ON SPARSITY OF REPRESENTATIONS OF POLYNOMIALS AS LINEAR COMBINATIONS OF EXPONENTIAL FUNCTIONS

DRAGOS GHIOCA, ALINA OSTAFE, SINA SALEH, AND IGOR E. SHPARLINSKI

Abstract. Given an integer g and also some given integers m (sufficiently large) and $c_1, \ldots, c_m$, we show that the number of all non-negative integers $n \leqslant M$ with the property that there exist non-negative integers $k_1, \ldots, k_m$ such that

$$n^2 = \sum_{i=1}^{m} c_i g^{k_i}$$

is $o\left((\log M)^{m-1/2}\right)$. We also obtain a similar bound when dealing with more general inequalities

$$\left|Q(n) - \sum_{i=1}^{m} c_i \lambda^{k_i}\right| \leqslant B,$$

where $Q \in \mathbb{C}[X]$ and also $\lambda \in \mathbb{C}$ (while B is a real number).

1. Introduction

1.1. **Set-up.** Motivated by applications to the *dynamical Mordell-Lang conjecture* (for more details on this open problem in arithmetic dynamics, we refer the reader to [BGT16]), the authors [GOSS21] have recently considered the question about representations of values of polynomials $Q \in \overline{\mathbb{Q}}[X]$ as fixed linear combinations of powers of a prime p. In particular, it is shown in [GOSS21] that for fixed coefficients $c_1, \ldots, c_m \in \overline{\mathbb{Q}}$ and integral exponents $a_1, \ldots, a_m$ the number of positive integers $n \leqslant N$ for which $Q(n)$ can be represented as

$$Q(n) = \sum_{i=1}^{m} c_i p^{a_i k_i}$$

with some $k_1, \ldots, k_m \in \mathbb{Z}$ is bounded by $O\left((1 + \log N)^m\right)$ where the implied constant depends only on the initial data. In fact it is easy

2010 *Mathematics Subject Classification.* 11A63, 11B57, 11T23.

Key words and phrases. Squares, sparse representations, square-sieve, character sums.

to see that for $Q(n) = n$, this bound is tight. Furthermore, a similar result is given in [GOSS21] for representations of the form

$$Q(n) = \sum_{i=1}^{m} \sum_{j=1}^{s} c_{i,j} \lambda_j^{a_i k_i}, \tag{1.1}$$

with algebraic integers $\lambda_1, \ldots, \lambda_s$, each one of them of absolute value equal to q or $\sqrt{q}$ (where q is a given power of a prime number).

Here we first consider representations of the form (1.1) with $s = 1$ but arbitrary complex (rather than algebraic) parameters. We also generalise this to approximations of polynomials rather than precise equalities, that is, we consider inequalities of the form

$$\left| Q(n) - \sum_{i=1}^{m} c_i \lambda^{k_i} \right| \leqslant B, \tag{1.2}$$

with $Q \in \mathbb{C}[X]$, $c_1, \ldots, c_m, \lambda \in \mathbb{C}$ and some $B \in \mathbb{R}$.

We then use a very different approach to obtain more precise results in the very appealing special case of squares, that is, for $Q(n) = n^2$. This approach is based on a version of the square-sieve of Heath-Brown [H-B84] augmented by results of Katz [Kat02] on bounds multiplicative character sums with non-singular multivariate polynomials and results of Baker and Harman [BaHa98] on shifted primes with a large prime divisors.

1.2. **Notation.** We now recall that the notations $A = O(B)$, $A \ll B$ and $B \gg A$ are all equivalent to the inequality $|A| \leqslant cB$ with some constant c. Throughout this work all implied constants may depend on the polynomial Q and the parameters c_i, $i = 1, \ldots, m$ and λ in (1.2) and also on g in (1.4) below.

For a finite set $\mathscr{S}$ we use $\#\mathscr{S}$ to denote its cardinality.

1.3. **New results.** We remark that the argument of [GOSS21] is based on a result of Laurent [Lau84, Théorème 6], which required all parameters to be defined over a number field; furthermore, the result of [Lau84] refers to equalities, not inequalities. Hence here we use a different approach to establish the following result.

Theorem 1.1. *Let $c_1, \ldots, c_m, \lambda \in \mathbb{C}$, $B \in \mathbb{R}$ and let $Q \in \mathbb{C}[X]$ be a non-constant polynomial. Then for $N \geqslant 2$ we have*

$$\#\{n \leqslant N : \text{ (1.2) holds for some } k_1, \ldots, k_m \in \mathbb{Z}\} \ll (\log N)^m.$$

We observe that the implied constant in Theorem 1.1 is effectively computable in terms of the sizes of the initial data, while in the result of [GOSS21] it is not.

We also note (see Example 2.1) that if one considers inequalities of the form

$$\left|Q(n) - \sum_{i=1}^{m}\sum_{j=1}^{s} c_{i,j}\lambda_j^{a_i k_i}\right| \leqslant B, \tag{1.3}$$

for some arbitrary complex numbers λ_j, then one cannot expect a similar result as in Theorem 1.1. More precisely, there exists $\lambda \in \mathbb{C}$ such that for any $\varepsilon > 0$ and *each* sufficiently large integer n, there exists some positive integer k_n with the property that

$$\left|n - \frac{i}{\pi}\cdot\left(2^{k_n} - \lambda^{k_n}\right)\right| \leqslant \varepsilon,$$

see Example 2.1 for more details.

Furthermore, we consider the case of perfect squares and study relations of the form

$$n^2 = \sum_{i=1}^{m} c_i g^{k_i}, \tag{1.4}$$

with non-zero integer coefficients $c_1, \dots, c_m$ and an integer basis $g \geqslant 2$. Using the square-sieve of Heath-Brown [H-B84] we improve the exponent m of $\log N$.

For $m = 2$, we write the equation (1.4) as $n^2 = g^{k_1}\left(c_1 + c_2 g^{k_2-k_1}\right)$ (with $k_2 \geqslant k_1$). Hence either $c_1 + c_2 g^{k_2-k_1}$ or $c_1 g + c_2 g^{k_2-k_1+1}$ is a perfect square j^2 for some $j \leqslant n \leqslant N$. Since the largest prime divisor of $j^2 + c$ for any $c \neq 0$ tends to infinity with j, see [Kea69], we see that $k_2 - k_1$ can take only finitely many values. Hence for $m = 2$ we have $O(\log N)$ solution to (1.4) with $n \leqslant N$. This bound is obviously the best possible as the example of the numbers $2^{k_1} + 2^{k_2}$, with $k_2 = k_1 + 3$ and even k_1, shows. We also note that in [CGSZ, Theorem 5.1 (B)], it is established even more generally the *precise* set of all positive integers n for which u_n is of the form $c_1 g^{k_1} + c_2 g^{k_2}$ (for some given g, c_1, c_2), where $\{u_n\}_{n\geqslant 1}$ is an arbitrary linear recurrence sequence (the result of [CGSZ, Theorem 5.1 (B)] is stated only when $g = p$ is a prime number, but as remarked in [CGSZ, Section 5], the method extends verbatim to an arbitrary integer g).

So we are mostly interested in the case of $m \geqslant 3$; furthermore, we note that for $m = 3$ (and in some cases, depending on g and the c_i, even for $m = 4$), more precise results are available in the literature (see [CoZa13]). However, when $m \geqslant 5$, it is very difficult to find a precise description of all $n \in \mathbb{N}$ such that n^2 is of the form (1.4) (for some given integers g and c_i).

Theorem 1.2. *Let $m \geqslant 3$ and let $c_1, \ldots, c_m$ and $g \geqslant 2$ be integers. Then for $N \geqslant 2$ we have*

$$\#\{n \leqslant N : \text{(1.4) holds for some } k_1, \ldots, k_m \in \mathbb{Z}\} \leqslant (\log N)^{m-\gamma_m+o(1)},$$

where

$$\gamma_3 = \frac{677}{1969} \qquad \text{and} \qquad \gamma_m = \frac{677m}{1323m + 1354} \quad \text{for } m \geqslant 4.$$

We observe that $\gamma_m \to 677/1323 = 0.5117\ldots$ as $m \to \infty$. Thus for large m Theorem 1.2 saves more than $1/2$ compared to the general bound of Theorem 1.1. More precisely, simple calculations show that $\gamma_m > 1/2$ for $m \geqslant 44$.

We remark that the proof of Theorem 1.2 is based on some ideas and results from [LuSh09], later enhanced in [BaSh17]. The numerical constants come from the work of Baker and Harman [BaHa98] on large prime divisors of shifted primes.

Furthermore, as in [BaSh17] we observe that under the Generalised Riemann Hypothesis we can obtain a slightly larger value of γ_m.

On the other hand defining s as the largest integer with $s(s+1)/2 \leqslant m$ and considering numbers $\left(g^{h_1} + \ldots + g^{h_s}\right)^2$ with

$$h_i \leqslant \frac{\log\left(N/s^2\right)}{2\log g}, \quad i = 1, \ldots, s,$$

we see that for at least one choice $c_1, \ldots, c_t > 0$ with $t \leqslant m$ and $c_1 + \ldots + c_t \leqslant s(s+1)/2$ occurs at least $C_0(\log N)^s$ times, for some constant $C_0 > 0$, which shows that the best possible exponent in any result of the type of Theorem 1.2 must grow with m (at least as about $\sqrt{2m}$ for large m).

