamma(\nu-\mu)}$$

whenever $\mu\le\frac{c}{c+2}\nu-C\frac{c+1}{c+2}$ and $\rho_1\le\nu-\mu$.

Let $d_\kappa(u,v) := f(u+vq^\kappa)\overline{f(vq^\kappa)} - f_{\kappa+\rho_1}(u+vq^\kappa)\overline{f_{\kappa+\rho_1}(vq^\kappa)}$, which is of modulus at most 2 and vanishes unless $(u,v) \in \mathcal{W}_{\kappa,\rho_1}$. We have

$$|G_{\kappa,2}(t)| \leq Q^{-\mu-\nu} \sum_{v \in \mathcal{N}_{\mu+\nu-\kappa}} \Big| \sum_{u \in \mathcal{N}_\kappa} d_\kappa(u,v) \mathrm{e}_{\mu+\nu}(-ut) \Big|,$$

from which we deduce, similarly as above,

$$\begin{aligned}
S_{I,2} &\ll \Sigma_V Q^{\mu+\nu} \sup_t \sum_{m \in \mathcal{N}_\mu} \frac{1}{N(m)} \sum_{k \in \mathcal{O}^\vee/m} \Big| G_{\kappa,2}\Big(t - \frac{k}{m} q^{\mu+\nu}\Big) \Big| \\
&\ll \mu^d \Sigma_V \sup_t \sum_{\kappa=0}^{2\mu+C} Q^{-\kappa/2} \sum_{\substack{\mathfrak{m} \text{ ideal} \\ N(\mathfrak{m})^2 \leq Q^\kappa}} \sum_{\sigma \pmod{\mathfrak{m}}^*} \sum_{v \in \mathcal{N}_{\mu+\nu-\kappa}} \Big| \sum_{u \in \mathcal{N}_\kappa} d_\kappa(u,v) \mathrm{e}_{\mu+\nu}(-ut) \sigma(u) \Big| \\
&\ll \mu \Sigma_V Q^{\frac{\mu+\nu}{2}} \sup_t \sum_{\kappa=0}^{2\mu+C} Q^{-\kappa/2} \times \\
&\qquad \times \Big(\sum_{v \in \mathcal{N}_{\mu+\nu-\kappa}} \sum_{\substack{\mathfrak{m} \text{ ideal} \\ N(\mathfrak{m}) \leq Q^\kappa}} \sum_{\sigma \pmod{\mathfrak{m}}^*} \Big| \sum_{u \in \mathcal{N}_\kappa} d_\kappa(u,v) \mathrm{e}_{\mu+\nu}(-ut) \sigma(u) \Big|^2 \Big)^{1/2} \\
&\ll \mu^{d+1} \Sigma_V Q^{\mu+\nu-\eta_1\rho_1/2}.
\end{aligned}$$

We choose $\rho_1 = \frac{2}{1+\eta_1}\gamma(\nu-\mu)$. This gives the bound (4.1) if $\mu \leq \frac{c}{c+2}\nu - C\frac{c+1}{c+2}$. If $C > 0$, then replacing ν by $\nu + \lfloor C(c+1)/c \rfloor + 1$ and rescaling V accordingly yields our result as stated. □

5. Type II sums

The following estimate is an analogue of Proposition 2 of [MR15], and is the core of the argument. Given a sequence $(\alpha_m)_{m\in\mathcal{O}}$ and $p \geq 1$, we denote by $\|\alpha\|_p$ the usual ℓ^p norm of (α_m).

Proposition 3. *Let $f : \mathcal{O} \to \mathbb{C}$ satisfy the Carry and Fourier properties (2.5)–(2.6), for some $c \geq 20\Theta\theta^{-1}$. Let $2 \leq \mu \leq \nu$, $(\alpha_m)_{m\in\mathcal{N}_\mu}$ and $(\beta_n)_{n\in\mathcal{N}_\nu}$ be two sequences of complex numbers, and $\psi : K \to \mathbb{R}$ be a linear map. Then we have*

$$S_{II} = \sum_{m \in \mathcal{N}_\mu} \sum_{n \in \mathcal{N}_\nu} \alpha_m \beta_n f(mn) \mathrm{e}(\psi(mn)) \ll \mu^{O(1)} \|\alpha\|_2 \|\beta\|_4 Q^{\mu/2+3\nu/4-\delta\gamma(\lfloor \frac{\mu}{20\Theta\theta^{-1}} \rfloor)}, \tag{5.1}$$

where

$$\delta = c \min\{\eta_1^2\eta_2, \eta_1\theta\}$$

for some absolute constant $c > 0$. The implied constant depends at most on $(q, \mathcal{D})$ and $\|\cdot\|$.

We let V_1 be given as in Lemma 6, and as before define $V, \widehat{V} : K \to \mathbb{C}$ by $V = V_1 \circ \iota^{-1}$ and $\widehat{V} = \widehat{V_1} \circ (\iota^\vee)^{-1}$, so that for any $\lambda \in \mathbb{N}$, we have $\mathbf{1}_{n\in\mathcal{N}_\lambda} \leq V(n/q^\lambda)$, and $\widehat{V}(\xi) = 0$ for $\|\xi\| > 1$.

5.1. **Preparatory lemma.** As in [MR15], we will now use the carry property (2.5) in the context of a multiplicative convolution $mn = u_1 + q^\kappa v$, and so we wish to count the pairs (m,n) yielding exceptional values of v. The following lemma is the analogue of Lemmas 7 to 9 of [MR15].

Lemma 16.

(1) For any finite set $\mathcal{B} \subset \mathcal{O}$ and $\mu, \mu', \nu \in \mathbb{N}$ with $\mu' \geq \mu$, we have

$$\operatorname{card}\Big\{(m,n) \in \mathcal{N}_\mu \times \mathcal{N}_\nu, \exists u \in \mathcal{N}_{\mu'}, v \in \mathcal{B}, mn = u + q^{\mu'} v\Big\} \ll \mu^d Q^{\mu'} \operatorname{card} \mathcal{B}.$$

(2) For $\mu, \nu, \rho \in \mathbb{N}$ with $\rho \leq 2\nu$, we have

$$\operatorname{card}\Big\{(m,n) \in \mathcal{N}_\mu \times \mathcal{N}_\nu, \exists k \in \mathcal{N}_{\mu+\rho}, f(mn+k)\overline{f(mn)} \neq f_{\mu+2\rho}(mn+k)\overline{f_{\mu+2\rho}(mn)}\Big\} \ll \mu^d Q^{\mu+\nu-\eta_1\rho}.$$

(3) Let $\mu, \nu, \mu_0, \mu_1, \mu_2 \in \mathbb{N}$, and assume that $\mu_0 \leq \mu_1 \leq \mu \leq \mu_2$. For all $a, b, c \in \mathcal{O}$, the number $\mathcal{E}(a,b,c)$ of pairs $(m,n) \in \mathcal{N}_\mu \times \mathcal{N}_\nu$ such that

$$f_{\mu_2}(mn+am+bn+c)\overline{f_{\mu_2}(q^{\mu_0} r_{\mu_0,\mu_2}(mn+am+bn+c))} \neq f_{\mu_1}(mn+am+bn+c)\overline{f_{\mu_1}(q^{\mu_0} r_{\mu_0,\mu_2}(mn+am+bn+c))}$$

satisfies

$$\mathcal{E}(a,b,c) \ll \mu_2^{O_q(1)} Q^{\mu+\nu-\eta_1(\mu_1-\mu_0)}.$$

Proof. (1) Following [MR15, p.2603], the quantity we wish to bound is at most

$$\sum_{m\in\mathcal{N}_\mu} \sum_{v\in\mathcal{B}} \sum_{\substack{u\in\mathcal{O} \\ u\equiv -q^{\mu'}v \pmod m}} V\Big(\frac{u}{q^{\mu'}}\Big)$$

$$= Q^{\mu'} \sum_{m\in\mathcal{N}_\mu} \frac{1}{N(m)} \sum_{v\in\mathcal{B}} \sum_{k\in\mathcal{O}^\vee/m} \mathrm{e}\Big(\Big\langle \frac{q^{\mu'}kv}{m}\Big\rangle\Big) \sum_{u\in\mathcal{O}} \widehat{V}\Big(q^{\mu'}\Big(\xi + \frac{k}{m}\Big)\Big)$$

$$\ll (\operatorname{card}\mathcal{B}) Q^{\mu'} \sum_{m\in\mathcal{N}_\mu} \frac{1}{N(m)} \operatorname{card}\Big\{\xi \in \mathcal{O}^\vee, \|q^{\mu'}\xi/m\| \leq 1\Big\}.$$

The claimed bound then follows from the fact that the condition $\|q^{\mu'}\xi/m\| \leq 1$ implies $\|\xi\| \ll \|m/q^{\mu'}\| \ll 1$ (since $\mu' \geq \mu$), and by Lemma 4 with $\mathfrak{m} = (1)$ (so that the condition $(k,m) \sim \sigma$ is equivalent to $k = 0$).

(2) Using point (1) and the carry property (2.5), the argument given in [MR15] can be applied with no modifications.

(3) We use the carry property (2.5) with $\kappa \leftarrow \mu_0$, $\lambda \leftarrow \mu_2 - \mu_0$, $\rho \leftarrow \mu_1 - \mu_0$. We deduce that for some set $\mathcal{B} \subset \mathcal{N}_{\mu_2-\mu_0}$, with $\operatorname{card}\mathcal{B} \ll Q^{\mu_2-\mu_0-\eta_1(\mu_1-\mu_0)}$, we have

$$\mathcal{E}(a,b,c) \leq \sum_{\ell\in\mathcal{B}} \operatorname{card}\{(m,n) \in \mathcal{N}_\mu \times \mathcal{N}_\nu, r_{\mu_0,\mu_2}(mn+am+bn+c) = \ell\}$$

$$\leq \sum_{\ell\in\mathcal{B}} \sum_{m\in\mathcal{O}} V\Big(\frac{m}{q^\mu}\Big) \sum_{n\in\mathcal{O}} V\Big(\frac{n}{q^\nu}\Big) \psi_{\mu_2-\mu_0}\Big(\frac{mn+am+bn+c}{q^{\mu_2}} - \frac{\ell}{q^{\mu_2-\mu_0}}\Big).$$

We apply Lemma 9 with $\tau = 0$ and $\lambda = \mu_2 - \mu_0$, and use the triangle inequality along with the bound (3.3) with $A = d+1$, obtaining

$$\mathcal{E}(a,b,c) \ll \frac{\operatorname{card}\mathcal{B}}{Q^{\mu_2-\mu_0}} \sum_{\xi\in\mathcal{O}^\vee} \frac{1}{(1+\|q^{-\mu_2+\mu_0}\xi\|)^{d+1}} \sum_{n\in\mathcal{O}} V\Big(\frac{n}{q^\nu}\Big) \Big| \sum_{m\in\mathcal{O}} V\Big(\frac{m}{q^\mu}\Big) \mathrm{e}_{\mu_2}(\xi m(n+a))\Big|.$$

The contribution of $\xi = 0$ is $\ll (\operatorname{card}\mathcal{B}) Q^{\mu+\nu-\mu_2+\mu_0} \ll Q^{\mu+\nu-\eta_1(\mu_1-\mu_0)}$. To bound the remainder, we apply Lemma 13 with $\mathfrak{t} = q^{\mu_2-\mu} D_K$ (this gives a slight loss, which is why we isolated $\xi = 0$), getting

$$\sum_{n\in\mathcal{O}} V\Big(\frac{n}{q^\nu}\Big) \Big| \sum_{m\in\mathcal{O}} V\Big(\frac{m}{q^\mu}\Big) \mathrm{e}_{\mu_2}(\xi m(n+a))\Big| \ll Q^{\nu+\mu_2-\mu} N(\xi D_k + (q^\mu)),$$

and so, by Lemma 14 with $\mathfrak{t} = q^{\mu_2-\mu_0}D_K$,

$$\begin{aligned}\mathcal{E}(a,b,c) &\ll Q^{\mu+\nu-\eta_1(\mu_1-\mu_0)} + Q^{\nu+\mu_2-\mu-\eta_1(\mu_1-\mu_0)} \sum_{\substack{\xi\in q^{\mu_0-\mu_2}\mathcal{O}^\vee\\ \xi\neq 0}} \frac{N(\xi q^{\mu_2-\mu_0}D_K + (q^\mu))}{(1+\|\xi\|)^{d+1}}\\ &\ll Q^{\mu+\nu-\eta_1(\mu_1-\mu_0)} + \tau(q^{\mu_2-\mu_0}Q^{\mu+\nu-\mu_0-\eta_1(\mu_1-\mu_0)},\end{aligned}$$

whence the claimed bound.