Note that cycling over all g^m choices of

$$(c_1, \ldots, c_m) \in \{0, \ldots, g-1\}^m$$

we obtain from Theorem 1.2 a result about the sparsity of the values of n for which n^2 has at most m non-zero digits to base g. Various finiteness results on sparse digital representations of perfect powers can be found in [BeBu14, BBM13, CoZa13, Mos21]. Note that as we have just seen, in our setting of arbitrary m no finiteness result is possible, and hence we can use Theorem 1.2 to provide a counting result related to such representations. More precisely we have the following straightforward consequence:

Corollary 1.3. *Let $m \geqslant 3$ and let $K \geqslant 1$ and $g \geqslant 2$ be integers. Then there are at most $K^{m-\gamma_m+o(1)}$ integer squares with g-ary expansion of length K and with at most m non-zero digits.*

2. Proof of Theorem 1.1

2.1. **Counterexample to a possible extension to (1.3).** Before proceeding to the proof of Theorem 1.1, we provide the Example 2.1 (mentioned in Section 1.3), which shows that one cannot expect to generalise Theorem 1.1 to (1.3), that is, to the case when we approximate $Q(n)$ with a sum of powers of different λ_j.

Example 2.1. *We consider the sequence of positive integers* $\{b_j\}_{j\geqslant 2}$ *given by*

$$b_2 = 2 \qquad \text{and} \qquad b_{j+1} = 2^{b_j} + b_j + 1 \text{ for } j \geqslant 2.$$

We let $\lambda = 2 \cdot e^{2\pi\alpha i}$, *where*

$$\alpha = \sum_{j=2}^{\infty} \frac{j-1}{2^{b_j}}.$$

We let n *be a positive integer and show that*

$$n - \frac{i}{\pi} \cdot \left(2^{2^{b_n}} - \lambda^{2^{b_n}} \right) \ll \frac{n}{b_{n+1}}. \tag{2.1}$$

Indeed, we first notice that

$$\lambda^{2^{b_n}} = 2^{2^{b_n}} \cdot e^{2\pi t_n i},$$

where

$$t_n = \sum_{j=n+1}^{\infty} \frac{j-1}{2^{b_j - b_n}}.$$

Then

$$\begin{aligned} 2^{2^{b_n}} - \lambda^{2^{b_n}} &= 2^{2^{b_n}} \cdot \left((1 - \cos(2\pi t_n)) - i \sin(2\pi t_n) \right) \\ &= 2^{2^{b_n}} \cdot 2\sin(\pi t_n) \cdot \left(\sin(\pi t_n) - i \cos(\pi t_n) \right), \end{aligned}$$

and so,

$$\frac{i}{\pi} \cdot \left(2^{2^{b_n}} - \lambda^{2^{b_n}} \right) = \frac{2^{1+2^{b_n}} \sin(\pi t_n)}{\pi} \cdot e^{\pi t_n i}. \tag{2.2}$$

Now, by the definition of the rapidly increasing sequence $\{b_j\}_{j\geqslant 2}$, *we have that*

$$0 < t_n - \frac{n}{2^{b_{n+1} - b_n}} < \frac{1}{2^{2^{b_{n+1}}}}; \tag{2.3}$$

also, clearly, $t_n \to 0$ *as* $n \to \infty$. *Furthermore, we know that when* t *is close to* 0, *then*

$$|\sin t - t| \leqslant t^2. \tag{2.4}$$

So, using the inequalities (2.3) and (2.4), along with the fact that $b_{n+1} = 2^{b_n} + b_n + 1$*, we get that*

$$\left| n - \frac{2^{1+2^{b_n}} \sin(\pi t_n)}{\pi} \right| < 2^{-b_n} \ll 1/b_{n+1} \tag{2.5}$$

for all n *sufficiently large. Also, for* n *large, using the inequality (2.3) we have that*

$$\left|1 - e^{\pi t_n i}\right| < 2^{-b_n} \ll 1/b_{n+1}. \tag{2.6}$$

Recalling (2.2) and using (2.5) and (2.6), we derive (2.1).

Therefore, the conclusion of Theorem 1.1 cannot be generalised to inequalities (1.3) where we approximate a polynomial $Q(n)$ with sums of powers of different $\lambda_1, \dots, \lambda_s$.

Next we proceed to proving Theorem 1.1.

2.2. **Preliminaries.** We first note that if $|\lambda| = 1$, then the inequality (1.2) yields that $|Q(n)|$ is uniformly bounded above and therefore, we can only have finitely many $n \in \mathbb{N}$ satisfying such inequality since Q is a non-constant polynomial. Furthermore, since the exponents k_i appearing in the inequality (1.2) are arbitrary integers, then without loss of generality, we may assume from now on that $|\lambda| > 1$.

Now, if some of the exponents k_i, $i = 1, \dots, m$, from (1.2) were non-positive, then the absolute value of the corresponding terms $c_i\lambda^{k_i}$ is uniformly bounded above. So, at the expense of replacing B by a larger constant (but depending only on the absolute values of the c_i), we may assume from now on, that each exponent k_i from (1.2) is positive.

Let $Q(X) = a_dX^d + \cdots + a_1X + a_0$ for complex numbers $a_0, \dots, a_d$ with $a_d \neq 0$. There exists $N_0 \geqslant 0$ (depending only on d and the absolute values of the coefficients of Q) such that

$$|Q(n)| \leqslant 2\left|a_d n^d\right| \leqslant N_0 \cdot n^d \text{ for each } n \geqslant N_0. \tag{2.7}$$

Furthermore, at the expense of replacing N_0 by a larger positive integer (but still depending only on d, the absolute values of the coefficients of Q and also depending on B in this case), we may also assume that

$$|Q(n_1 + n_2) - Q(n_1)| > 2B \text{ for each } n_1, n_2 \geqslant N_0. \tag{2.8}$$

2.3. **Induction.** We proceed to prove our desired result by induction on m.

We prove first the base case $m = 1$, which also constitutes the inspiration for our proof for the general case in Theorem 1.1. So, we have that $|Q(n)| = O(N^d)$ for each $0 \leqslant n \leqslant N$ (see also the inequality (2.7)). Therefore, for $n \leqslant N$ satisfying the inequality

$$\left|Q(n) - c_1\lambda^{k_1}\right| \leqslant B \tag{2.9}$$

one has $|\lambda|^{k_1} = O\left(N^d\right)$ and thus, $k_1 = O(\log N)$. On the other hand, for a given k_1, the inequality (2.9) is satisfied by $O(1)$ non-negative integers n (see also (2.8)), thus proving the desired bound in the case $m = 1$.

So, suppose that the result is true for $m \leqslant s$ and we prove that Theorem 1.1 holds when $m = s+1$; clearly we may assume each c_i for $i = 1, \ldots, s+1$ is nonzero. Since there are m powers of λ in the inequality (1.2), then in order to prove Theorem 1.1, it suffices to prove that the set $\mathscr{S}_0$, consisting of all $n \in \mathbb{N}$ for which there exist integers

$$1 \leqslant k_1 \leqslant k_2 \leqslant \cdots \leqslant k_{s+1} \tag{2.10}$$

such that

$$\left|Q(n) - \sum_{j=1}^{s+1} c_j\lambda^{k_j}\right| \leqslant B \tag{2.11}$$

satisfies

$$\{n \in \mathscr{S}_0 : \ n \leqslant N\} \ll (\log N)^{s+1}. \tag{2.12}$$

Let $\Delta \in \mathbb{N}$ be sufficiently large (but depending only on $|\lambda|$, which is larger than 1, and also depending on the absolute values of the $c_1, \ldots, c_{s+1}$) such that we have

$$\frac{|c_{s+1}|}{2} \cdot |\lambda|^{k_{s+1}} \leqslant \left|\sum_{j=1}^{s+1} c_j\lambda^{k_j}\right|, \tag{2.13}$$

for all integers $k_{s+1} \geqslant \cdots \geqslant k_1 \geqslant 0$ satisfying the inequality (2.11) along with the inequality $k_{s+1} - k_s \geqslant \Delta$.

Now, we let $\mathscr{U}$ be the subset of $\mathscr{S}_0$ consisting of integers $n \in \mathbb{N}$ for which one can find integers k_j satisfying (2.11) and in addition, $k_{s+1} - k_s < \Delta$. Then the existence of such a solution tuple $(k_1, \ldots, k_{s+1})$ for each $n \in \mathscr{U}$ means that

$$\left|Q(n) - \left(c_1\lambda^{k_1} + \cdots + c_{s-1}\lambda^{k_{s-1}} + \left(c_s + c_{s+1}\lambda^{k_{s+1}-k_s}\right)\lambda^{k_s}\right)\right| \leqslant B.$$

Because $k_{s+1} - k_s \in \{0, \ldots, \Delta - 1\}$, applying the induction hypothesis for each of the possible Δ values of $k_{s+1} - k_s$, we obtain the desired conclusion regarding the asymptotic growth given by (2.12) (furthermore, we actually get that the exponent from the right-hand side of the inequality (2.12) is $s = m - 1$ not $s + 1 = m$).

On the other hand, for each $n \in \mathscr{S}_0 \setminus \mathscr{U}$ satisfying $n \geqslant N_0$, we know that there must exist some tuple of nonnegative integers $(k_1, \ldots, k_{s+1})$ satisfying (2.11) and in addition, $k_{s+1} - k_s \geqslant \Delta$. Then using both (2.7) and (2.13), we get

$$\frac{|c_{s+1}|}{2} \cdot |\lambda|^{k_{s+1}} - B \leqslant \left| c_0 + \sum_{j=1}^{s+1} c_j \lambda^{k_j} \right| - B \leqslant |Q(n)| \leqslant 2|a_d| \cdot n^d,$$

which implies that

$$k_{s+1} \leqslant b_0 (1 + \log n) \tag{2.14}$$

for some positive real number b_0 depending only on B, $|\lambda|$, d, $|a_d|$ and $|c_{s+1}|$.