□

5.2. **Van der Corput step.** The rest of this section is devoted to the proof of Proposition 3. Let $\rho_1, \rho_2, \rho \in \mathbb{N}$, assume that

$$\rho_2 \leq \rho_1, \quad \rho_1 + \rho \leq \frac{\mu}{2}, \tag{5.2}$$

and define

$$\mu_0 = \mu - 2(\rho_1+\rho), \quad \mu_1 = \mu - 2\rho_1, \quad \mu_2 = \mu + 2\rho_2.$$

We recall the definition (3.1), and we define further, for all $\lambda \in \mathbb{N}$,

$$\Delta_\lambda^* = \Delta_\lambda \smallsetminus \{0\}. \tag{5.3}$$

The beginning of the argument mirrors closely pp. 2610-2613 of [MR15], using the van der Corput inequality in the form of Lemma (3.1), twice. The computations being the same, we restrict to mentionning the main steps: we obtain, using Lemma 5, Cauchy–Schwarz's inequality, and 16.(2),

$$\begin{aligned}|S_{II}| &\leq \sum_{m\in\mathcal{O}} V\Big(\frac{m}{q^\mu}\Big)\Big|\sum_{n\in\mathcal{N}_\nu}\beta_n f(mn)\mathrm{e}(\psi(mn))\Big|\\ &\ll \|\alpha\|_2\|\beta\|_2 Q^{\mu/2+\nu/2-\rho_2/2}\\ &\quad + \|\alpha\|_2 Q^{\nu/2}\Big(Q^{-\rho_2}\sum_{r\in\Delta_{\rho_2}^*}\sum_{n\in\mathcal{N}_\nu}|\beta_{n+r}\beta_n|\Big|\sum_{m\in\mathcal{O}}V\Big(\frac{m}{q^\mu}\Big)f(mn+mr)\overline{f(mn)}\mathrm{e}(\psi(mr))\Big|\Big)^{1/2}\\ &\ll \mu^{d/4}\|\alpha\|_2\|\beta\|_4 Q^{\mu/2+3\nu/4-\eta_1\rho_2/4}\\ &\quad + \|\alpha\|_2 Q^{\nu/2}\Big(Q^{-\rho_2}\sum_{r\in\Delta_{\rho_2}^*}\sum_{n\in\mathcal{N}_\nu}|\beta_{n+r}\beta_n|\Big|\sum_{m\in\mathcal{O}}V\Big(\frac{m}{q^\mu}\Big)f_{\mu_2}(mn+mr)\overline{f_{\mu_2}(mn)}\mathrm{e}(\psi(mr))\Big|\Big)^{1/2}\\ &\ll \mu^{d/4}\|\alpha\|_2\|\beta\|_4 Q^{\mu/2+3\nu/4-\eta_1\rho_2/4} + \|\alpha\|_2\|\beta\|_4 Q^{\mu/4+\nu/2}\Big(Q^{-\rho_2-2\rho_1}\sum_{\substack{r\in\Delta_{\rho_2}^*\\ s\in\Delta_{2\rho_1}^*}}|S_{II,1}(r,s)|\Big)^{1/4},\end{aligned} \tag{5.4}$$

where

$$\begin{aligned}S_{II,1}(r,s) &= \sum_{n,m\in\mathcal{O}} V\Big(\frac{n}{q^\nu}\Big)V\Big(\frac{m+q^{\mu_1}s}{q^\mu}\Big)V\Big(\frac{m}{q^\mu}\Big)f_{\mu_2}((m+q^{\mu_1}s)(n+r))f_{\mu_2}(mn)\times\\ &\qquad\qquad \times\overline{f_{\mu_2}((m+q^{\mu_1}s)n)f_{\mu_2}(m(n+r))}\\ &= \sum_{n,m\in\mathcal{O}} V\Big(\frac{n}{q^\nu}\Big)V_s\Big(\frac{m}{q^\mu}\Big)f_{\mu_1,\mu_2}((m+q^{\mu_1}s)(n+r))f_{\mu_1,\mu_2}(mn)\times\\ &\qquad\qquad \times\overline{f_{\mu_1,\mu_2}((m+q^{\mu_1}s)n)f_{\mu_1,\mu_2}(m(n+r))}.\end{aligned}$$

Here we let $V_s(x) = V(x+sq^{\mu_1})V(x)$, and $f_{\mu_1,\mu_2} = f_{\mu_2}\overline{f_{\mu_1}}$. The part (3) of Lemma 16 allows to replace, in $S_{II,1}(r,s)$, each term $f_{\mu_1,\mu_2}(u)$ by $g(u) = f(q^{\mu_0}r_{\mu_0,\mu_2}(u))$. We deduce

$$S_{II,1}(r,s) = S_{II,2}(r,s) + O(\mu_2^{O(1)}Q^{\mu+\nu-2\eta_1\rho}), \tag{5.5}$$

where, abbreviating $u_0 = r_{\mu_0,\mu_2}(mn)$, $u_1 = r_{\mu_0,\mu_2}(mn+mr)$,

$$S_{II,2}(r,s) = \sum_{m\in\mathcal{O}} V_s\Big(\frac{m}{q^\mu}\Big)\sum_{n\in\mathcal{O}} V\Big(\frac{n}{q^\nu}\Big)g(u_1+q^{\mu_1-\mu_0}sn+q^{\mu_1-\mu_0}sr)\overline{g}(u_1)\overline{g}(u_0+q^{\mu_1-\mu_0}sn)g(u_0)$$

Let $\sigma = \mu_2 - \mu_0$. The definition of u_0 and u_1 is inserted as

$$S_{II,2}(r,s) = \sum_{m\in\mathcal{O}}\sum_{n\in\mathcal{O}}\sum_{u_0,u_1\in\mathcal{O}/q^\sigma} V_s\Big(\frac{m}{q^\mu}\Big)V\Big(\frac{n}{q^\nu}\Big)\psi_\sigma\Big(\frac{mn}{q^{\mu_2}}-\frac{u_0}{q^\sigma}\Big)\psi_\sigma\Big(\frac{mn+mr}{q^{\mu_2}}-\frac{u_1}{q^\sigma}\Big)\times$$
$$\times\, g(u_1+q^{\mu_1-\mu_0}sn+q^{\mu_1-\mu_0}sr)\overline{g}(u_1)\overline{g}(u_0+q^{\mu_1-\mu_0}sn)g(u_0).$$

Let $\tau\in\mathbb{N}$ be a parameter. We may proceed as in Lemma 2 of [MR15] to deduce

$$|S_{II,2}(r,s)| \le |S_4(r,s)| + E_4(r,0) + E_4(0,r) + E_4'(r), \tag{5.6}$$

where

$$S_4(r,s) = \sum_{m\in\mathcal{O}}\sum_{n\in\mathcal{O}}\sum_{u_0,u_1\in\mathcal{O}/q^\sigma} V_s\Big(\frac{m}{q^\mu}\Big)V\Big(\frac{n}{q^\nu}\Big)A_{\sigma,\tau}\Big(\frac{mn}{q^{\mu_2}}-\frac{u_0}{q^\sigma}\Big)A_{\sigma,\tau}\Big(\frac{mn+mr}{q^{\mu_2}}-\frac{u_1}{q^\sigma}\Big)\times$$
$$\times\, g(u_1+q^{\mu_1-\mu_0}sn+q^{\mu_1-\mu_0}sr)\overline{g}(u_1)\overline{g}(u_0+q^{\mu_1-\mu_0}sn)g(u_0),$$

$$E_4(r,r') = \sum_{m\in\mathcal{O}}\sum_{n\in\mathcal{O}}\sum_{u_0\in\mathcal{O}/q^\sigma} V_s\Big(\frac{m}{q^\mu}\Big)V\Big(\frac{n}{q^\nu}\Big)B_{\sigma,\tau}\Big(\frac{mn+mr}{q^{\mu_2}}-\frac{u_0}{q^\sigma}\Big)\sum_{u_1\in\mathcal{O}/q^\sigma}\psi_\sigma\Big(\frac{mn+mr'}{q^{\mu_2}}-\frac{u_1}{q^\sigma}\Big),$$

$$E_4'(r) = \sum_{m\in\mathcal{O}}\sum_{n\in\mathcal{O}}\sum_{u_0\in\mathcal{O}/q^\sigma} V_s\Big(\frac{m}{q^\mu}\Big)V\Big(\frac{n}{q^\nu}\Big)B_{\sigma,\tau}\Big(\frac{mn}{q^{\mu_2}}-\frac{u_0}{q^\sigma}\Big)\sum_{u_1\in\mathcal{O}/q^\sigma}B_{\sigma,\tau}\Big(\frac{mn+mr}{q^{\mu_2}}-\frac{u_1}{q^\sigma}\Big).$$

At this point, we are in a situation analogous to eq. (64) of [MR15].

5.3. **Bound on $E_4(r,r')$.** In $E_4(r,r')$, the u_1-sum evaluates to 1. Therefore,

$$E_4(r,r') = \sum_{m\in\mathcal{O}}\sum_{n\in\mathcal{O}} V_s\Big(\frac{m}{q^\mu}\Big)V\Big(\frac{n}{q^\nu}\Big)\sum_{u_0\in\mathcal{O}/q^\sigma}B_{\sigma,\tau}\Big(\frac{mn+mr}{q^{\mu_2}}-\frac{u}{q^\sigma}\Big).$$

By Lemme 9,

$$E_4(r,r') = \sum_{h\in\mathcal{O}^\vee} b_{\sigma,\tau}(h)\sum_{m\in\mathcal{O}}\sum_{n\in\mathcal{O}} V_s\Big(\frac{m}{q^\mu}\Big)V\Big(\frac{n}{q^\nu}\Big)\sum_{u_0\in\mathcal{O}/q^\sigma}\mathrm{e}_{\mu_2}(h(mn+mr))\mathrm{e}_\sigma(-hu_0)$$
$$= Q^\sigma\sum_{h\in\mathcal{O}^\vee} b_{\sigma,\tau}(hq^\sigma)\sum_{m\in\mathcal{O}}\sum_{n\in\mathcal{O}} V_s\Big(\frac{m}{q^\mu}\Big)V\Big(\frac{n}{q^\nu}\Big)\mathrm{e}_{\mu_0}(h(mn+mr))$$

by orthogonality. We apply Lemma 13 with $\mathfrak{t} = D_K$, using the fact that $V_s \ll V$, getting

$$E_4(r,r') \ll Q^{\mu+\nu+\sigma-\mu_0}\sum_{h\in\mathcal{O}^\vee}|b_{\sigma,\tau}(hq^\sigma)|N(hD_K+(q^{\mu_0}))$$
$$\ll Q^{\mu+\nu-\mu_0-\eta_2\tau}\sum_{h\in\mathcal{O}^\vee}\frac{N(hD_K+(q^{\mu_0}))}{(1+\|h/q^\tau\|)^{d+1}}.$$

Here we may apply Lemma 14 after changing h to $q^\tau h$, with $\mathfrak{t} = q^\tau D_K$. Along with partial summation, we obtain

$$E_4(r,r') \ll \mu^{O(1)}Q^{\mu+\nu}\Big\{Q^{-\eta_2\tau} + Q^{(1-\eta_2)\tau+2(\rho+\rho_1)-\mu}\Big\}. \tag{5.7}$$

5.4. **Bound on $E_4'(r)$.** Similarly as before, we use Lemma 9 to expand $B_{\sigma,\tau}$, and we execute the u_j-sums, which selects frequencies which are multiples of q^σ. We get

$$E_4'(r) = Q^{2\sigma} \sum_{h_0,h_1\in\mathcal{O}^\vee} b_{\sigma,\tau}(h_0q^\sigma)b_{\sigma,\tau}(h_1q^\sigma) \sum_{m\in\mathcal{O}}\sum_{n\in\mathcal{O}} V_s\Big(\frac{m}{q^\mu}\Big)V\Big(\frac{n}{q^\nu}\Big)\mathrm{e}_{\mu_0}(mn(h_0+h_1)+mrh_1).$$

The contribution of the diagonal contribution $h_0+h_1=0$ is bounded by

$$\ll Q^{2\sigma+\mu+\nu}\sum_{h\in\mathcal{O}^\vee}|b_{\sigma,\tau}(hq^\sigma)|^2 \ll Q^{\mu+\nu-\eta_2\tau}.$$

Therefore, using again $V_s \ll V$, it suffices to obtain a non-trivial bound for

$$T_4 := Q^{2\sigma} \sum_{\substack{h_0,h_1\in\mathcal{O}^\vee\\ h_0+h_1\neq 0}} |b_{\sigma,\tau}(h_0q^\sigma)b_{\sigma,\tau}(h_1q^\sigma)| \sum_{m\in\mathcal{O}} V\Big(\frac{m}{q^\mu}\Big)\Big| \sum_{n\in\mathcal{O}} V\Big(\frac{n}{q^\nu}\Big)\mathrm{e}_{\mu_0}(mn(h_0+h_1))\Big|.$$

The (m,n)-sums are bounded using Lemma 13 with $\mathfrak{t}=D_K$, which yields

$$\begin{aligned} T_4 &\ll Q^{\mu+\nu+2\sigma-\mu_0} \sum_{\substack{h_0,h_1\in\mathcal{O}^\vee\\ h_0+h_1\neq 0}} |b_{\sigma,\tau}(h_0q^\sigma)b_{\sigma,\tau}(h_1q^\sigma)| N((h_0+h_1)D_K+(q^{\mu_0})) \\ &\ll Q^{\mu+\nu-\mu_0} \sum_{\substack{h_0,h_1\in\mathcal{O}^\vee\\ h_0+h_1\neq 0}} \frac{N((h_0+h_1)D_K+(q^{\mu_0}))}{(1+\|h_0/q^\tau\|)^{2d+1}(1+\|h_1/q^\tau\|)^{d+1}} \\ &\ll \mu^{O(1)}Q^{\mu+\nu+2\tau-\mu_0} \end{aligned}$$

by Lemma 15 and partial summation. We conclude that

$$E_4'(r) \ll Q^{\mu+\nu}\Big\{Q^{-\eta_2\tau}+\mu^{O(1)}Q^{2\tau-\mu_0}\Big\}. \tag{5.8}$$

5.5. **Bound on S_4.** In $S_4(r,s)$, we expand $A_{\sigma,\tau}$ in Fourier series, and we sort according to the values of $u_3 = u_1 + q^{\mu_1-\mu_0}s(n+r) \pmod{q^\sigma}$ and $u_2 = u_0 + q^{\mu_1-\mu_0}sn \pmod{q^\sigma}$. We get

$$S_4(r,s) = Q^{-2\sigma} \sum_{\substack{\boldsymbol{h}=(h_0,h_1,h_2,h_3)\\ h_0,h_1\in\mathcal{O}^\vee\\ h_2,h_3\in\mathcal{O}^\vee/q^\sigma}} a_{\sigma,\tau}(h_0)a_{\sigma,\tau}(h_1)\mathrm{e}_{\mu_2-\mu_1}(h_3sr)U(\boldsymbol{h})W(\boldsymbol{h}), \tag{5.9}$$

where

$$\begin{aligned} U(\boldsymbol{h}) &:= \sum_{m,n\in\mathcal{O}} V_s\Big(\frac{m}{q^\mu}\Big)V\Big(\frac{n}{q^\nu}\Big)\mathrm{e}_{\mu_2}(mn(h_0+h_1)+mrh_1+q^{\mu_1}ns(h_2+h_3)), \\ W(\boldsymbol{h}) &:= \sum_{\substack{u_0,u_1,u_2,u_3\\ u_j\in\mathcal{O}/q^\sigma}} g(u_0)\overline{g}(u_1)\overline{g}(u_2)g(u_3)\mathrm{e}_\sigma(u_0(h_2-h_0)+u_1(h_3-h_1)-u_2h_2-u_3h_3). \end{aligned}$$

With the notation

$$\widehat{g}(h) := Q^{-\sigma}\sum_{u\in\mathcal{O}/q^\sigma} g(u)\mathrm{e}_\sigma(-uh), \tag{5.10}$$

we have $W(\boldsymbol{h}) = Q^{4\sigma}\widehat{g}(h_0-h_2)\overline{\widehat{g}}(h_3-h_1)\overline{\widehat{g}}(-h_2)\widehat{g}(h_3)$.

5.5.1. *Off-diagonal terms.* First we consider the contribution $S_4''(r,s)$ to the sum (5.9) of those indices which satisfy $h_0+h_1\neq 0$. By Lemma 13 with $q\leftarrow q^\mu$, $\alpha\leftarrow q^{-2\rho}(h_0+h_1)$ and $\mathfrak{t}\leftarrow(q^{2\rho_2})$, we obtain

$$U(\boldsymbol{h})\ll Q^{\nu+2\rho_2}N((h_0+h_1)D_K+(q^\mu)).$$

On the other hand, arguing as in p. 2621 of [MR15] by Cauchy-Schwarz and Parseval's identity, for all $h_0,h_1\in\mathcal{O}^\vee$ we have

$$\sum_{h_2,h_3\in\mathcal{O}^\vee/q^\sigma}|W(\boldsymbol{h})|\leq Q^{4\sigma}.$$

Therefore, we obtain

$$\begin{aligned}S_4''(r,s)&\ll Q^{\nu+2\sigma+2\rho_2}\sum_{\substack{h_0,h_1\in\mathcal{O}^\vee\\ h_0+h_1\neq 0}}|a_{\sigma,\tau}(h_0)a_{\sigma,\tau}(h_1)|N((h_0+h_1)D_K+(q^\mu))\\&\ll Q^{\nu+2\rho_2}\sum_{\substack{h_0,h_1\in\mathcal{O}^\vee\\ h_0+h_1\neq 0}}\frac{N((h_0+h_1)D_K+(q^\mu))}{((1+\|\frac{h_0}{q^{\sigma+\tau}}\|)(1+\|\frac{h_1}{q^{\sigma+\tau}}\|))^{2d+1}}\\&=Q^{\nu+2\rho_2}\sum_{\substack{h_0,h_1\in(q^{\sigma+\tau}D_K)^{-1}\\ h_0+h_1\neq 0}}\frac{N((h_0+h_1)q^{\sigma+\tau}D_K+(q^\mu))}{((1+\|h_0\|)(1+\|h_1\|))^{2d+1}}\\&\ll \mu^{O(1)}Q^{\nu+2\rho_2+2(\sigma+\tau)-\mu}\end{aligned}\tag{5.11}$$

by Lemma 13 with $\mathfrak{t}=q^{\sigma+\tau}D_K$ and partial summation.

5.5.2. *Diagonal terms.* Note that $A_{\sigma,\tau}(\xi)\in\mathbb{R}$, so that $a_{\sigma,\tau}(-\xi)=\overline{a_{\sigma,\tau}(\xi)}$. Let $S_4'(r,s)$ denote the contribution to $S_4(r,s)$ coming from indices $h_0+h_1=0$, so that

$$S_4(r,s)=S_4'(r,s)+S_4''(r,s).\tag{5.12}$$

We define

$$U_1(h;r,s):=\sum_{m\in\mathcal{O}}V_s\Big(\frac{m}{q^\mu}\Big)\mathrm{e}_{\mu_2}(-mrh),\quad U_2(h'):=\sum_{n\in\mathcal{O}}V\Big(\frac{n}{q^\nu}\Big)\mathrm{e}_{\mu_2-\mu_1}(nsh'),$$

so that

$$\begin{aligned}S_4'(r,s)=Q^{2\sigma}\sum_{\substack{h\in\mathcal{O}^\vee\\ h_2,h_3\in\mathcal{O}^\vee/q^\sigma}}&|a_{\sigma,\tau}(h)|^2\mathrm{e}_{\mu_2-\mu_1}(h_3sr)U_1(h;r,s)U_2(h_2+h_3)\times\\&\times\widehat{g}(h-h_2)\overline{\widehat{g}}(h_3+h)\overline{\widehat{g}}(-h_2)\widehat{g}(h_3)\end{aligned}$$

and consequently

$$\begin{aligned}|S_4'(r,s)|\leq Q^{2\sigma}\sum_{\substack{h\in\mathcal{O}^\vee\\ h'\in\mathcal{O}^\vee/q^\sigma}}&|a_{\sigma,\tau}(h)|^2|U_1(h;r,s)||U_2(h')|\times\\&\times\sum_{h_3\in\mathcal{O}^\vee/q^\sigma}|\widehat{g}(h-h'+h_3)\widehat{g}(h_3+h)\widehat{g}(-h'+h_3)\widehat{g}(h_3)|.\end{aligned}$$

Note that by Cauchy–Schwarz,

$$\sum_{h_3\in\mathcal{O}^\vee/q^\sigma}|\widehat{g}(h-h'+h_3)\widehat{g}(h_3+h)\widehat{g}(-h'+h_3)\widehat{g}(h_3)|\leq W(h),$$

where

$$W(h)=\sum_{h_3\in\mathcal{O}^\vee/q^\sigma}|\widehat{g}(h_3+h)\widehat{g}(h_3)|^2.$$

We note for further reference that, using $|\widehat{g}| \leq 1$ and Parseval's identity,

$$|W(h)| \leq 1. \tag{5.13}$$

Assume

$$\nu \geq \mu_2 - \mu_1 = 2(\rho_1 + \rho_2). \tag{5.14}$$

We have

$$\begin{aligned}\sum_{h' \in \mathcal{O}^\vee/q^\sigma} |U_2(h')| &\leq Q^\nu \sum_{h' \in \mathcal{O}^\vee/q^\sigma} \sum_{\xi \in \mathcal{O}^\vee} |\widehat{V}(q^{\nu-2(\rho_1+\rho_2)}(sh' + q^{2(\rho_1+\rho_2)}\xi))| \\ &= Q^{\nu+2\rho'} \sum_{\xi \in \mathcal{O}^\vee} |\widehat{V}(q^{\nu-2(\rho_1+\rho_2)}\xi)| \sum_{h' \in \mathcal{O}^\vee/q^{2(\rho_1+\rho_2)}} \mathbf{1}(sh' - \xi \in q^{2(\rho_1+\rho_2)}\mathcal{O}^\vee).\end{aligned}$$

By Lemma 6, the only ξ contributing to the sum is $\xi = 0$. We bound the h'-sum as in Lemma 12: the condition $sh' \in q^{2(\rho_1+\rho_2)}\mathcal{O}^\vee$ means $h' \in q^{2(\rho_1+\rho_2)}\mathfrak{d}^{-1}\mathcal{O}^\vee$, where $\mathfrak{d} = (s) + (q^{2(\rho_1+\rho_2)})$. Since $|q^{2(\rho_1+\rho_2)}\mathfrak{d}^{-1}\mathcal{O}^\vee/(q^{2(\rho_1+\rho_2)})| = |\mathcal{O}/\mathfrak{d}D_K| = N(\mathfrak{d}D_K) \ll N(\mathfrak{d})$, we find

$$\sum_{h' \in \mathcal{O}^\vee/q^\sigma} |U_2(h')| \leq Q^{\nu+2\rho'} N((s) + (q^{2(\rho_1+\rho_2)})),$$

and so

$$S_4'(r,s) \ll Q^{\nu+2\sigma+2\rho'} N((s) + (q^{2(\rho_1+\rho_2)})) \sum_{h \in \mathcal{O}^\vee} |a_{\sigma,\tau}(h)|^2 |U_1(h;r,s)| W(h),$$

where

We now execute the sum over $s \in \Delta^*_{2\rho_1}$. Define

$$U_1(h;r) = \sup_{s \in \Delta^*_{2\rho_1}} |U_1(h;r,s)|.$$

Then, with $C = 2R_{\mathcal{F}}^+$ (where we recall the definition (2.3)), we have

$$\begin{aligned}\frac{1}{Q^{2\rho_1}} \sum_{s \in \Delta^*_{2\rho_1}} N((s) + (q^{2(\rho_1+\rho_2)})) &\leq \frac{1}{Q^{2\rho_1}} \sum_{\mathfrak{d} | (q^{2(\rho_1+\rho_2)})} N(\mathfrak{d}) \operatorname{card}\left\{ s \in q^{-2\rho_1}\mathfrak{d}, 0 < \|s\| \leq C \right\} \\ &\ll \tau(q^{2(\rho_1+\rho_2)})\end{aligned}$$

by Lemma 11, and the last quantity is $O(\rho_1^{O(1)})$. We deduce

$$\frac{1}{Q^{2\rho_1}} \sum_{s \in \Delta^*_{2\rho_1}} |S_4'(r,s)| \ll \mu^{O(1)} Q^{\nu+2\sigma+2\rho'} \sum_{h \in \mathcal{O}^\vee} |a_{\sigma,\tau}(h)|^2 U_1(h;r) W(h).$$