So, let N be an integer larger than N_0; then for each integer $N_0 \leqslant n \leqslant N$ contained in $\mathscr{S}_0 \setminus \mathscr{U}$, we know there exists an $(s+1)$-tuple of integers k_i satisfying (2.10) and (2.11). Combining the fact that $1 \leqslant k_i \leqslant k_{s+1}$ with the inequality (2.14), we get that there are at most $(b_0 (1 + \log N))^{s+1}$ tuples $(k_1, \ldots, k_{s+1})$ for which we could find some $n \in \mathscr{S}_0 \setminus \mathscr{U}$ satisfying the inequality $N_0 \leqslant n \leqslant N$. However, since $n \geqslant N_0$, then the inequality (2.8) yields that for any such $(s+1)$-tuple of integers k_i, there are *at most* N_0 integers $n \in (\mathscr{S}_0 \setminus \mathscr{U}) \cap [N_0, N]$ satisfying (2.11) with respect to the tuple $(k_1, \ldots, k_{s+1})$. Hence, we get the inequality

$$\# \{n \leqslant N : \ n \in \mathscr{S}_0 \setminus \mathscr{U}\} \leqslant N_0 \cdot \left(1 + (b_0 \cdot (1 + \log N))^{s+1}\right).$$

for each positive integer $N \geqslant N_0$. This concludes our proof of Theorem 1.1.

3. Construction and properties of the sieving set of primes

3.1. **Multiplicative orders.**

Let $\tau_\ell(g)$ denote the multiplicative order of an integer $g \geqslant 2$ modulo a prime ℓ, that is, the smallest positive integer τ for which $g^\tau \equiv 1 \bmod \ell$.

Let α be a fixed real number such that

$$\# \{\ell \leqslant z : \ell \text{ is prime and } P(\ell - 1) \geqslant \ell^\alpha\} \gg \frac{z}{\log z} \tag{3.1}$$

for all sufficiently large z, where $P(k)$ denotes the largest prime divisor of an integer $k \geqslant 2$, and the implied constant depends only on α.

We recall the following well known result which follows from the divisibility $\tau_\ell(g) \mid \ell - 1$ (provided $\gcd(g, \ell) = 1$) and the bound

$$\# \left\{\ell \leqslant z : \ell \text{ is prime}, \ P(\ell - 1) > \ell^{1/2}\right\} = (1 + o(1)) \frac{z}{\log z}$$

as $z \to \infty$, which easily follows from a stronger result of Erdős and Murty [ErMu96, Theorem 3]. Details can be found in the work of Kurlberg and Pomerance [KuPo05, Lemma 20].

Lemma 3.1. *For any fixed $\alpha \geqslant 1/2$ satisfying (3.1) and any fixed integer $g \geqslant 1$ we have*

$$\#\{\ell \leqslant z : \ell \text{ is prime}, \ \tau_\ell(g) \geqslant \ell^\alpha\} \gg \frac{z}{\log z}$$

as $z \to \infty$.

For an integer $s \geqslant 1$ we denote by $\nu_2(s)$ the 2-adic order of s, that is, the largest power ν such that $2^\nu \mid s$.

Lemma 3.2. *For any fixed $\alpha \geqslant 1/2$ satisfying (3.1) and any fixed integer $g \geqslant 1$ there are some absolute constants $C_1, C_2 > 0$, such that for every sufficiently large real number $z > 1$, there exist some integer u_0 and a set $\mathscr{L}_z \subseteq [z, C_1 z]$ of primes of cardinality*

$$\#\mathscr{L}_z \geqslant \frac{C_2 z}{\log z \log\log z}$$

such that for every $\ell \in \mathscr{L}_z$ we have

$$P(\ell-1) \geqslant z^\alpha, \qquad P(\ell-1) \mid \tau_\ell(g), \qquad \nu_2\left(\tau_\ell(g)\right) = u_0.$$

Proof. Lemma 3.1 obviously implies that for some absolute constants C_1, C_3 there are at least $C_3 z/\log z$ primes $\ell \in [z, C_1 z]$ satisfying only the first two conditions, see also [LuSh09, Lemma 5.1]. Let $\overline{\mathscr{L}}_z$ be this set. Trivially, there are at at most $z/2^{v_0}$ primes ℓ with $\nu_2(\tau_\ell(g)) \geqslant v_0$. Hence taking a sufficiently large C_4, and $v_0 = \lfloor C_4 \log\log z \rfloor$, we see that if we remove these primes from $\overline{\mathscr{L}}_z$ we obtain the set of $\widetilde{\mathscr{L}_z} \subseteq \overline{\mathscr{L}}_z$ of cardinality

$$\#\widetilde{\mathscr{L}_z} \geqslant \#\overline{\mathscr{L}}_z - z/2^{v_0} \geqslant 0.5\#\overline{\mathscr{L}}_z \geqslant 0.5 C_3 z/\log z.$$

Since obviously $\nu_2\left(\tau_\ell(g)\right) \leqslant \nu_2\left(\ell - 1\right) \leqslant v_0$, making a majority decision we can find a set of $\mathscr{L}_z$ of cardinality

$$\#\mathscr{L}_z \geqslant \frac{\#\widetilde{\mathscr{L}_z}}{v_0} \geqslant \frac{0.5 C_3 z}{v_0 \log z}$$

with $\nu_2\left(\tau_\ell(g)\right) = u_0$ for some fixed $u_0 \leqslant v_0$ for every $\ell \in \mathscr{L}_z$. Taking $C_2 = 0.5 C_3/C_4$ we conclude the proof. □

We note that the *Brun-Titchmarsh* theorem (see [IwKo04, Theorem 6.6]) can be used to remove $\log\log z$ in the bound on $\#\mathscr{L}_z$ of Lemma 3.2. However in our final result we do not try to optimise terms of this order, so we ignore this and similar potential improvements.

3.2. **Sieving set $\mathscr{L}_z$.** We see that using a result of Baker and Harman [BaHa98] one can take

$$\alpha = 0.677, \tag{3.2}$$

in Lemmas 3.1 and 3.2.

From now on, for any positive real number z, we fix a set $\mathscr{L}_z$ satisfying the conclusion of Lemma 3.2 with α given by (3.2).

3.3. **Bounds of some arithmetic sums.** For an integer K we consider the set

$$\mathscr{K} = \mathscr{K}_m(K) \tag{3.3}$$

where

$$\mathscr{K}_m(K) = \{0, \ldots, K\}^m, \tag{3.4}$$

and for $\mathbf{k} = (k_1, \ldots, k_m) \in \mathscr{K}$ we define

$$F(\mathbf{k}) = \sum_{i=1}^{m} c_i g^{k_i}. \tag{3.5}$$

For a real $z \geqslant 2$ let $\omega_z(n)$ be the number of distinct prime factors $\ell \in \mathscr{L}_z$ of n.

Lemma 3.3. *Let an integer K and a real z be sufficiently large. For $\mathscr{K}$ and $F(\mathbf{k})$ as in (3.3) and (3.5), respectively, we have*

$$\sum_{\mathbf{k} \in \mathscr{K}} \omega_z(F(\mathbf{k})) \ll \left(K^m z^{-\alpha} + K^{m-1}\right) \# \mathscr{L}_z.$$

Proof. We have

$$\sum_{\mathbf{k} \in \mathscr{K}} \omega_z(F(\mathbf{k})) \ll \sum_{\mathbf{k} \in \mathscr{K}} \sum_{\substack{\ell \in \mathscr{L}_z \\ \ell \mid F(\mathbf{k})}} 1 = \sum_{\ell \in \mathscr{L}_z} \sum_{\substack{\mathbf{k} \in \mathscr{K} \\ \ell \mid F(\mathbf{k})}} 1.$$

Clearly the last sum can be estimated as

$$\begin{aligned} \sum_{\substack{\mathbf{k} \in \mathscr{K} \\ \ell \mid F(\mathbf{k})}} 1 &\leqslant (K+1)^{m-1} \left(\frac{K+1}{\tau_\ell(g)} + 1\right) \\ &\ll K^m \ell^{-\alpha} + K^{m-1} \leqslant K^m z^{-\alpha} + K^{m-1}, \end{aligned}$$

and the result follows. □

Remark 3.4. *The proof of Lemma 3.3 appeals to essentially trivial bound $O\left(K^{m-1}\left(K/\tau_\ell(g) + 1\right)\right)$ on the number of solution to the congruence $F(\mathbf{k}) \equiv 0 \pmod{\ell}$, $\mathbf{k} \in \mathscr{K}$. Using bounds of exponential* *sums one can obtain a better bound, which however does not improve our final result (see also our Appendix).*

For a real κ we define the sums

$$D_\kappa = \sum_{\substack{\ell, r \in \mathscr{L}_z \\ P(\ell-1) \neq P(r-1)}} \gcd(\ell-1, r-1)^\kappa .$$

Lemma 3.5. *Let a real z be sufficiently large. Then for $\kappa \geqslant 1$ we have*

$$D_\kappa \leqslant z^{\kappa+\alpha-\alpha\kappa+1+o(1)}.$$

Proof. Clearly for each pair of primes (ℓ, r) in the sum D_κ we have $\gcd(\ell-1, r-1) \leqslant (\ell-1)/P(\ell-1) \leqslant H$ for some integer $H \ll z^{1-\alpha}$. Hence

$$D_\kappa \leqslant \sum_{h=1}^{H} h^\kappa \sum_{\substack{\ell, r \in \mathscr{L}_z \\ P(\ell-1) \neq P(r-1) \\ \gcd(\ell-1, r-1) = h}} 1.$$

We estimate the inner sum trivially as $O\left((z/h)^2\right)$ and derive

$$D_\kappa \leqslant z^2 \sum_{h=1}^{H} h^{\kappa-2} \leqslant z^{2+o(1)} H^{\kappa-1} \leqslant z^{2+(\kappa-1)(1-\alpha)+o(1)},$$

and the desired result follows. □

4. Bounds of character sums

4.1. **Complete character sums with diagonal forms over finite fields.** Let q be an odd prime power and let $\mathbb{F}_q$ be the finite field of q elements. We note that for the purpose of proving Theorem 1.2, we only need to estimate the sums of this section over a prime finite field. However, since our proofs work over arbitrary finite fields, we present them in this more general setting with the hope they would be of independent interest.