Define $\tau = \rho_2(2 + \theta^{-1})$, $\tau' := \tau + \sigma + \lfloor \mu\varepsilon \rfloor$ for some parameter $\varepsilon \in (0,1]$ to be chosen later, and impose the condition

$$\Theta\tau' \leq \tfrac{1}{2}\theta\mu.$$

We will prove the three bounds

$$\sum_{\substack{h \in \mathcal{O}^\vee \\ \|h/q^{\tau'}\| > 1}} |a_{\sigma,\tau}(h)|^2 U_1(h;r) W(h) \ll_\varepsilon Q^{-10\mu}, \tag{5.15}$$

$$\frac{1}{Q^{\rho_2}} \sum_{r \in \Delta^*_{\rho_2}} U_1(h;r) \ll_A \mu^{O(1)} \Big(Q^{\mu - A\theta\rho_2} + Q^{-10\mu} \Big), \qquad \text{if } \|\tfrac{h}{q^{\tau'}}\| \leq 1, \|\tfrac{h}{q^\tau}\| > 1, \tag{5.16}$$

$$\sum_{\substack{h \in \mathcal{O}^\vee \\ \|h/q^\tau\| \leq 1}} W(h) \ll Q^{2\rho' - \eta''\gamma(\sigma-\tau)} + Q^{2\rho' - \eta_1\tau}. \tag{5.17}$$

Along with the bounds (5.13) and $|a_{\sigma,\tau}(h)| \ll Q^{-\sigma}$, this will yield

$$\begin{aligned}(5.18)\qquad &\frac{1}{Q^{\rho_1+2\rho_2}} \sum_{\substack{r\in\Delta^*_{\rho_2}\\ s\in\Delta^*_{2\rho_1}}} |S_4'(r,s)| \\ &\ll_A \mu^{O(A)} Q^{\mu+\nu+2\rho'} \Big\{ Q^{-10\mu} + Q^{\tau'-A\theta\rho_2} + Q^{2\rho'-\eta''\gamma(\sigma-\tau)} + Q^{2\rho'-\eta_1\tau} \Big\}.\end{aligned}$$

5.5.3. *Large h.* First, for $\|h/q^{\tau'}\| > 1$, we have

$$\|q^{-\sigma-\tau}h\| \gg \|h/q^{\tau'}\| Q^{\theta\mu\varepsilon}\mu^{1-d}$$

by Lemma 1 and our definition (2.8). By using Lemma 9, we have for any $A \geq 1$,

$$|a_{\sigma,\tau}(h)|^2 \ll_A \frac{1}{Q^{2\sigma+A\theta\mu\varepsilon}\|h/q^{\tau'}\|^A}.$$

We deduce, by (5.13),

$$\begin{aligned}\sum_{\substack{h\in\mathcal{O}^\vee\\ \|h/q^{\tau'}\|>1}} |a_{\sigma,\tau}(h)|^2 U_1(h;r)W(h) &\ll_A Q^{-2\sigma-A\theta\mu\varepsilon} \sum_{h\in q^{-\tau'}\mathcal{O}^\vee} (1+\|h\|)^{-d-1} \\ &\ll_\varepsilon Q^{-10\mu}\end{aligned}$$

by assuming $\rho \leq \mu$ and by picking A large enough in terms of ε. This proves (5.15).

5.5.4. *Middle-sized h.* Assume that $\|h/q^{\tau'}\| \leq 1$ and $\|h/q^{\tau}\| > 1$. For all $r \in \Delta^*_{\rho_2}$, we have

$$\Big\| \frac{rh}{q^{2\rho_2}} \Big\| \gg \|h/q^\tau\| \|q^{2\rho_2-\tau} r^{-1}\|^{-1}$$

by the triangle inequality, while

$$\|q^{2\rho_2-\tau}r^{-1}\| \ll \|q^{\rho_2-\tau}\| Q^{\rho_2} N(r)^{-1} \|r/q^{\rho_2}\|^{d-1} \ll \|q^{\rho_2-\tau}\| Q^{\rho_2} \ll \rho_2^{1-d} Q^{-\theta\rho_2},$$

by Lemma 1 and since $r \in \Delta_{\rho_2} \subset \mathcal{O}$. We conclude that for $h \in \mathcal{N}_{\tau'} \smallsetminus \mathcal{N}_\tau$, for all $r \in \Delta^*_{\rho_2}$, we have

$$\|q^{-2\rho_2} rh\| \gg \rho_2^{O(1)} Q^{\theta\rho_2}. \tag{5.19}$$

On the other hand, we have

$$\begin{aligned}\frac{1}{Q^{\rho_2}} \sum_{r\in\Delta^*_{\rho_2}} U_1(h;r) &= \frac{1}{Q^\rho} \sum_{r\in\Delta^*_{\rho_2}} \sup_{s\in\Delta^*_{2\rho_1}} \Big| \sum_{m\in\mathcal{O}} V_s\Big(\frac{m}{q^\mu}\Big) \mathrm{e}_{\mu_2}(mrh) \Big| \\ &= Q^{\mu-\rho} \sum_{r\in\Delta^*_{\rho_2}} \sup_{s\in\Delta^*_{2\rho_1}} \Big| \sum_{\xi\in\mathcal{O}^\vee} \widehat{V}_s\Big(q^\mu\xi + \frac{rh}{q^{2\rho_2}}\Big) \Big|.\end{aligned}$$

Here have $\|\frac{rh}{q^{2\rho_2}}\| \ll \|h\| \leq Q^{\Theta\tau'}$, while for $\xi \neq 0$, $\|q^\mu\xi\| \gg \mu^{O(1)} Q^{\theta\mu}$. Moreover, since $V_s(x) = V(x)V(x+q^{\mu_1-\mu}s)$, the derivatives of V_s are bounded uniformly in s, and so $\big|\widehat{V}_s(x)\big| \ll_A (1+\|x\|)^{-A}$ for all $x \in K$ and $A \geq 0$. Assuming

$$\Theta\tau' \leq \tfrac{1}{2}\theta\mu, \tag{5.20}$$

we obtain that for μ large enough, either $\xi = 0$ or

$$\Big\| q^\mu\xi + \frac{rh}{q^{2\rho_2}} \Big\| \geq \frac{\|q^\mu\xi\|}{2} \gg \mu^{O(1)} Q^{\theta\mu} \|\xi\|.$$

Summarizing the above, we conclude that for $\|h/q^{\tau'}\| \leq 1$ and $\|h/q^{\tau}\| > 1$,

$$\frac{1}{Q^{\rho_2}} \sum_{r \in \Delta_{\rho_2}} U_1(h;r) \ll_A Q^{\mu} \mu^{O(A)} \Big(Q^{-A\theta\rho_2} + Q^{-A\theta\mu} \Big).$$

for any fixed $A \geq 0$. This yields (5.16).

5.5.5. *Small h.* Finally, we focus on the case $\|h/q^{\tau}\| \leq 1$. In this range, we use the estimate $|a_{\gamma,\tau}(h)| \ll Q^{-\sigma}$ from Lemma 9, and the trivial bound $U_1(h;r) \ll Q^{\mu}$. We get

$$\sum_{\substack{h \in \mathcal{O}^\vee \\ h \in \mathcal{N}_\tau}} |a_{\sigma,\tau}(h)|^2 U_1(h;r) W(h) \ll Q^{\mu - 2\sigma} \sum_{\substack{h \in \mathcal{O}^\vee \\ \|h/q^{\tau}\| \leq 1}} W(h).$$

Assuming that

$$\mu_0 \leq c(\sigma - \tau),$$

Lemma 1 applies, and yields

$$\sum_{\substack{h \in \mathcal{O}^\vee \\ \|h/q^{\tau}\| \leq 1}} W(h) \ll Q^{2\rho'} \Big(Q^{-\eta''\gamma(\sigma-\tau)} + Q^{-\eta_1 \tau} \Big) \sum_{h_3 \in \mathcal{O}^\vee / q^{\rho_3}} \left| \widehat{g}(h_3) \right|^2.$$

The sum over h_3 evaluates to 1 by Parseval's identity, and we obtain (5.17).

5.6. **Optimization.** Grouping successively the bounds (5.11), (5.12), (5.18), and (5.4)–(5.8) yields

$$S_{II} = \sum_{m \in \mathcal{N}_\mu} \sum_{n \in \mathcal{N}_\nu} \alpha_m \beta_n f(mn) \ll_\varepsilon \mu^{O(1)} \|\alpha\|_2 \|\beta\|_4 Q^{\mu/2 + 3\nu/4 - \delta/4},$$

where

$$\delta = \min \Big\{ \eta_1\rho_2, 2\eta_1\rho', \eta_2\tau, \mu - 2(\tau + \rho' + \rho_1), \eta''\gamma(\sigma - \tau) - 4\rho', \eta_1\tau - 4\rho' \Big\},$$

with $\tau = (2 + \theta^{-1})\rho_2$ and $\tau' = \tau + 2(\rho' + \rho_1 + \rho_2) + \lfloor \mu\varepsilon \rfloor$, under the conditions:

$$\rho_2 \leq \rho_1 \leq \mu, \quad 2(\rho' + \rho_1 + \rho_2) \leq \mu, \quad \mu + c\theta^{-1}\rho_2 \leq 2(c+1)\rho' + (2c+1)\rho_1, \quad \Theta\tau' \leq \tfrac{1}{2}\theta\mu.$$

Let $K = 20\Theta\theta^{-1}$, so that by hypothesis $c \geq K$. Then with the choice

$$\rho_1 = \frac{\mu}{K} + O(1), \quad \rho' = \frac{\eta''}{8}\gamma\Big(\Big\lfloor \frac{\mu}{K} \Big\rfloor \Big) + O(1), \quad \rho_2 = \frac{\theta\mu}{K} + O(1),$$

the claimed result follows.

6. Sums over prime elements: proof of Theorem 3

In this section we assume that $\mathcal{O}$ is principal. Our goal is to use Propositions 2 and 3 to estimate mean values over prime elements of $\mathcal{O}$, and prove Theorem 3.

6.1. **Combinatorial identity.** In this section we express the characteristic function of prime elements into convolutions for which Propositions 2 and 3 apply. The methods that have been developed to perform this step has a long history, since Vinogradov's work [Vin37]. We refer to [Ram13] for an account and references. In [MR10, MR15], this rôle is played by the combinatorial identity of Vaughan [Vau80]; see [Hin88] for a number field analogue.

One advantage of Vaughan's identity as it is cast in [MR10] is the absence of divisor functions in the upper-bound. One inconvenient, as with all methods which pass through the van Mangoldt function, is the necessity to use partial summation to detect the size of $\log N(n)$. Here we take the opportunity to proceed along a slightly different argument (see [DT18, Theorem 3.3]), with the benefit that we avoid completely partial summation.

For a non-zero ideal $\mathfrak{n} \subset \mathcal{O}$, let

$$P^+(\mathfrak{n}) = \max_{\mathfrak{p}|\mathfrak{n}} N(\mathfrak{p}), \qquad P^-(\mathfrak{n}) = \min_{\mathfrak{p}|\mathfrak{n}} N(\mathfrak{p}),$$

where $\mathfrak{p}$ denotes a prime ideal, and by convention $P^+((1)) = 1$ and $P^-((1)) = +\infty$.

Lemma 17. *Let $X \geq 2$, and $(g(\mathfrak{n}))_{\mathfrak{n}\neq 0}$ be complex numbers with $g(\mathfrak{n}) = 0$ if $N(\mathfrak{n}) > X$. Then*

$$\Big|\sum_{\mathfrak{p}} g(\mathfrak{p})\Big| \ll \|g\|_\infty X^{\frac{1}{2}} + \sum_{N(\mathfrak{m})\leq X^{\frac{1}{4}}} \Big|\sum_{\mathfrak{n}} g(\mathfrak{m}\mathfrak{n})\Big| + (\log X) \sup_{(\alpha,\beta)} \Big| \sum_{X^{\frac{1}{4}}<N(\mathfrak{m})\leq X^{\frac{3}{4}}} \sum_{\mathfrak{m}} \sum_{\mathfrak{n}} \alpha_{\mathfrak{m}}\beta_{\mathfrak{n}} g(\mathfrak{m}\mathfrak{n})\Big|,$$

where the supremum is over all sequences $(\alpha_{\mathfrak{m}}), (\beta_{\mathfrak{n}})$ satisfying $|\alpha_{\mathfrak{m}}| \leq 1$ and $|\beta_{\mathfrak{n}}| \leq \tau(\mathfrak{n})$.

Proof. Discarding those prime ideals of norm at most $X^{\frac{1}{2}}$, the sum we wish to evaluate is

$$O(\|g\|_\infty X^{\frac{1}{2}}) + \sum_{\substack{\mathfrak{n} \\ P^-(\mathfrak{n})>X^{\frac{1}{2}}}} g(\mathfrak{n}).$$

The condition is detected by Möbius inversion,

$$\sum_{\substack{\mathfrak{n} \\ P^-(\mathfrak{n})>X^{\frac{1}{2}}}} g(\mathfrak{n}) = \sum_{P^+(\mathfrak{m})\leq X^{\frac{1}{2}}} \mu(\mathfrak{m}) \sum_{\mathfrak{n}} g(\mathfrak{m}\mathfrak{n}).$$

The contribution of those $\mathfrak{m}$ with $N(\mathfrak{m}) \leq X^{\frac{1}{4}}$ yields the first term. Suppose that $N(\mathfrak{m}) > X^{\frac{1}{4}}$ and $\mathfrak{m}$ squarefree. Let $\prec$ be any ordering of the prime ideals which respects the norm, *i.e.* $N(\mathfrak{p}_1) < N(\mathfrak{p}_2)$ implies $\mathfrak{p}_1 \prec \mathfrak{p}_2$. Enumerating the prime ideals with respect to this ordering induces a bijection $\phi : \{\mathfrak{p} \text{ prime}\} \to \mathbb{N}_{>0}$, satisfying $\phi(\mathfrak{p}) \ll N(\mathfrak{p})$. Let $\mathfrak{p}^+(\mathfrak{n})$ (resp. $\mathfrak{p}^-(\mathfrak{n})$) denote the maximal (resp. minimal) prime divisor of $\mathfrak{n} \neq (1)$ with respect to ϕ. Write

$$\mathfrak{m} = \mathfrak{p}_1 \cdots \mathfrak{p}_k,$$

where $\phi(\mathfrak{p}_j) < \phi(\mathfrak{p}_{j+1})$. Then there is a minimal index $j_{\mathfrak{m}}$ for which, letting $\mathfrak{m}_1 = \mathfrak{p}_1 \cdots \mathfrak{p}_{j_{\mathfrak{m}}}$, we have $N(\mathfrak{m}_1) > X^{\frac{1}{4}}$. The ideal $\mathfrak{m}_1$ is characterized by the conditions

$$\mathfrak{m}_1 \mid \mathfrak{m}, \quad X^{\frac{1}{4}} < \mathfrak{m}_1 \leq X^{\frac{1}{4}} P^+(\mathfrak{m}_1), \quad \phi(\mathfrak{p}^+(\mathfrak{m}_1)) < \phi(\mathfrak{p}^-(\mathfrak{m}/\mathfrak{m}_1)).$$

We deduce

$$\sum_{\substack{N(\mathfrak{m})>X^{\frac{1}{4}} \\ P^+(\mathfrak{m})\leq X^{\frac{1}{2}}}} \mu(\mathfrak{m}) \sum_{\mathfrak{n}} g(\mathfrak{m}\mathfrak{n}) = \sum_{\substack{X^{\frac{1}{4}}<N(\mathfrak{m}_1)\leq X^{\frac{1}{4}}P^+(\mathfrak{m}_1) \\ P^+(\mathfrak{m}_2)\leq X^{\frac{1}{2}} \\ \phi(\mathfrak{p}^+(\mathfrak{m}_1))<\phi(\mathfrak{p}^-(\mathfrak{m}_2))}} \sum_{\mathfrak{n}} \mu(\mathfrak{m}_1)\mu(\mathfrak{m}_2) g(\mathfrak{m}_1\mathfrak{m}_2\mathfrak{n}).$$

The condition $\phi(\mathfrak{p}^+(\mathfrak{m}_1)) < \phi(\mathfrak{p}^-(\mathfrak{m}_2))$ is detected by means of Lemma 13.11 of [IK04], so that setting

$$\alpha_{\mathfrak{m}}(t) = \phi(\mathfrak{p}^+(\mathfrak{m}))^{it}\mu(\mathfrak{m}),$$
$$\beta_{\mathfrak{n}}(t) = \sum_{\substack{\mathfrak{d}|\mathfrak{n},\mathfrak{d}\neq(1) \\ P^+(\mathfrak{d})\leq X^{\frac{1}{2}}}} \phi(\mathfrak{p}^-(\mathfrak{d}))^{-it}\mu(\mathfrak{d}),$$

we have

$$\Big|\sum_{\substack{X^{\frac{1}{4}}<N(\mathfrak{m}) \\ P^+(\mathfrak{m})\leq X^{\frac{1}{2}}}} \mu(\mathfrak{m}) \sum_{\mathfrak{n}} g(\mathfrak{m}\mathfrak{n})\Big| \ll (\log X) \sup_{t\in\mathbb{R}} \Big| \sum_{\substack{\mathfrak{m} \\ P^+(\mathfrak{m})\leq X^{\frac{1}{2}} \\ X^{\frac{1}{4}}<N(\mathfrak{m})\leq X^{\frac{1}{4}}P^+(\mathfrak{m})}} \sum_{\mathfrak{n}} \alpha_{\mathfrak{m}}(t)\beta_{\mathfrak{n}}(t) g(\mathfrak{m}\mathfrak{n})\Big|,$$

as claimed. □

6.2. **Quotient by units.** When translating sums over ideals (coming from the combinatorial identities) to sums over $\mathcal{O}$, we will use the following partition of unity, inspired from [Tót00, Lemma 4.2], to account for the quotient by units.

Lemma 18. *There exists a smooth function $\Phi_0 : P(\mathbb{R}^d) \to [0,1]$ such that, letting $\Phi = \Phi_0 \circ \iota^{-1}$, we have*

$$\sum_{\varepsilon \in \mathcal{O}^*} \Phi(n\varepsilon) = 1 \qquad (n \in \mathcal{O} \smallsetminus \{0\}), \tag{6.1}$$

and for any given n, there are only finitely many non-zero terms in the sum. Moreover, for all $x \in K^*$ with $\Phi(x) \neq 0$, and all $\pi \in G_K$, we have $|x^\pi| \asymp N(x)^{1/d}$ with an implied constant depending only on K.

In particular, if $\mathcal{O}$ is principal, then for any function $g : \{\mathfrak{n} \neq 0\} \to \mathbb{C}$ of finite support and any $\varepsilon \in \mathcal{O}^*$, we have

$$\sum_{\mathfrak{n} \neq 0} g(\mathfrak{n}) = \sum_{n \in \mathcal{O} \smallsetminus \{0\}} \Phi(n\varepsilon) g((n)). \tag{6.2}$$

Proof. Let r be the rank of the free part of $\mathcal{O}^*$, and $\varepsilon_1, \dots, \varepsilon_r$ be any fixed basis [Neu99, Theorem I.7.3], so

$$\mathcal{O}^* = \{\omega \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}, \omega \in \Omega, n_j \in \mathbb{Z}\}$$

where Ω are the roots of unity in $\mathcal{O}$. As in [MV07, p.55], we let $\Psi : \mathbb{R}^d \to \mathbb{R}^r$ be the map defined by $\Psi(x) = (\psi_1(x), \dots, \psi_r(x))$, where

$$\log(|\iota(x)^\pi / N(\iota(x))|) = \sum_{j=1}^{r} \psi_j(x) \log \left|\varepsilon_j^\pi\right|$$

for all $\pi \in G_K$. Then for $\lambda \in \mathbb{R}^*$ and $1 \leq j \leq r$, ψ_j is smooth and $\psi_j(\lambda x) = \psi_j(x)$. Let a smooth function $w : \mathbb{R} \to [0,1]$ with $\operatorname{supp} w \subset [-1,1]$ be a partition of unity as

$$\sum_{n \in \mathbb{Z}} w(x+n) = 1 \qquad (x \in \mathbb{R}), \tag{6.3}$$

and define, for all $x \in K^*$, $\Phi(x) := w(\psi_1(x)) \cdots w(\psi_r(x))$. Then the function Φ is smooth, well-defined on $P(\mathbb{R}^d)$, and the property (6.1) follows by r applications of (6.3).

To prove (6.2), let $\mathfrak{n} = (n_0) \neq 0$ be an integral ideal, with $n_0 \in \mathcal{O}$. Then

$$\sum_{\substack{n \in \mathcal{O} \\ (n) = \mathfrak{n}}} \Phi(n\varepsilon) = \sum_{\varepsilon' \in \mathcal{O}^*} \Phi(n_0 \varepsilon \varepsilon') = 1$$

by (6.1). □

6.3. **Proof of Theorem 3.**

6.3.1. *Preparations.* We borrow the notation χ_τ from Lemma 9 (see (3.6)). Let $W : \mathbb{R}_+ \to \mathbb{R}_+$ be a smooth function defining a partition of unity along powers of Q in the sense that for all $x \geq 0$,

$$W(x) \leq \mathbf{1}_{[1/(2Q),1]}(x), \qquad \sum_{k \in \mathbb{Z}} W(Q^{-k}x) = 1.$$

For all $\kappa \in \mathbb{N}$, let

$$g_\lambda(\mathfrak{n}) = \sum_{\substack{n \in \mathcal{N}_\lambda \\ (n) = \mathfrak{n}}} f(n), \qquad S_\lambda(\kappa) = \sum_{\mathfrak{p}} W\Big(\frac{N(\mathfrak{p})}{Q^\kappa}\Big) g_\lambda(\mathfrak{p}).$$

Note that by Lemma 2, we have

$$|g_\lambda(\mathfrak{n})| \ll \lambda^{d-1}. \tag{6.4}$$

Next we smooth out the condition $n \in \mathcal{N}_\lambda$ as in Lemma 9. Let $\tau \in \mathbb{N}$ be a parameter, and for all $X \geq 1$,

$$g_{\lambda,\tau}(\mathfrak{n}) = \sum_{\substack{n\in\mathcal{O}\\(n)=\mathfrak{n}}} \chi_\tau \circ \iota^{-1}\Big(\frac{n}{q^\lambda}\Big) f(n), \qquad S_{\lambda,\tau}(\kappa) = \sum_{\mathfrak{p}} W\Big(\frac{N(\mathfrak{p})}{Q^\kappa}\Big) g_{\lambda,\tau}(\mathfrak{p}).$$

The function g_λ also satisfies the trivial bound (6.4), so that

$$S_{\lambda,\tau}(\kappa) \ll \lambda^{d-1} Q^\kappa.$$

Borrowing temporarily the notations ϕ_τ and V_2 from Lemma 9, we have

$$\begin{aligned} |S_\lambda(\kappa) - S_{\lambda,\tau}(\kappa)| &\leq \sum_{n\in\mathcal{O}} (\mathbf{1}_{V_2} * \phi_\tau)\Big(\iota^{-1}\Big(\frac{n}{q^\lambda}\Big)\Big) \\ &\ll Q^{\lambda-\eta_2\tau} \end{aligned}$$

by Poisson summation, the bound (3.7) and Lemma 11. Finally, let $\kappa_0 \in [\lambda/2, \lambda] \cap \mathbb{N}$. We use the trivial bound for $\kappa \leq \kappa_0$. Since $g(\mathfrak{n}) \neq 0$ implies $1 \leq N(\mathfrak{n}) \ll Q^\lambda$, we deduce

$$\sum_{\substack{n\in\mathcal{N}_\lambda\\ n \text{ prime}}} f(n) \ll \lambda Q^{\lambda-\eta_2\tau} + \lambda^d Q^{\kappa_0} + \lambda \sup_{\kappa_0\leq\kappa\leq\lambda+C} |S_{\lambda,\tau}(\kappa)|,$$

for some C depending on $(q, \mathcal{D})$ at most. Using Lemma 17, we find

$$\sum_{\substack{n\in\mathcal{N}_\lambda\\ n \text{ prime}}} f(n) \ll \lambda Q^{\lambda-\eta_2\tau} + \lambda^d Q^{\kappa_0} + \lambda \sup_{\kappa_0\leq\kappa\leq\lambda+C} \Big(\Big|S^I_{\lambda,\tau}(\kappa)\Big| + \sup_{\alpha,\beta} \Big|S^{II,\alpha,\beta}_{\lambda,\tau}(\kappa)\Big| \Big), \tag{6.5}$$

where

$$S^I_{\lambda,\tau}(\kappa) = \sum_{N(\mathfrak{m})\leq Q^{\kappa/4}} \Big| \sum_{\mathfrak{n}} W\Big(\frac{N(\mathfrak{mn})}{Q^\kappa}\Big) g_{\lambda,\tau}(\mathfrak{mn})\Big| \tag{6.6}$$

$$S^{II,\alpha,\beta}_{\lambda,\tau}(\kappa) = \sum_{Q^{\kappa/4}<N(\mathfrak{m})\leq Q^{3\kappa/4}} \sum_{\mathfrak{m}} \sum_{\mathfrak{n}} \alpha_{\mathfrak{m}}\beta_{\mathfrak{n}} W\Big(\frac{N(\mathfrak{mn})}{Q^\kappa}\Big) g_{\lambda,\tau}(\mathfrak{mn}) \tag{6.7}$$