We let $m \geqslant 1$ and $d \geqslant 2$ be integers with d coprime with q.

Let $\mathscr{X}$ denote the set of multiplicative characters of $\mathbb{F}_q^*$ and let $\mathscr{X}^* = \mathscr{X} \setminus \{\chi_0\}$ be the set of non-principal characters, we refer to [IwKo04, Chapter 3] for a background on characters. We also denote by $\eta \in \mathscr{X}^*$ the quadratic characters (that is $\eta^2 = \chi_0$).

We recall that the implied constant may depend on m (but not on d, q and other parameters).

We start with 'pure' bounds of sums of quadratic characters.

We note that in our next result we have an additional condition of d being an even integer.

Lemma 4.1. *Assume that the integer $d \geqslant 2$ satisfies $\gcd(d,q)=1$ and is even. Let $a_1,\ldots,a_m \in \mathbb{F}_q^*$. Then for*

$$S = \sum_{x_1,\ldots,x_m \in \mathbb{F}_q} \eta\left(a_1x_1^d + \cdots + a_mx_m^d\right)$$

we have

$$|S| \leqslant d^{m-1}(q-1)q^{(m-1)/2}.$$

Proof. The proof follows by induction on m. For $m=1$, since d is even, the sum becomes

$$\left|\sum_{x_1 \in \mathbb{F}_q} \eta\left(a_1x_1^d\right)\right| = q-1.$$

We assume the bound true for $m-1$ and we prove it for m. We have

$$S = \sum_{x_m \in \mathbb{F}_q^*} \sum_{x_1,\ldots,x_{m-1} \in \mathbb{F}_q} \eta\left(a_1x_1^d + \cdots + a_mx_m^d\right) \\ + \sum_{x_1,\ldots,x_{m-1} \in \mathbb{F}_q} \eta\left(a_1x_1^d + \cdots + a_{m-1}x_{m-1}^d\right).$$

By the induction hypothesis, the second sum in the above is bounded by $d^{m-2}(q-1)q^{(m-2)/2}$. Hence, we have

$$|S| \leqslant |S^*| + d^{m-2}(q-1)q^{(m-2)/2}, \tag{4.1}$$

where

$$S^* = \sum_{x_m \in \mathbb{F}_q^*} \sum_{x_1,\ldots,x_{m-1} \in \mathbb{F}_q} \eta\left(a_1x_1^d + \cdots + a_mx_m^d\right),$$

to which we apply a bound of Katz [Kat02, Theorem 2.2]. Indeed, since $x_m \neq 0$ in S^*, we make the transformation $x_i \to x_ix_m$, $i = 1,\ldots,m-1$, which does not change the sum. Moreover, since again d is even and $\eta(x_m^d)=1$, we obtain

$$\begin{aligned} S^* &= \sum_{x_m \in \mathbb{F}_q^*} \sum_{x_1,\ldots,x_{m-1} \in \mathbb{F}_q} \eta\left(a_1x_1^d + \cdots + a_{m-1}x_{m-1}^d + a_m\right) \\ &= (q-1) \sum_{x_1,\ldots,x_{m-1} \in \mathbb{F}_q} \eta\left(a_1x_1^d + \cdots + a_{m-1}x_{m-1}^d + a_m\right). \end{aligned} \tag{4.2}$$

Let now

$$F(X_1,\ldots,X_{m-1}) = a_1X_1^d + \cdots + a_{m-1}X_{m-1}^d + a_m \in \mathbb{F}_q[X_1,\ldots,X_{m-1}].$$

We note that the equation $F(X_1,\ldots,X_{m-1}) = 0$ defines a smooth hypersurface in the affine space $\mathbb{A}^{m-1}(\mathbb{F}_q)$. Indeed, considering the partial derivatives of F with respect to each variable X_i, we obtain that the only possible singular point would be $(0,\dots,0)$. However, since $a_m \neq 0$, this point does not belong to the hypersurface $F(X_1,\dots,X_{m-1}) = 0$.

Similarly, the equation given by the leading homogenous part of F, $a_1X_1^d + \cdots + a_{m-1}X_{m-1}^d = 0$, defines a smooth hypersurface in the projective space $\mathbb{P}^{m-2}(\mathbb{F}_q)$.

Applying now [Kat02, Theorem 2.2], we conclude from (4.2) that

$$|S^*| \leqslant (d-1)^{m-1}(q-1)q^{(m-1)/2}. \tag{4.3}$$

Substituting (4.3) in (4.1), we obtain

$$\begin{aligned} |S| &\leqslant (d-1)^{m-1}(q-1)q^{(m-1)/2} + d^{m-2}(q-1)q^{(m-2)/2} \\ &\leqslant d^{m-2}(q-1)q^{(m-2)/2}\left((d-1)q^{\frac{1}{2}}+1\right). \end{aligned}$$

Since $(d-1)q^{\frac{1}{2}}+1 < dq^{1/2}$, we conclude the proof. □

Next we need the following bound on multidimensional sum of quadratic characters, twisted by arbitrary characters. In the next result we do not use that d is even.

Lemma 4.2. *Assume that the integer $d \geqslant 2$ satisfies $\gcd(d,q)=1$. Let $a_1,\dots,a_m \in \mathbb{F}_q^*$. Then for any $\chi_1,\dots,\chi_m \in \mathscr{X}$ we have*

$$\sum_{x_1,\dots,x_m\in\mathbb{F}_q} \eta\left(a_1x_1^d+\cdots+a_mx_m^d\right)\chi_1(x_1)\dots\chi_m(x_m) \ll d^m q^{(m+1)/2}.$$

Proof. First we note that if each χ_i is equal to the principal character, then the result follows from Lemma 4.1. So, from now on, we assume that not all of the characters χ_i are equal to the principal character.

We have

$$\sum_{x_1,\dots,x_m\in\mathbb{F}_q} \eta\left(a_1x_1^d+\cdots+a_mx_m^d\right)\chi_1(x_1)\dots\chi_m(x_m) = S_1 - S_0, \tag{4.4}$$

where

$$S_0 = \sum_{x_1,\dots,x_m\in\mathbb{F}_q} \chi_1(x_1)\dots\chi_m(x_m)$$

and

$$S_1 = \sum_{y\in\mathbb{F}_q^*} \sum_{\substack{x_1,\dots,x_m\in\mathbb{F}_q \\ a_1x_1^d+\cdots+a_mx_m^d=y^2}} \chi_1(x_1)\dots\chi_m(x_m).$$

Indeed, we observe that each vector $(x_1,\dots,x_m) \in \mathbb{F}_q^m$ contributes $2\chi_1(x_1)\dots\chi_m(x_m)$ to the sum S_1. It is also easy to see that S_0 vanishes unless $\chi_1 = \ldots = \chi_m = \chi_0$; therefore, due to our assumption from above, we get that $S_0 = 0$. We now fix a nontrivial additive character ψ of $\mathbb{F}_q$. By the orthogonality relation,

$$\frac{1}{q}\sum_{\lambda\in\mathbb{F}_q}\psi(\lambda u) = \begin{cases}1, & \text{if } u=0,\\ 0, & \text{if } u\in\mathbb{F}_q^*,\end{cases}$$

see [IwKo04, Section 3.1]. Hence we write

$$\begin{aligned}S_1 = &\sum_{x_1,\ldots,x_m\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q^*}\\ &\qquad\frac{1}{q}\sum_{\lambda\in\mathbb{F}_q}\psi\left(\lambda\left(a_1x_1^d+\cdots+a_mx_m^d-y^2\right)\right)\chi_1(x_1)\ldots\chi_m(x_m)\\ &=\frac{1}{q}\sum_{\lambda\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q^*}\psi\left(-\lambda y^2\right)\\ &\qquad\sum_{x_1,\ldots,x_m\in\mathbb{F}_q}\psi\left(\lambda\left(a_1x_1^d+\cdots+a_mx_m^d\right)\right)\chi_1(x_1)\ldots\chi_m(x_m)\\ &=\frac{1}{q}\sum_{\lambda\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q^*}\psi\left(-\lambda y^2\right)\prod_{i=1}^{m}\sum_{x_i\in\mathbb{F}_q}\psi\left(\lambda a_ix_i^d\right)\chi_i(x_i).\end{aligned}$$