Before we proceed we require the following estimate. Define functions on $\mathbb{R}^d$, resp. K, by

$$V_0(x) = W(Q^{\lambda-\kappa} N(\iota(x)))\chi_\tau(x), \qquad V = V_0 \circ \iota^{-1}.$$

Lemma 19. *We have*

$$\sum_{\xi\in\mathbb{Z}^d} \Big|\widehat{V}_0(\xi)\Big| + \int_{\mathbb{R}^d} \Big|\widehat{V}_0(\xi)\Big| \,\mathrm{d}\xi \ll Q^{\tau+\lambda-\kappa},$$

with an implied constant depending only on $(q, \mathcal{D})$.

Proof. We introduce a smooth, compactly supported function W_0, majorizing the indicator function of the support of χ_0, and redundant in the sense that $\chi_\tau = \chi_\tau W_0$. We then have, for all $\xi \in \mathbb{R}^d$,

$$\widehat{V}(\xi) = \int_{\mathbb{R}^d} \widehat{\chi}_\tau(\xi')\widehat{W}_1(\xi - \xi')\mathrm{d}\xi',$$

with $W_1(x) = W(N \circ \iota(q^{\lambda-\kappa}x))W_0(x)$. By (3.6) and (3.8), we have

$$|\widehat{\chi}_\tau(\xi)| \ll_A (1 + \|q^{-\tau}\xi\|)^{-A} \tag{6.8}$$

for all $A \geq 0$. On the other hand, we have

$$\widehat{W}_1(\xi) = Q^{\kappa-\lambda} \int_{\mathbb{R}^d} W(N \circ \iota(x)) W_0(q^{\kappa-\lambda}x) \mathrm{e}(\big\langle x, \widetilde{q}^{\kappa-\lambda}\xi \big\rangle) \mathrm{d}x.$$

By partial differentiation, since $\|\widetilde{q}^{\kappa-\lambda}\| \ll 1$, we obtain for all $A \geq 0$

$$\Big|\widehat{W}_1(\xi)\Big| \ll_A (1 + \|\widetilde{q}^{\kappa-\lambda}\xi\|)^{-A}. \tag{6.9}$$

The bound for $\int_{\mathbb{R}^d} \Big|\widehat{V}_0(\xi)\Big| \mathrm{d}\xi$ immediately follows by multiplying the integrals of (6.8) and (6.9) with respect to ξ. The bound for $\sum_{\xi\in\mathbb{Z}^d} \Big|\widehat{V}_0(\xi)\Big|$ follows by the upper bound

$$\sum_{\xi\in\mathbb{Z}^d} (1 + \|\widetilde{q}^{-\tau}(\xi + \xi_0)\|)^{-d-1} \ll Q^{\tau},$$

valid for all $\xi_0 \in \mathbb{R}^d$: indeed, by translating we may ensure that $\widetilde{q}^{-\tau}\xi_0 \in \mathscr{F}$, and the resulting sum is estimated by Lemma 11.

□

6.3.2. *Type I sums.* For each $\mathfrak{m}$ in the sum (6.6), we have

$$\sum_{\mathfrak{n}} W\Big(\frac{N(\mathfrak{mn})}{Q^\kappa}\Big) g_{\lambda,\tau}(\mathfrak{mn}) = \sum_{\substack{n\in\mathcal{O}\\ \mathfrak{m}|(n)}} V\Big(\frac{n}{q^\lambda}\Big) f(n).$$

Using Lemma 18 on the $\mathfrak{m}$-sum, we deduce, for any $\varepsilon \in \mathcal{O}^*$,

$$S^I_{\lambda,\tau}(\kappa) = \sum_{\substack{m\in\mathcal{O}\\ 0<N(m)\leq Q^{\kappa/4}}} \Phi(m\varepsilon) \Big| \sum_{n\in\mathcal{O}} V\Big(\frac{mn}{q^\lambda}\Big) f(mn)\Big|. \tag{6.10}$$

Let $\mu \geq \lfloor \kappa/4 \rfloor + 1$. We pick ε so that $|(q^\mu\varepsilon)^\pi| \asymp Q^{\mu/d}$. This ensures that for any m in the sum, we have $|m/q^\mu| \ll 1$, so that for some choice $\mu = \kappa/4 + O(1)$, we have $m \in \mathcal{N}_\mu$. We deduce

$$S^I_{\lambda,\tau}(\kappa) \leq \sum_{m\in\mathcal{N}_\mu} \Big| \sum_{n\in\mathcal{O}} V\Big(\frac{mn}{q^\lambda}\Big) f(mn)\Big|.$$

Note that $\mathrm{supp}(V) \subset \mathrm{supp}\,\chi_0$, which depends only on $(q, \mathcal{D})$. Apply Proposition 2 along with Lemma 19 yields

$$S^I_{\lambda,\tau}(\kappa) \ll \lambda^{d+1} Q^{\lambda - \frac{\eta_1}{1+\eta_1}\gamma(\lambda/3)+\tau+\lambda-\kappa}. \tag{6.11}$$

6.3.3. *Type II sums.* Splitting the interval $[Q^{\kappa/4}, Q^{3\kappa/4}]$, we have

$$\sup_{(\alpha,\beta)} \Big|S^{II,\alpha,\beta}_{\lambda,\tau}(\kappa)\Big| \leq \kappa \sup_{\substack{\mu\in\mathbb{N}\\ \frac{\kappa}{4}\leq\mu\leq\frac{3\kappa}{4}}} \sup_{(\alpha,\beta)} \Big| \sum_{\substack{\mathfrak{m}\\ Q^\mu<N(\mathfrak{m})\leq Q^{\mu+1}}} \sum_{\mathfrak{n}} \alpha_{\mathfrak{m}}\beta_{\mathfrak{n}} W\Big(\frac{N(\mathfrak{mn})}{Q^\kappa}\Big) g_{\lambda,\tau}(\mathfrak{mn})\Big|.$$

Let μ, α, β satisfy the conditions in the suprema. By arguing as in (6.10), we have

$$\sum_{\substack{\mathfrak{m}\\ Q^\mu<N(\mathfrak{m})\leq Q^{\mu+1}}} \sum_{\mathfrak{n}} \alpha_{\mathfrak{m}}\beta_{\mathfrak{n}} W\Big(\frac{N(\mathfrak{mn})}{Q^\kappa}\Big) g_{\lambda,\tau}(\mathfrak{mn}) = \sum_{\substack{m,n\in\mathcal{O}\\ Q^\mu<N(m)\leq Q^{\mu+1}}} \alpha_m \Phi(m\varepsilon)\beta_n V\Big(\frac{mn}{q^\lambda}\Big) f(mn)$$

for all $\varepsilon \in \mathcal{O}^*$. Here we abbreviated $\alpha_m := \alpha_{(m)}$ and $\beta_n := \beta_{(n)}$. We pick ε so that $|(m/q^\mu)^\pi| \asymp 1$. Since also $\|mn/q^\lambda\| \ll 1$ by the support of V, we deduce that

for some $\mu' = \mu + O(1)$ and ν with $\mu' + \nu = \lambda + O(1)$, we have $m \in \mathcal{N}_{\mu'}$ and $n \in \mathcal{N}_\nu$. Writing, for all $x \in K$,

$$V(x) = \int_{\mathbb{R}^d} \widehat{V}_0(\xi) \mathrm{e}(\langle \xi, \iota^{-1}(x) \rangle) \mathrm{d}\xi,$$

we apply Proposition 3, exchanging the roles of μ and ν if $\mu' > \nu$, and setting $\psi(x) = \langle \xi, \iota^{-1}(x/q^\lambda) \rangle$. By Lemma 19, and the divisor-bound

$$\sum_{n \in \mathcal{N}_\nu} \tau((n))^4 \ll \sum_{N(\mathfrak{n}) \ll Q^\nu} \tau(\mathfrak{n})^4 \sum_{\substack{n \in \mathfrak{n} \\ \|n/q^\nu\| \ll 1}} 1 \ll \nu^{O(1)} Q^\nu,$$

we deduce

$$\Big| \sum_{\substack{m,n \in \mathcal{O} \\ Q^\mu < N(m) \leq Q^{\mu+1}}} \alpha_m \Phi(m\varepsilon) \beta_n V\Big(\frac{mn}{q^\lambda}\Big) f(mn) \Big| \ll \lambda^{O(1)} Q^{\lambda - \delta\gamma(\lfloor \frac{\theta\lambda}{100\Theta} \rfloor) + \tau + \lambda - \kappa},$$

where $\delta \gg \min\{\eta_1^2 \eta_2, \eta_1 \theta\}$. We conclude that

$$\sup_{(\alpha,\beta)} \big| S^{II,\alpha,\beta}_{\lambda,\tau}(\kappa) \big| \ll \lambda^{O(1)} Q^{\lambda - \delta\gamma(\lfloor \frac{\theta\lambda}{100\Theta} \rfloor) + \tau + \lambda - \kappa} \tag{6.12}$$

6.3.4. *Conclusion.* The claimed bound follows upon grouping the estimates (6.5), (6.11) and (6.12), and optimizing τ and κ_0 by

$$\lambda - \kappa_0 = \frac{\delta}{2 + \eta_2^{-1}} \gamma\Big(\Big\lfloor \frac{\theta\lambda}{100\Theta} \Big\rfloor\Big) + O(1), \quad \tau = \eta_2^{-1}(\lambda - \kappa_0) + O(1).$$

7. Two arithmetic applications : sums of digits and Rudin-Shapiro sequences

In this section we prove Theorems 1 and 2. In view of Theorem 3, it will suffice to prove that the functions $s_{q,\mathcal{D}}(n)$ and $r_{q,\mathcal{D}}(n)$ defined in (1.1)–(1.3) satisfy the Carry and Fourier properties (2.5)–(2.6).

7.1. **Sums of digits in $\mathcal{O}$.** We let $\sum_{j=0}^d c_j X^j$ be the minimal polynomial of q (with $c_d = 1$), and also

$$\mu_q = \sum_{j=0}^d c_j \in \mathbb{Z}, \qquad M_q := \sum_{j=0}^d |c_j|^2 .$$

Lemma 20. *Let $\alpha \in K$. The function given by $f(n) = \mathrm{e}(\langle \alpha s_{q,\mathcal{D}}(n) \rangle)$ satisfies the Carry property* (2.5) *with $\eta_1 = \eta_2$, and the Fourier property* (2.6) *with a function γ satisfying, for some $\delta_Q > 0$ depending on Q only,*

$$\gamma(\lambda) \geq C_{q,\mathcal{D},\alpha} \lambda + O(1), \qquad C_{q,\mathcal{D},\alpha} = \frac{\delta_Q}{M_q(d+1)} \sum_{b \in \mathcal{D}} \|\langle \mu_q \alpha b \rangle\|^2_{\mathbb{R}/\mathbb{Z}}. \tag{7.1}$$

Proof. We consider first the Carry property. If (2.5) holds, then there is a carry propagation in the sum $m + n$, where $m = u_1 + vq^\kappa$ and $n = u_2$. Then, in the notations of Lemma 8, the exists some $b \in \mathcal{B}_{st}$ such that in the addition $v + b$, the carry propagates beyond the ρ-th digit. By Lemma 8 and finiteness of $\mathcal{B}_{st}$, there are at most $O(2^{\lambda - \eta_2 \rho})$ possibilities for v.