The contribution from the terms corresponding to $\lambda = 0$ is obviously equal to $\frac{q-1}{q}\cdot S_0 = 0$ since $S_0 = 0$ (because not all of the characters χ_i are equal to the principal character). Hence

$$S_1 = W, \tag{4.5}$$

where

$$W = \frac{1}{q}\sum_{\lambda\in\mathbb{F}_q^*}\sum_{y\in\mathbb{F}_q^*}\psi\left(-\lambda y^2\right)\prod_{i=1}^{m}\sum_{x_i\in\mathbb{F}_q}\psi\left(\lambda a_ix_i^d\right)\chi_i(x_i).$$

Now the sum over y differs from the classical Gauss sums by only one term corresponding to $y = 0$, and so we have

$$\sum_{y\in\mathbb{F}_q^*}\psi\left(-\lambda y^2\right) \ll q^{1/2}, \tag{4.6}$$

see [IwKo04, Theorem 3.4]. For the remaining sums, using that $\lambda a_i \in \mathbb{F}_q^*$ we apply the Weil bound [Wei74, Appendix 5, Example 12] of mixed sums of additive and multiplicative characters which implies

$$\sum_{x_i\in\mathbb{F}_q}\psi\left(\lambda a_ix_i^d\right)\chi_i(x_i) \ll dq^{1/2}, \tag{4.7}$$

see also [Li96, Chapter 6, Theorem 3]. Therefore, the bounds (4.6) and (4.7), combined together yield

$$W \ll d^m q^{(m+1)/2}.$$

and together with (4.4) and (4.5) we conclude the proof. □

We remark that some, or all, of the characters $\chi_1, \ldots, \chi_m \in \mathscr{X}$ can be principal and that the implied constant from the conclusion of Lemma 4.2 depends only on m.

4.2. **Incomplete character sums with exponential functions.** We now extend the definition of $\tau_\ell(g)$ to orders modulo any composite moduli q with $\gcd(g, q) = 1$. We also use (u/q) to denote the *Jacobi symbol* modulo an odd q.

Here we need to obtain multidimensional analogues of the result on character sums from [BaSh17, Section 3]. Although this does not require new ideas and can be achieved at the cost of merely typographical changes we present some short proofs of these results.

As usual, we write $\mathbf{e}(t) = \exp(2\pi i t)$ for all $t \in \mathbb{R}$.

We use the following variant of the result of [BaSh17, Lemma 3.1], which in turn is based on some ideas of Korobov [Kor70, Theorem 3].

Lemma 4.3. *Let* $a_1, b_1 \ldots, a_m, b_m \in \mathbb{Z}$ *and let* $\vartheta \in \mathbb{Z}$ *with* $\vartheta \geqslant 2$. *Let* ℓ *and* r *be distinct primes with*

$$t_\ell = \tau_\ell(\vartheta), \qquad t_r = \tau_r(\vartheta), \qquad t = \tau_{\ell r}(\vartheta)$$

and such that

$$\gcd(\ell r, a_1 \ldots a_m \vartheta) = \gcd(t_\ell, t_r) = 1.$$

We define integers $b_{i,\ell}$ *and* $b_{i,r}$ *by the conditions*

$$b_{i,\ell} t_r + b_{i,r} t_\ell \equiv b_i \pmod t, \qquad 0 \leqslant b_{i,\ell} < t_\ell, \quad 0 \leqslant b_{i,r} < t_r,$$

for $i = 1, \ldots, m$. *Then, for*

$$S = \sum_{k_1, \ldots, k_m = 1}^{t} \left(\frac{a_1 \vartheta^{k_1} + \ldots + a_m \vartheta^{k_m}}{\ell r} \right) \mathbf{e}\left(\frac{b_1 k_1 + \ldots + b_m k_m}{t} \right)$$

we have

$$S = S_\ell S_r$$

where

$$S_\ell = \sum_{x_1,\ldots,x_m=1}^{t_\ell} \left(\frac{a_1\vartheta^{x_1} + \ldots + a_m\vartheta^{x_m}}{\ell}\right) \mathbf{e}\left(\frac{b_{1,\ell}x_1 + \ldots + b_{m,\ell}x_m}{t_\ell}\right),$$

$$S_r = \sum_{y_1,\ldots,y_m=1}^{t_r} \left(\frac{a_1\vartheta^{y_1} + \ldots + a_m\vartheta^{y_m}}{r}\right) \mathbf{e}\left(\frac{b_{1,r}y_1 + \ldots + b_{m,r}y_m}{t_r}\right).$$

Proof. As in the proof of [BaSh17, Lemma 3.1], using that $\gcd(t_\ell, t_r) = 1$, we see that the integers

$$xt_r + yt_\ell, \qquad 0 \leqslant x < t_\ell, \qquad 0 \leqslant y < t_r,$$

run through the complete residue system modulo

$$t = t_\ell t_r.$$

Moreover,

$$\vartheta^{xt_r+yt_\ell} \equiv \vartheta^{xt_r} \pmod{\ell}, \qquad \vartheta^{xt_r+yt_\ell} \equiv \vartheta^{yt_\ell} \pmod{r}, \tag{4.8}$$

and

$$\mathbf{e}(b(xt_r + yt_\ell)/t) = \mathbf{e}(bx/t_\ell)\,\mathbf{e}(by/t_r). \tag{4.9}$$

Hence,

$$\begin{aligned} S = \sum_{x_1,\ldots,x_m=1}^{t_\ell} \sum_{y_1,\ldots,y_m=1}^{t_r} &\left(\frac{a_1\vartheta^{x_1t_r+y_1t_\ell} + \ldots + a_m\vartheta^{x_mt_r+y_mt_\ell}}{\ell r}\right) \\ &\mathbf{e}\left(\frac{b_1\left(x_1t_r + y_1t_\ell\right) + \ldots + b_m\left(x_mt_r + y_mt_\ell\right)}{t}\right). \end{aligned} \tag{4.10}$$

Using the multiplicativity of the Jacobi symbol, and recalling the congruences (4.8), we derive

$$\begin{aligned} &\left(\frac{a_1\vartheta^{x_1t_r+y_1t_\ell} + \ldots + a_m\vartheta^{x_mt_r+y_mt_\ell}}{\ell r}\right) \\ &\qquad = \left(\frac{a_1\vartheta^{x_1t_r+y_1t_\ell} + \ldots + a_m\vartheta^{x_mt_r+y_mt_\ell}}{\ell}\right) \\ &\qquad\qquad \left(\frac{a_1\vartheta^{x_1t_r+y_1t_\ell} + \ldots + a_m\vartheta^{x_mt_r+y_mt_\ell}}{r}\right) \\ &\qquad = \left(\frac{a_1\vartheta^{x_1t_r} + \ldots + a_m\vartheta^{x_mt_r}}{\ell}\right) \\ &\qquad\qquad \left(\frac{a_1\vartheta^{y_1t_\ell} + \ldots + a_m\vartheta^{y_mt_\ell}}{r}\right). \end{aligned} \tag{4.11}$$

Furthermore, by (4.9) we have

$$\begin{aligned}\mathbf{e}\left(\frac{b_1(x_1t_r+y_1t_\ell)+\ldots+b_m(x_mt_r+y_mt_\ell)}{t}\right)\\ =\mathbf{e}\left(\frac{b_1x_1+\ldots+b_mx_m}{t_\ell}\right)\mathbf{e}\left(\frac{b_1y_1+\ldots+b_mt_m}{t_r}\right).\end{aligned} \tag{4.12}$$

Using (4.11) and (4.12) in (4.10), we see that the sum S can be decomposed into a product of two sums as follows

$$\begin{aligned}S=\sum_{x_1,\ldots,x_m=1}^{t_\ell}\left(\frac{a_1\vartheta^{x_1t_r}+\ldots+a_m\vartheta^{x_mt_r}}{\ell}\right)\mathbf{e}\left(\frac{b_1x_1+\ldots+b_mx_m}{t_\ell}\right)\\ \sum_{y_1,\ldots,y_m=1}^{t_r}\left(\frac{a_1\vartheta^{y_1t_\ell}+\ldots+a_m\vartheta^{y_mt_\ell}}{r}\right)\mathbf{e}\left(\frac{b_1y_1+\ldots+b_mt_m}{t_r}\right).\end{aligned}$$

We now replace x_i with $x_it_r^{-1} \pmod{t_\ell}$ and y_i with $y_it_\ell^{-1} \pmod{t_r}$, and take into account that

$$b_it_r^{-1}\equiv b_{i,\ell}\pmod{t_\ell}\qquad\text{and}\qquad b_it_\ell^{-1}\equiv b_{i,r}\pmod{t_r},$$

for $i=1,\ldots,m$. This concludes the proof. □

Next we estimate the sums S_ℓ and S_r which appear in Lemma 4.3. Namely we now establish an analogue of [BaSh17, Lemma 3.2].