To establish the Fourier property, we argue as in Lemme 20 of [MR10], and Lemma 6.3 of [DRS08]. We let

$$\phi(t) := \left| \sum_{b \in \mathcal{D}} \mathrm{e}(\langle (\alpha + t)b \rangle) \right|.$$

Using that $0 \in \mathcal{D}$ and Taylor expansion near the origin, we obtain the existence of $\varpi_Q > 0$, depending only on Q, such that

$$\left| \sum_{b \in \mathcal{D}} \mathrm{e}(\theta_b) \right| \leq Q^{1-\varpi_Q \sum_{b \in \mathcal{D}} \|\theta_b\|^2}$$

for all tuples of real numbers $(\theta_b)_{b \in \mathcal{D}}$ with $\theta_0 = 0$. We deduce, for any fixed $t \in K$,

$$\left| \phi(t)\phi(tq) \cdots \phi(tq^d) \right| \leq Q^{d+1-\varpi_Q \sum_{b \in \mathcal{D}} \sum_{j=0}^{d} \| \left\langle (\alpha + tq^d)b \right\rangle \|^2} \tag{7.2}$$

On the other hand, by the triangle and the Cauchy–Schwarz inequalities,

$$\begin{aligned} \| \langle \mu_q \alpha b \rangle \|_{\mathbb{R}/\mathbb{Z}}^2 &\leq \Big(\sum_{j=0}^{d} |c_j| \, \| \left\langle (\alpha + tq^j)b \right\rangle \|_{\mathbb{R}/\mathbb{Z}} \Big)^2 \\ &\leq M_q \sum_{j=0}^{d} \| \left\langle (\alpha + tq^j)b \right\rangle \|_{\mathbb{R}/\mathbb{Z}}^2. \end{aligned}$$

Summing this inequality over b and inserting in (7.2) yields

$$\sup_{t \in K} |\phi(t)\phi(tq) \cdots \phi(tq^n)| \leq Q^{(n+1)(1-C_{q,\mathcal{D},\alpha})},$$

where $C_{q,\mathcal{D},\alpha}$ is given in (7.1) with $\delta_Q = Q\varpi_Q$. From here, reasonning as in Lemme 20 of [MR10] concludes the proof. □

Proof of Theorem 1. Let $h \in \mathbb{Z}_{\neq 0}$. For some $\alpha \in K$ and all $x \in K$, we have $\phi(x) = \langle \alpha x \rangle$. If $\phi(b) \notin \mathbb{Q}$ for some $b \in \mathcal{D}$, then $\|h\langle \mu_q \alpha b \rangle\|_{\mathbb{R}/\mathbb{Z}} > 0$. We apply Theorem 3 with $f(n) = \mathrm{e}(h\phi(s_q(n)))$. Using Lemma 20, we deduce the existence of $\delta > 0$ such that for all $\lambda \in \mathbb{N}$,

$$\sum_{n \in \mathcal{N}_\lambda} \mathrm{e}(h\phi(s_q(n))) \ll Q^{(1-\delta)\lambda}.$$

The Weil criterion [Ten15, Theorem I.6.13] concludes the proof. □

7.2. **Rudin-Shapiro sequences.**

Lemma 21. *Let $\alpha \in \mathbb{R}$, and $(q, \mathcal{D})$ be a binary FNS. The function given by $f(n) = \mathrm{e}(\alpha r_{q,\mathcal{D}}(n))$ satisfies the Carry property* (2.5) *with $\eta_1 = \eta_2$, and the Fourier property* (2.6) *with a function γ satisfying*

$$\gamma(\lambda) \geq \frac{\lambda}{2} \log\Big(\frac{2}{1 + |\cos(\pi\alpha)|} \Big) + O(1),$$

and any $\kappa \in \mathbb{N}$.

Proof. The Carry property follows by an argument identical to the one used in Lemma For the Fourier property, we use Theorem 3.1 in [AL91]. Note that the sum is restricted to integers there, but what is actually considered is a sum over all words of fixed length. The corresponding reduction in pages 12-13 is not needed in our case, since we are summing over the full set $\mathcal{N}_\lambda$. □

Proof of Theorem 2. The deduction of Theorem 2 is identical to the argument used in the case $s_{q,\mathcal{D}}(n)$. □

Acknowledgements. This work was partly supported by ANR-14-CE34-0009 MUDERA.

Appendix A. Asymptotic behaviour of the addition constant

The constant η_2 from Lemma 8 does not seem to admit an explicit expression in terms *e.g.* of the minimal polynomial of q. In this section we consider the special case of canonical number systems (CNS), meaning those number systems $(q, \mathcal{D})$ satisfying $\mathcal{D} = \{0, 1, \dots, Q-1\}$. By [Kov81], if q_0 is the basis of a CNS, then for all large enough $m \in \mathbb{N}$, $-m+q$ is also the basis of a CNS. The goal of this appendix is to show that as $m \to +\infty$, there are admissible carry constants (from Lemma 8) which are very close to the best possible value.

Proposition 4. *Suppose that q_0 is the basis of a CNS, and let $m \in \mathbb{N}$ be large enough that $q_m := -m + q_0$ also is. Then, for the CNS associated with q_m, Lemma 8 holds for a value of $\eta_{2,m}$ satisfying*

$$\eta_{2,m} \geq \frac{1}{d} - O\Big(\frac{1}{\log m}\Big),$$

where the implied constant depends at most on K and q_0. Consequently, the border $\partial\mathcal{F}_m$ of the fundamental tile associated to q_m has upper-box dimension

$$\overline{\dim_B}(\partial\mathcal{F}_m) \leq d - 1 + O\Big(\frac{1}{\log m}\Big).$$

Note that we always have $\overline{\dim_B}(\partial\mathcal{F}_m) \geq d-1$.

Proof. The value $\eta_{2,m}$, as was apparent from the proof of Lemma 8, is related to the largest eigenvalue of the adjacency matrix of the tranducer describing carry propagation in base q_m (which was used in the above proof of Lemma 8). We will work with the formalism described in [ST02], where this transducer was described explicitely for CNS. For all $m \in \mathbb{N}_{\geq 0}$ we let $\sum_{j=0}^{d} c_{j,m} X^j$ be the minimal polynomial of $q_m = -m + q_0$, with $c_{d,m} = 1$. Note that as $m \to \infty$, we have $c_{j,m} \sim m^{d-j}\binom{d}{j}$, so that for m large enough in terms of q_0 the condition $c_{j,m} < c_{j-1,m}$ is satisfied for $1 \leq j \leq d$. We define a transducer $\mathcal{T}$ in the following way :

- The set of states is indexed by subsets $I \subset \{0, \dots, d\}$,
- The set of labels is $\mathcal{D} = \{0, \dots, b_0 - 1\}$,
- Given a state $I = \{i_0, \dots, i_r\}$ (with $i_0 \leq \cdots \leq i_r$), we define
$$\eta(I) = \sum_{j \geq 0} (-1)^j c_{i_j,m},$$
with the convention $\eta(\varnothing) = 0$.
- From a labeled state (I_1, d_1), there is a transition to another labeled state (I_2, d_2) determined as follows :
  - If $d_1 + \eta(I_1) < c_{0,m}$, then $d_2 = d_1 + \eta(I_1)$ and $I_2 = I + 1 := \{i+1, i \in I\}$.
  - Otherwise, $d_2 = d_1 + \eta(I_1) - c_{0,m}$ and $I_2 = ((I+1) \smallsetminus \{0,1\}) \cup (\{0,1\} \smallsetminus (I+1))$.

The states $I = \{0\}$ and $I = \varnothing$ are absorbing. Let $N_m(\ell)$ be the number of possible length ℓ paths in $\mathcal{T}$ not leading to an absorbing state. Then any value $\eta_{2,m} > 0$ such that $N_m(\ell) = O(Q^{(1-\eta_2)\ell})$ is admissible as a carry constant.

We wish to upper-bound the number $N_m(\ell)$. To this end, we partition the subsets of $\{0, \dots, d\}$ into $d+1$ classes, according to their smallest or second smallest element :

$$V_\varnothing, V_1, V_2 \dots, V_d,$$

where $V_\varnothing = \{\{0\}, \varnothing\}$, and for $j \geq 1$, V_j consists of the sets whose minimal nonzero element is j. We consider the directed graph G whose vertices are $V_\varnothing, V_1, \dots, V_d$, and for each pair (V, V') of vertices, we have an edge $V \to V'$ with (possibly nil) multiplicity given by the number of transitions $(I_1, d_1) \to (I_2, d_2)$ in $\mathcal{T}$ where $I_1 \in V$ and $I_2 \in V'$. Let $N'_m(\ell)$ be the total number of paths in G avoiding $V_\varnothing$ with multiplicity. Then, by construction, we have $N_m(\ell) \leq N'_m(\ell)$

For $j \geq 1$, the number of edges in G from V_j to V_{j+1} (with the convention $V_{d+1} = V_\varnothing$) is given by

$$\begin{aligned}\alpha_{j,m} &= \sum_{\substack{I \\ \min(I)=j}} (c_{0,m} - \eta(I)) + \sum_{\substack{I:\ 0\in I \\ \min(I\smallsetminus\{0\})=j}} \eta(I) \\ &= 2^{d-j+1}(c_{0,m} - c_{j,m}) + 2^{d-j} c_{j+1,m},\end{aligned}$$

while the rest of the edges going from V_j lead to V_1, and the number of them is given by

$$\beta_{j,m} = 2^{d-j+1} c_{j,m} - 2^{d-j} c_{j+1,m}.$$

By Perron-Frobenius' theorem, the number of such path is controlled by the leading eigenvalue $\lambda_m > 0$ of the adjacency matrix (where the absorbing state $V_\varnothing$ is taken away)

$$M_m = \begin{pmatrix} \beta_{1,m} & \beta_{2,m} & \beta_{3,m} & \cdots & \beta_{d-1,m} & \beta_{d,m} \\ \alpha_{1,m} & 0 & 0 & \cdots & 0 & 0 \\ 0 & \alpha_{2,m} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & 0 & \cdots & \alpha_{d-1,m} & 0 \end{pmatrix},$$

in the sense that $N'_m(\ell) = O((2\lambda_m)^\ell)$, say; we will not require anything more precise. The characteristic polynomial of M_m is

$$P_m(x) = x^d - \sum_{k=1}^{d} \alpha_{1,m} \cdots \alpha_{k-1,m} \beta_{k,m} x^{d-k}.$$

Uniformly for $x \geq 0$, as $m \to \infty$, we have

$$\begin{aligned}\sum_{k=1}^{d} \alpha_{1,m} \cdots \alpha_{k-1,m} \beta_{k,m} x^{d-k} &= (1+o(1)) m^{-d} \sum_{k=1}^{d} 2^{\frac{k(2d+1-k)}{2}} (m^d)^k (mx)^{d-k} \binom{d}{k} \\ &\leq (1+o(1)) 2^{\frac{d(d+1)}{2}} ((x+m^{d-1})^d - x^d).\end{aligned}$$

Therefore $P_m(x) > 0$ if $x \geq C m^{d-1}$ for a suitable number C (depending on K and x), and so $\lambda_m = O(m^{d-1})$, so that $N_m(\ell)^{1/\ell} \ll m^{d-1}$. We deduce that there is an admissible constant $\eta_{2,m}$ satisfying $Q^{1-\eta_{2,m}} \ll m^{d-1}$. Since $Q \sim m^d$, we conclude $\eta_{2,m} \geq \frac{1}{d} - O(\frac{1}{\log m})$ as claimed. The bound on the upper-box dimension follows by [ST02, Theorem 4.7] (with $\mu = Q^{1-\eta_2}$, $Q \sim m^d$, and $\beta_{max} \sim m$). □

References

[ABP03] S. Akiyama, H. Brunotte, and A. Pethő, *Cubic CNS polynomials, notes on a conjecture of W. J. Gilbert*, J. Math. Anal. Appl. **281** (2003), no. 1, 402–415.

[AP02] S. Akiyama and A. Pethő, *On canonical number systems*, Theoret. Comput. Sci. **270** (2002), no. 1-2, 921–933.