Lemma 4.4. *Let $a_1,b_1\ldots,a_m,b_m\in\mathbb{Z}$ and let $\vartheta\in\mathbb{Z}$ with $\vartheta\geqslant 2$. Let ℓ be a prime with*

$$t_\ell=\tau_\ell(\vartheta)$$

and such that

$$\gcd(\ell,a_1\ldots a_m\vartheta)=1\qquad\textit{and}\qquad\gcd(t_\ell,2)=1.$$

Then for

$$S_\ell=\sum_{x_1,\ldots,x_m=1}^{t_\ell}\left(\frac{a_1\vartheta^{x_1}+\ldots+a_m\vartheta^{x_m}}{\ell}\right)\mathbf{e}\left(\frac{b_1x_1+\ldots+b_mx_m}{t_\ell}\right)$$

we have

$$S_\ell\ll\begin{cases}\ell^{(m+1)/2}, & \textit{for arbitrary } b_1,\ldots,b_m,\\ t_\ell\ell^{(m-1)/2}, & \textit{for } b_1=\ldots=b_m=0.\end{cases}$$

Proof. Denoting $d = (\ell-1)/t_\ell$, we can write $\vartheta = \rho^d$ with *some* primitive root ρ modulo ℓ. Then,

$$\begin{aligned} S_\ell &= \frac{1}{d^m} \sum_{x_1,\ldots,x_m=1}^{\ell-1} \left(\frac{a_1\rho^{dx_1} + \ldots + a_m\rho^{dx_m}}{\ell}\right) \\ &\qquad \mathbf{e}\left(\frac{d\left(b_1x_1 + \ldots + b_mx_m\right)}{\ell-1}\right) \qquad (4.13) \\ &= \frac{1}{d^m} \sum_{w_1,\ldots,w_m=1}^{\ell-1} \left(\frac{a_1w_1^d + \ldots + a_mw_m^d}{\ell}\right) \chi_1(w_1)\ldots\chi_m(w_m), \end{aligned}$$

where for $w \in \mathbb{F}_\ell$ we define χ_i by

$$\chi_i(w) = \mathbf{e}\left(b_i dx/(\ell-1)\right), \qquad i = 1,\ldots,m,$$

where x is any integer for which $w \equiv \rho^x \pmod \ell$.

As in the proof of [BaSh17, Lemma 3.2] we observe χ_i is a multiplicative character of $\mathbb{F}_\ell$ for each $i = 1,\ldots,m$. Recalling Lemma 4.2, we derive from (4.13)

$$S_\ell \ll \frac{1}{d^m} d^m \ell^{(m+1)/2} = \ell^{(m+1)/2},$$

which establishes the desired bound for arbitrary $b_1,\ldots,b_m \in \mathbb{Z}$.

For $b_1 = \ldots = b_m = 0$ we observe that since t_ℓ is odd, d is even and hence we can use Lemma 4.1 instead of Lemma 4.2. Thus in this case (4.13) implies

$$S_\ell \ll \frac{1}{d^m} d^{m-1} \ell^{(m+1)/2} = \frac{1}{d} \ell^{(m+1)/2} \ll t_\ell \ell^{(m-1)/2},$$

which concludes the proof. □

Lemmas 4.3 and 4.4 combined together imply the following bound.

Corollary 4.5. *Let $a_1, b_1 \ldots, a_m, b_m \in \mathbb{Z}$ and let $\vartheta \in \mathbb{Z}$ with $\vartheta \geqslant 2$. Let ℓ and r be distinct primes with*

$$t_\ell = \tau_\ell(\vartheta), \qquad t_r = \tau_r(\vartheta), \qquad t = \tau_{\ell r}(\vartheta)$$

and such that

$$\gcd\left(\ell r, a_1\ldots a_m\vartheta\right) = \gcd\left(t_\ell, t_r\right) = \gcd(t_\ell t_r, 2) = 1.$$

Then, for

$$S = \sum_{k_1,\ldots,k_m=1}^{t} \left(\frac{a_1\vartheta^{k_1} + \ldots + a_m\vartheta^{k_m}}{\ell r}\right) \mathbf{e}\left(\frac{b_1k_1 + \ldots + b_mk_m}{t}\right)$$

we have

$$S \ll \begin{cases} (\ell r)^{(m+1)/2}, & \text{for arbitrary } b_1, \ldots, b_m, \\ t(\ell r)^{(m-1)/2}, & \text{for } b_1 = \ldots = b_m = 0. \end{cases}$$

Clearly in Lemma 4.4 and Corollary 4.5 the parity condition on multiplicative orders is important only in the case where $b_1 = \ldots = b_m = 0$, as only these parts appeal to Lemma 4.1 (which required d to be even).

Combining Corollary 4.5 with the completing method, see [IwKo04, Section 12.2], we derive an analogue of [BaSh17, Lemma 3.4], which is our main technical tool.

Lemma 4.6. *Let $a_1, \ldots, a_m \in \mathbb{Z}$ and let $\vartheta \in \mathbb{Z}$ with $\vartheta \geqslant 2$. Let ℓ and r be distinct primes with*

$$\gcd(\ell r, a_1 \ldots a_m \vartheta) = \gcd(\tau_\ell(\vartheta), \tau_r(\vartheta)) = \gcd(\tau_\ell(\vartheta)\tau_r(\vartheta), 2) = 1.$$

Then, for any integers $L_1, \ldots L_m \geqslant 1$, we have

$$\sum_{k_1=1}^{L_1} \cdots \sum_{k_m=1}^{L_m} \left(\frac{a_1 \vartheta^{k_1} + \ldots + a_m \vartheta^{k_m}}{\ell r} \right) \\ \ll L_1 \ldots L_m t^{-m+1} (\ell r)^{(m-1)/2} \\ + \left(L^{m-1} t^{-m+1} + 1 \right) (\ell r)^{(m+1)/2} (\log(\ell r))^m ,$$

where

$$L = \max\{L_1, \ldots L_m\} \qquad \text{and} \qquad t = \tau_{\ell r}(\vartheta),$$

and the implied constant is absolute.

Proof. Clearly we can split the above sum into $\lfloor L_1/t \rfloor \cdot \cdots \cdot \lfloor L_m/t \rfloor$ complete sums, where each variable runs over the complete residue system modulo t and into at most $O\left((L/t)^{m-1} + 1\right)$ incomplete sums over a complete residue system modulo ℓr.

By Corollary 4.5 each of these complete sums can be estimated as $O\left(t(\ell r)^{(m-1)/2}\right)$, so they contribute $O\left(L_1 \ldots L_m t^{-m+1} (\ell r)^{(m-1)/2}\right)$ in total.

By the standard completing techniques, see, for example, [IwKo04, Section 12.2], we derive from Corollary 4.5 that each incomplete sum can be estimated as $O\left((\ell r)^{(m+1)/2} (\log(\ell r))^m\right)$. Therefore, in total they contribute $O\left(\left(L^{m-1} t^{-m+1} + 1\right) (\ell r)^{(m+1)/2} (\log(\ell r))^m\right)$.

Combining both contributions together, we conclude the proof. □

5. Proof of Theorem 1.2

5.1. **Preliminary transformations.** We can always assume that

$$k_m \geqslant \ldots \geqslant k_1.$$

We note that there is an integer constant h_0 depending only on the initial data such that if $k_m \geqslant k_{m-1} + h_0$ then

$$n^2 = \sum_{i=1}^{m} c_i g^{k_i} \geqslant 0.5 g^{k_m}$$

and hence for some

$$K \ll \log N \tag{5.1}$$

we have

$$k_m = \max\{k_1, \ldots, k_m\} \ll K. \tag{5.2}$$

On the other hand, for $k_m < k_{m-1} + h_0$, writing $k_m = k_{m-1} + h$, $h = 0, \ldots, h_0 - 1$ and

$$n^2 = \sum_{i=1}^{m} c_i g^{k_i} = \sum_{i=1}^{m-2} c_i g^{k_i} + (c_{m-1} + c_m g^h) g^{k_{m-1}}$$

by Theorem 1.1 we obtain at most $O\left((\log N)^{m-1}\right)$ solutions $n \leqslant N$.

Hence we now estimate the number of solutions to (1.4) with (5.2) (for K as in (5.1)).

We recall the notation (3.3) and (3.5), and we write (1.4) as

$$n^2 = F(\mathbf{k}). \tag{5.3}$$

We also recall the definitions of the set $\mathscr{L}_z$ in Section 3.2 and of $\omega_z(n)$ from Section 3.3.

To simplify the exposition everywhere below we replace logarithmic, and double logarithmic factors of z with $z^{o(1)}$ (implicitly assuming that $z \to \infty$). In particular we simply write

$$\#\mathscr{L}_z = z^{1+o(1)}. \tag{5.4}$$

Since $z^{o(1)}$ also absorbs all implied constants, we use $\leqslant$ instead of $\ll$ in the corresponding bounds.

5.2. **Sieving.** Note that if $F(\mathbf{k})$ is a perfect square, then we always have

$$\sum_{\ell \in \mathscr{L}_z} \left(\frac{F(\mathbf{k})}{\ell}\right) = \#\mathscr{L}_z - \omega_z\left(F(\mathbf{k})\right).$$

Hence

$$\#\mathscr{L}_z \leqslant \left| \sum_{\ell \in \mathscr{L}_z} \left(\frac{F(\mathbf{k})}{\ell}\right) \right| + \omega_z\left(F(\mathbf{k})\right).$$

Denote by $\mathscr{M}$ the set of values of $\mathbf{k} \in \mathscr{K}$ satisfying (5.3) and let $M = \#\mathscr{M}$ be its cardinality. Invoking Lemma 3.3, we obtain

$$\begin{aligned} M\#\mathscr{L}_z &\leqslant \sum_{\mathbf{k}\in\mathscr{M}} \left| \sum_{\ell\in\mathscr{L}_z} \left(\frac{F(\mathbf{k})}{\ell}\right) \right| + \sum_{\mathbf{k}\in\mathscr{M}} \omega_z\left(F(\mathbf{k})\right) \\ &\leqslant \sum_{\mathbf{k}\in\mathscr{M}} \left| \sum_{\ell\in\mathscr{L}_z} \left(\frac{F(\mathbf{k})}{\ell}\right) \right| + \sum_{\mathbf{k}\in\mathscr{K}} \omega_z\left(F(\mathbf{k})\right) \\ &\ll \sum_{\mathbf{k}\in\mathscr{M}} \left| \sum_{\ell\in\mathscr{L}_z} \left(\frac{F(\mathbf{k})}{\ell}\right) \right| + \left(K^m z^{-\alpha} + K^{m-1}\right) \#\mathscr{L}_z. \end{aligned}$$

Therefore either

$$M\#\mathscr{L}_z \ll \sum_{\mathbf{k}\in\mathscr{M}} \left| \sum_{\ell\in\mathscr{L}_z} \left(\frac{F(\mathbf{k})}{\ell}\right) \right| \tag{5.5}$$

or

$$M \ll K^m z^{-\alpha} + K^{m-1}. \tag{5.6}$$

Assuming that (5.5) holds, by the Cauchy inequality

$$\left(M\#\mathscr{L}_z\right)^2 \leqslant M \sum_{\mathbf{k}\in\mathscr{M}} \left| \sum_{\ell\in\mathscr{L}_z} \left(\frac{F(\mathbf{k})}{\ell}\right) \right|^2$$

and extending summation back to all $\mathbf{k} \in \mathscr{K}$ and using (5.4), we obtain

$$M \leqslant z^{-2+o(1)} W, \tag{5.7}$$

where

$$W = \sum_{\mathbf{k}\in\mathscr{K}} \left| \sum_{\ell\in\mathscr{L}_z} \left(\frac{F(\mathbf{k})}{\ell}\right) \right|^2 = \sum_{\mathbf{k}\in\mathscr{K}} \sum_{\ell,r\in\mathscr{L}_z} \left(\frac{F(\mathbf{k})}{\ell r}\right).$$

Combining (5.6) and (5.7), we see that in any case we have

$$M \leqslant \left(K^m z^{-\alpha} + K^{m-1} + z^{-2} W\right) z^{o(1)}. \tag{5.8}$$

We further split the sum W into two sums as $W = U + V$, where

$$\begin{aligned} U &= \sum_{\substack{\ell,r\in\mathscr{L}_z \\ P(\ell-1)=P(r-1)}} \sum_{\mathbf{k}\in\mathscr{K}} \left(\frac{F(\mathbf{k})}{\ell r}\right), \\ V &= \sum_{\substack{\ell,r\in\mathscr{L}_z \\ P(\ell-1)\neq P(r-1)}} \sum_{\mathbf{k}\in\mathscr{K}} \left(\frac{F(\mathbf{k})}{\ell r}\right). \end{aligned} \tag{5.9}$$

To estimate U (which also includes the diagonal case $\ell = r$), we use the trivial bound $(K+1)^m$ on each inner sum, deriving that

$$\begin{aligned} U &\leqslant (K+1)^m \sum_{\substack{\ell, r \in \mathscr{L}_z \\ P(\ell-1)=P(r-1)}} 1 \\ &\leqslant (K+1)^m \sum_{d \geqslant z^\alpha} \sum_{\substack{\ell, r \in \mathscr{L}_z \\ \ell \equiv r \equiv 1 \bmod d}} 1 \ll K^m \sum_{d \geqslant z^\alpha} \frac{z^2}{d^2} \ll K^m z^{2-\alpha}. \end{aligned}$$

Hence we can write (5.8) as

$$M \leqslant \left(K^m z^{-\alpha} + K^{m-1} + z^{-2} V\right) z^{o(1)}. \tag{5.10}$$

5.3. **Bounds of character sums.** To estimate V, we first observe that for every $\ell \in \mathscr{L}_z$ the inequality $\tau_\ell(g) \geqslant P(\ell-1) \geqslant \ell^\alpha$ implies (since $\alpha > \frac{1}{2}$) that $P(\ell-1) \mid \tau_\ell(g)$.

Fix a pair $(\ell, r) \in \mathscr{L}_z \times \mathscr{L}_z$ with $P(\ell-1) \neq P(r-1)$ and define

$$h = \gcd\left(\tau_\ell(g), \tau_r(g)\right) \qquad \text{and} \qquad \vartheta = g^h.$$

We observe that

$$\tau_\ell(\vartheta) = \tau_\ell(g)/h \qquad \text{and} \qquad \tau_r(\vartheta) = \tau_r(g)/h.$$

Furthermore, due to our choice of the set $\mathscr{L}_z$ in Section 3.2 we have

$$\nu_2(\tau_\ell(g)) = \nu_2(\tau_r(g)) = \nu_2(h)$$

and hence both $\tau_\ell(\vartheta)$ and $\tau_r(\vartheta)$ are odd.

We now write

$$\sum_{\mathbf{k} \in \mathscr{K}} \left(\frac{F(\mathbf{k})}{\ell r}\right) = \sum_{j_1, \ldots, j_m = 1}^{h} T_{\ell, r}\left(j_1, \ldots, j_m\right), \tag{5.11}$$

where

$$\begin{aligned} T_{\ell, r}\left(j_1, \ldots, j_m\right) &= \sum_{1 \leqslant k_1 \leqslant (K-j_1)/h} \\ &\qquad \ldots \sum_{1 \leqslant k_m \leqslant (K-j_m)/h} \left(\frac{c_1 g^{k_1 h + j_1} + \ldots + c_m g^{k_m h + j_m}}{\ell r}\right) \\ &= \sum_{1 \leqslant k_1 \leqslant (K-j_1)/h} \\ &\qquad \ldots \sum_{1 \leqslant k_m \leqslant (K-j_m)/h} \left(\frac{c_1 g^{j_1} \vartheta^{k_1} + \ldots + c_m g^{j_m} \vartheta^{k_m}}{\ell r}\right). \end{aligned}$$

We can certainly assume that z is large enough so that

$$\gcd(c_1 \cdots c_m, \ell r) = 1$$

for $\ell, r \in \mathscr{L}_z$. Therefore Lemma 4.6 applies to $T_{\ell,r}(j_1, \ldots, j_m)$ and implies

$$\begin{aligned} T_{\ell,r}(j_1, \ldots, j_m) \\ \ll (K/h)^m \left(\tau_\ell(\vartheta)\tau_r(\vartheta)\right)^{-m+1} (\ell r)^{(m-1)/2} \\ + \left((K/h)^{m-1} \left(\tau_\ell(\vartheta)\tau_r(\vartheta)\right)^{-m+1} + 1\right) (\ell r)^{(m+1)/2} \left(\log(\ell r)\right)^m. \end{aligned}$$

Using

$$\tau_\ell(\vartheta)\tau_r(\vartheta) \gg z^{2\alpha} \qquad \text{and} \qquad \ell r \ll z^2$$

we see that

$$\begin{aligned} T_{\ell,r}(j_1, \ldots, j_m) \\ \leqslant \left((K/h)^m z^{(m-1)(1-2\alpha)} + \left((K/h)^{m-1} z^{(m-1)(1-2\alpha)+2} + z^{m+1}\right)\right) z^{o(1)}. \end{aligned}$$

Therefore, after the substitution in (5.11) we obtain

$$\begin{aligned} \left| \sum_{\mathbf{k} \in \mathscr{K}} \left(\frac{F(\mathbf{k})}{\ell r} \right) \right| \\ \leqslant \left(K^m z^{(m-1)(1-2\alpha)} + K^{m-1} h z^{(m-1)(1-2\alpha)+2} + h^m z^{m+1}\right) z^{o(1)}. \end{aligned}$$

Since obviously $h \leqslant \gcd(\ell - 1, r - 1)$, from the definition of V in (5.9) and using (5.4), we now derive

$$V \leqslant \left(K^m z^{(m-1)(1-2\alpha)} + D_1 K^{m-1} z^{(m-1)(1-2\alpha)} + D_m z^{m-1}\right) z^{2+o(1)},$$

where D_1 and D_m are as in Lemma 3.5 and thus we get

$$D_1 \leqslant z^{2+o(1)} \qquad \text{and} \qquad D_m \leqslant z^{m+\alpha-\alpha m+1+o(1)}.$$

Therefore

$$V \leqslant \left(K^m z^{(m-1)(1-2\alpha)} + K^{m-1} z^{(m-1)(1-2\alpha)+2} + z^{2m+\alpha-\alpha m}\right) z^{2+o(1)}.$$

which after the substitution in (5.10) yields

$$\begin{aligned} M \leqslant (K^m z^{-\alpha} + K^{m-1} + K^m z^{(m-1)(1-2\alpha)} \\ + K^{m-1} z^{(m-1)(1-2\alpha)+2} + z^{2m+\alpha-\alpha m}) z^{o(1)}. \end{aligned}$$

5.4. **Optimisation.** Clearly we can assume that

$$z \leqslant K^{1/(2-\alpha)} \tag{5.12}$$

as otherwise the last term $z^{2m+\alpha-\alpha m}$ exceeds the trivial bound K^m. Furthermore, for $m \geqslant 3$ and α as in (3.2), we have

$$(m-1)(2\alpha-1) > \alpha \tag{5.13}$$

and hence (using that $z^{(m-1)(1-2\alpha)} < z^{-\alpha}$ due to the inequality (5.13)), we can simplify the above bound as follows:

$$M \leqslant \left(K^m z^{-\alpha} + K^{m-1} + K^{m-1} z^{2-(m-1)(2\alpha-1)} + z^{2m+\alpha-\alpha m}\right) z^{o(1)}.$$

Moreover, since we have (5.12) and $\alpha < 1$, we see that

$$K^m z^{-\alpha} > K^{m-1}$$

which means that

$$M \leqslant \left(K^m z^{-\alpha} + K^{m-1} z^{2-(m-1)(2\alpha-1)} + z^{2m+\alpha-\alpha m}\right) z^{o(1)}. \tag{5.14}$$

First we note that for $m \geqslant 5$, with our choice of $\alpha = 0.677$ in (3.2) along with our assumption (5.12), we have that

$$K^m z^{-\alpha} > K^{m-1} z^{2-(m-1)(2\alpha-1)}$$

and thus the second term in (5.14) never dominates and we choose

$$z = K^{m/(2m+2\alpha-\alpha m)}$$

to balance the first and the third terms. Hence for if $m \geqslant 5$, we obtain:

$$M \leqslant K^{m-m\alpha/(2m+2\alpha-\alpha m)+o(1)}. \tag{5.15}$$

For $m = 4$ and with (3.2), direct calculations show that as for $m \geqslant 5$, it is better to balance the first and the third terms in (5.14) (rather than the first and the second terms), hence (5.15) also holds for $m = 4$.