[AL91] J.-P. Allouche and P. Liardet, *Generalized Rudin-Shapiro sequences*, Acta Arith. **60** (1991), no. 1, 1–27. MR 1129977

[BBLT06] G. Barat, V. Berthé, P. Liardet, and J. M. Thuswaldner, *Dynamical directions in numeration*, Ann. Inst. Fourier (Grenoble) **56** (2006), no. 7, 1987–2092.

[BvH05] A. Barbé and F. von Haeseler, *Correlation and spectral properties of higher-dimensional paperfolding and Rudin-Shapiro sequences*, J. Phys. A **38** (2005), no. 12, 2599–2622. MR 2132076

[BvH06] ———, *Binary number systems for* $\mathbb{Z}^k$, J. Number Theory **117** (2006), no. 1, 14–30. MR 2204733

[Bou15] J. Bourgain, *Prescribing the binary digits of primes, II*, Israel J. Math. **206** (2015), no. 1, 165–182. MR 3319636

[BHP06] H. Brunotte, A. Huszti, and A. Pethő, *Bases of canonical number systems in quartic algebraic number fields*, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 537–557.

[CD93] A. Cohen and I. Daubechies, *Nonseparable bidimensional wavelet bases*, Rev. Mat. Iberoamericana **9** (1993), no. 1, 51–137.

[CD96] ———, *A new technique to estimate the regularity of refinable functions*, Rev. Mat. Iberoamericana **12** (1996), no. 2, 527–591.

[DT05] C. Dartyge and G. Tenenbaum, *Sommes des chiffres de multiples d'entiers*, Ann. Inst. Fourier (Grenoble) **55** (2005), no. 7, 2423–2474. MR 2207389

[DT18] S. Drappeau and B. Topacogullari, *Combinatorial identities and Titchmarsh's problem for multiplicative functions*, Preprint, 2018.

[DGL08] M. Drmota, P. J. Grabner, and P. Liardet, *Block additive functions on the Gaussian integers*, Acta Arith. **135** (2008), no. 4, 299–332. MR 2465714

[DMR09] M. Drmota, C. Mauduit, and J. Rivat, *Primes with an average sum of digits*, Compositio Math. **145** (2009), no. 2, 271–292. MR 2501419

[DMR11] ———, *The sum-of-digits function of polynomial sequences*, J. London Math. Soc. **84** (2011), no. 1, 81–102. MR 2819691

[DMR19] ———, *Normality along squares*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 2, 507–548. MR 3896209

[DM12] M. Drmota and J. F. Morgenbesser, *Generalized Thue-Morse sequences of squares*, Israel J. Math. **190** (2012), 157–193. MR 2956237

[DRS08] M. Drmota, J. Rivat, and T. Stoll, *The sum of digits of primes in* $\mathbb{Z}[i]$, Monatsh. Math. **155** (2008), no. 3-4, 317–347.

[FM96a] É. Fouvry and C. Mauduit, *Méthodes de crible et fonctions sommes des chiffres*, Acta Arith. **77** (1996), no. 4, 339–351. MR 1414514

[FM96b] É. Fouvry and C. Mauduit, *Sommes des chiffres et nombres presque premiers*, Math. Ann. **305** (1996), no. 3, 571–599.

[Gel68] A. O. Gel'fond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith. **13** (1967/1968), 259–265. MR 0220693

[GK07] L. Germán and A. Kovács, *On number system constructions*, Acta Math. Hungar. **115** (2007), no. 1-2, 155–167.

[Gil86] W. J. Gilbert, *The fractal dimension of sets derived from complex bases*, Canad. Math. Bull. **29** (1986), no. 4, 495–500.

[GT00] B. Gittenberger and J. M. Thuswaldner, *Asymptotic normality of b-additive functions on polynomial sequences in the Gaussian number field*, J. Number Theory **84** (2000), no. 2, 317–341.

[GL99] P. Grabner and P. Liardet, *Harmonic properties of the sum-of-digits function for complex bases*, Acta Arith. **91** (1999), no. 4, 329–349.

[GKP98] P. J. Grabner, P. Kirschenhofer, and H. Prodinger, *The sum-of-digits function for complex bases*, J. Lond. Math. Soc. (2) **57** (1998), no. 1, 20–40. MR 1624777

[GH94] K. Gröchenig and A. Haas, *Self-similar lattice tilings*, J. Fourier Anal. Appl. **1** (1994), no. 2, 131–170.

[Han17] G. Hanna, *Sur les occurrences des mots dans les nombres premiers*, Acta Arith. **178** (2017), no. 1, 15–42. MR 3626236

[HK08] G. Harman and I. Kátai, *Primes with preassigned digits. II*, Acta Arith. **133** (2008), no. 2, 171–184. MR 2417463

[Hin88] J. G. Hinz, *A generalization of Bombieri's prime number theorem to algebraic number fields*, Acta Arith. **51** (1988), no. 2, 173–193.

[Hux68] M. N. Huxley, *The large sieve inequality for algebraic number fields*, Mathematika **15** (1968), 178–187.
[IK04] H. Iwaniec and E. Kowalski, *Analytic number theory*, vol. 53, Cambridge Univ Press, 2004.
[KK80] 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.
[KK81] ———, *Canonical number systems in imaginary quadratic fields*, Acta Math. Acad. Sci. Hungar. **37** (1981), no. 1-3, 159–164.
[KS75] I. Kátai and J. Szabó, *Canonical number systems for complex integers*, Acta Sci. Math. (Szeged) **37** (1975), no. 3-4, 255–260.
[Kee99] J. Keesling, *The boundaries of self-similar tiles in* $\mathbf{R}^n$, Topology Appl. **94** (1999), no. 1-3, 195–205.
[Knu81] D. E. Knuth, *The art of computer programming. Vol. 2*, second ed., Addison-Wesley Publishing Co., Reading, Mass., 1981, Seminumerical algorithms, Addison-Wesley Series in Computer Science and Information Processing. MR 633878
[Kov81] B. Kovács, *Canonical number systems in algebraic number fields*, Acta Math. Acad. Sci. Hungar. **37** (1981), no. 4, 405–407.
[KP91] B. Kovács and A. Pethő, *Number systems in interal domains, especially in orders of algebraic number fields*, Acta Sci. Math. (Szeged) **55** (1991), no. 3-4, 287–299.
[LW96] J. C. Lagarias and Y. Wang, *Self-affine tiles in* R^n, Adv. Math. **121** (1996), no. 1, 21–49.
[Mad10] M. G. Madritsch, *Asymptotic normality of b-additive functions on polynomial sequences in number systems*, Ramanujan J. **21** (2010), no. 2, 181–210.
[Man82] B. B. Mandelbrot, *The fractal geometry of nature*, W. H. Freeman and Co., San Francisco, Calif., 1982, Schriftenreihe für den Referenten. [Series for the Referee]. MR 665254
[MR09] C. Mauduit and J. Rivat, *La somme des chiffres des carrés*, Acta Math. **203** (2009), no. 1, 107–148.
[MR10] ———, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*, Ann. of Math. (2) **171** (2010), no. 3, 1591–1646.
[MR15] ———, *Prime numbers along Rudin-Shapiro sequences*, J. Eur. Math. Soc. **17** (2015), no. 10, 2595–2642.
[MR18] ———, *Rudin-Shapiro sequences along squares*, Trans. Amer. Math. Soc. **370** (2018), no. 11, 7899–7921. MR 3852452
[Mon78] H. L. Montgomery, *The analytic principle of the large sieve*, Bull. Amer. Math. Soc. **84** (1978), no. 4, 547–567.
[Mor10] J. F. Morgenbesser, *The sum of digits of squares in* $Z[i]$, J. Number Theory **130** (2010), no. 7, 1433–1469.
[Mor12] ———, *The sum of digits of Gaussian primes*, Ramanujan J. **27** (2012), no. 1, 43–70.
[MTT01] W. Müller, J. M. Thuswaldner, and R. F. Tichy, *Fractal properties of number systems*, Period. Math. Hungar. **42** (2001), no. 1-2, 51–68.
[Mül17] C. Müllner, *Automatic sequences fulfill the Sarnak conjecture*, Duke Math. J. **166** (2017), no. 17, 3219–3290. MR 3724218
[MS17] C. Müllner and L. Spiegelhofer, *Normality of the Thue-Morse sequence along Piatetski-Shapiro sequences, II*, Israel J. Math. **220** (2017), no. 2, 691–738.
[MV07] R. M. Murty and J. Van Order, *Counting integral ideals in a number field*, Exposition. Math. **25** (2007), no. 1, 53–66.
[Nar04] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, third ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004.
[Neu99] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR 1697859
[PT18] A. Pethő and J. M. Thuswaldner, *Number systems over orders*, Monatshefte für Mathematik **187** (2018), no. 4, 681–704. MR 3861324
[PW08] M. Pollicott and H. Weiss, *How smooth is your wavelet? Wavelet regularity via thermodynamic formalism*, Commun. Math. Phys. **281** (2008), no. 1, 1–21.
[Ram13] O. Ramaré, *Prime numbers: emergence and victories of bilinear forms decomposition*, Eur. Math. Soc. Newsl. (2013), no. 90, 18–27.

[Rud59] W. Rudin, *Some theorems on Fourier coefficients*, Proc. Amer. Math. Soc. **10** (1959), 855–859. MR 0116184

[Sar12] P. Sarnak, *Mobius randomness and dynamics*, Not. S. Afr. Math. Soc. **43** (2012), no. 2, 89–97.

[ST02] K. Scheicher and J. M. Thuswaldner, *Canonical number systems, counting automata and fractals*, Math. Proc. Cambridge Phil. Soc. **133** (2002), no. 1, 163–182.

[Sha53] H. S. Shapiro, *Extremal problems for polynomials and power series*, ProQuest LLC, Ann Arbor, MI, 1953, Thesis (Ph.D.)–Massachusetts Institute of Technology. MR 2938495

[Spi18] L. Spiegelhofer, *The level of distribution of the Thue–Morse sequence*, Preprint, 2018.

[Ste02] W. Steiner, *Parry expansions of polynomial sequences*, Integers **2** (2002), Paper A14, 28.

[Swa19] C. Swaenepoel, *Prime numbers with a positive proportion of preassigned digits*, Preprint, 2019.

[Ten15] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, third ed., Graduate Studies in Mathematics, vol. 163, American Mathematical Society, Providence, RI, 2015, Translated from the 2008 French edition by Patrick D. F. Ion. MR 3363366

[Thu98a] J. M. Thuswaldner, *Fractal dimension of sets induced by bases of imaginary quadratic fields*, Math. Slovaca **48** (1998), no. 4, 365–371.

[Thu98b] ———, *The sum of digits function in number fields*, Bull. London Math. Soc. **30** (1998), no. 1, 37–45. MR 1479034

[Thu01] ———, *Fractals and number systems in real quadratic number fields*, Acta Math. Hungar. **90** (2001), no. 3, 253–269.

[Tót00] Á. Tóth, *Roots of quadratic congruences*, Int. Math. Res. Notices **2000** (2000), no. 14, 719–739.

[Vaa85] J. D. Vaaler, *Some extremal functions in Fourier analysis*, Bull. Amer. Math. Soc. (N.S.) **12** (1985), no. 2, 183–216. MR 776471

[Vau80] R. C. Vaughan, *An elementary method in prime number theory*, Polska Akademia Nauk. Instytut Matematyczny. Acta Arith. **37** (1980), 111–115.

[Vin95] A. Vince, *Rep-tiling Euclidean space*, Aequationes Math. **50** (1995), no. 1-2, 191–213.

[Vin37] I. M. Vinogradov, *Representation of an odd number as a sum of three primes*, Dokl. Akad. Nauk SSSR **15** (1937), 291–294, English Translation in *Selected Works*, pages 129–132, Springer-Verlag, Berlin, 1985.

[Wir98] F. Wirth, *On the calculation of time-varying stability radii*, Internat. J. Robust Nonlinear Control **8** (1998), no. 12, 1043–1058.

Aix Marseille Université, CNRS, Centrale Marseille, I2M UMR 7373, 13453, Marseille, France

Email address: sary-aurelien.drappeau@univ-amu.fr

Institut Élie Cartan de Lorraine, Université de Lorraine, Site de Nancy, B.P. 70239, F-54506 Vandoeuvre-lès-Nancy Cedex

Email address: gautier.hanna@univ-lorraine.fr