Finally, for $m = 3$ one checks that balancing the first and the second terms in (5.14) with $z = K^{1/(4-3\alpha)}$ leads to an optimal result

$$M \leqslant \left(K^{3-\alpha/(4-3\alpha)} + K^{(6-2\alpha)/(4-3\alpha)}\right) K^{o(1)} \leqslant K^{3-\alpha/(4-3\alpha)+o(1)},$$

which concludes the proof (see also (5.1)).

6. Comments

The proof of Theorem 1.2, depends on the bound

$$\sum_{\mathbf{k} \in \mathscr{K}} \omega_z\left(F(\mathbf{k})\right) \leqslant \sum_{\ell \in \mathscr{L}_z} T_m(K, \ell),$$

where $T_m(K, \ell)$ is the number of solutions to the congruence

$$F(\mathbf{k}) \equiv 0 \pmod{\ell}, \qquad \mathbf{k} \in \mathscr{K}_m(K),$$

where $\mathscr{K}_m(K)$ is given by (3.4), see the proof of Lemma 3.3. In fact, in the proof of Lemma 3.3 we use the trivial bound

$$T_m(K,\ell) \leqslant (K+1)^{m-1}\left(\frac{K+1}{\tau_\ell(g)}+1\right) \ll K^m z^{-\alpha} + K^{m-1}, \tag{6.1}$$

which holds for any $\ell \in \mathscr{L}_z$ and is the best possible for $m = 2$. For $m \geqslant 3$ we get a better bound using exponential sum. This does not improve our final result, however since it can be of independent interest and since it maybe becomes important if better bounds of W in (5.7) become available (or maybe with some other modifications of the argument) we present such a better bound in Appendix A, see Lemma A.2.

The method of the proof of Theorem 1.2 also works for relations of the form

$$n^2 = \sum_{i=1}^{m} c_i g_i^{k_i},$$

with integer coefficients $c_1, \ldots, c_m$ of the same sign and arbitrary integer bases $g_1, \ldots, g_m \geqslant 2$. Indeed, in this case we still have a bound $O(\log N)$ on the exponents $k_1, \ldots, k_m$, which is important for our method. It is an interesting open question to establish such a bound for arbitrary $c_1, \ldots, c_m$. Similarly, our method can also be used to estimate the number of $n \leqslant N$ which can be represented as

$$n^2 = u_1 + \ldots + u_m$$

for some $\mathscr{S}$*-units* $u_1, \ldots, u_m$, that is, as a sum of m integers which have all their prime factors from a prescribed finite set of primes $\mathscr{S}$. Again, if negative values of $u_1, \ldots, u_m$ are allowed then some additional arguments are needed to bound the powers of primes in each $\mathscr{S}$-unit.

Furthermore, as in [BaSh17] we observe that under the Generalised Riemann Hypothesis we can obtain a slightly larger value of γ_m. We now recall that p is called a *Sophie Germain prime* if p and $2p+1$ are both prime. Under the assumption of the existence of the expected number of Sophie Germain primes in intervals, or in fact of just $z^{1+o(1)}$ such primes up to z, we can choose a set $\mathscr{L}_z$ in the argument of the proof of Theorem 1.2 with any $\alpha < 1$ and we see that under this assumption we can take $\gamma_m = m/(m+2)$ for $m \geqslant 3$.

Finally, we note that other perfect powers n^ν for a fixed $\nu = 3, 4, \ldots,$ can be investigated by our method. However, one needs a version of a result of Baker and Harman [BaHa98] for primes ℓ in the arithmetic progression $\ell \equiv 1 \pmod{\nu}$, so that there are multiplicative characters modulo ℓ of order ν.

Appendix A. Congruences with exponential functions

First we recall the following special case of a classical result of Korobov [Kor72, Lemma 2].

Lemma A.1. *Let $a \in \mathbb{Z}$ and let $\vartheta \in \mathbb{Z}$ with $\vartheta \geqslant 2$. Let ℓ be a prime with*

$$t = \tau_\ell(\vartheta),$$

and such that

$$\gcd(\ell, a\vartheta) = 1.$$

Then, we have

$$\left| \sum_{k=1}^{t} \mathbf{e}\left(a\vartheta^k/t\right) \right| \leqslant \ell^{1/2}.$$

We now have a bound on $T_m(K, \ell)$ which improves (6.1) in some ranges.

Lemma A.2. *Let $m \geqslant 3$. Then for $K \geqslant z$ and $\ell \in \mathscr{L}_z$, where $\mathscr{L}_z$ is as in Section 3.2, we have*

$$T_m(K, \ell) \ll K^m z^{-1} + K^m z^{m/2-\alpha(m-1)-1}.$$

Proof. Let $t = \tau_\ell(g)$; then since $\ell \in \mathscr{L}_z$, we know that $t \geqslant z^\alpha$. We also let

$$T_m(\ell) = T_m(t-1, \ell).$$

First we observe that $K \geqslant z \gg t$ and thus

$$T_m(K, \ell) \leqslant \left(\frac{K+1}{t} + 1\right)^m T_m(\ell) \ll K^m t^{-m} T_m(\ell). \tag{A.1}$$

Now, using the orthogonality of exponential functions, we write

$$T_m(\ell) = \frac{1}{\ell} \sum_{\mathbf{k} \in \mathscr{K}_m(t-1)} \sum_{a=0}^{\ell-1} \mathbf{e}\left(aF(\mathbf{k})/\ell\right),$$

where $\mathscr{K}_m(t-1)$ consists of all m-tuples $(k_1, \ldots, k_m)$ of non-negative integers $k_i < t$. Now changing the order of summation, we obtain

$$T_m(\ell) = \frac{1}{\ell} \sum_{a=0}^{\ell-1} \sum_{\mathbf{k} \in \mathscr{K}_m(t-1)} \mathbf{e}\left(aF(\mathbf{k})/\ell\right) = \frac{1}{\ell} \sum_{a=0}^{\ell-1} \prod_{i=1}^{m} \sum_{k_i=0}^{t-1} \mathbf{e}\left(ac_i g^{k_i}/\ell\right).$$

The term corresponding to $a = 0$ is equal to t^m/ℓ. We can assume that z is large enough (as otherwise the bound is trivial) so that $\gcd(c_1 \cdots c_m, \ell) = 1$ for $\ell \in \mathscr{L}_z$. We apply now the bound of Lemma A.1 to $m-2$ sums over $k_3, \ldots, k_m$ and derive

$$T_m(\ell) \leqslant t^m/\ell + \ell^{(m-2)/2} \frac{1}{\ell} R, \tag{A.2}$$

where

$$R = \sum_{a=0}^{\ell-1} \left| \sum_{k_1=0}^{t-1} \mathbf{e}\left(ac_1 g^{k_1}/\ell\right) \right| \cdot \left| \sum_{k_2=0}^{t-1} \mathbf{e}\left(ac_2 g^{k_2}/\ell\right) \right|$$

(note that after an application of Lemma A.1 we have added the term corresponding to $a = 0$ back to the sum). By the Cauchy inequality

$$R^2 \leqslant \left(\sum_{a=0}^{\ell-1} \left| \sum_{k_1=0}^{t-1} \mathbf{e}\left(ac_1 g^{k_1}/\ell\right) \right|^2 \right) \cdot \left(\sum_{a=0}^{\ell-1} \left| \sum_{k_2=0}^{t-1} \mathbf{e}\left(ac_2 g^{k_2}/\ell\right) \right|^2 \right).$$

Using the orthogonality of exponential functions again, we derive

$$\sum_{a=0}^{\ell-1} \left| \sum_{k_1=0}^{t-1} \mathbf{e}\left(ac_1 g^{k_1}/\ell\right) \right|^2 = \ell t$$

and similarly for the sum over k_2. Hence $R \leqslant \ell t$, and after substitution in (A.2) we derive

$$T_m(\ell) \leqslant t^m/\ell + \ell^{(m-2)/2} t,$$

which together with the inequality (A.1) and the fact that $t \geqslant z^\alpha$ concludes the proof. □

Acknowledgements

D. G. and S. S. were partially supported by a Discovery Grant from NSERC, A. O. by ARC Grants DP180100201 and DP200100355, and I. S. by an ARC Grant DP200100355.

References

[BaHa98] R. C. Baker and G. Harman, 'Shifted primes without large prime factors', *Acta Arith.*, **83** (1998), 331–361. 2, 4, 10, 25

[BaSh17] W. D. Banks and I. E. Shparlinski, 'On coincidences among quadratic fields generated by the Shanks sequence', *Quart. J Math.*, **68** (2017), 465–484. 4, 15, 16, 17, 18, 19, 25

[BGT16] J. P. Bell, D. Ghioca and T. J. Tucker, 'The dynamical Mordell-Lang conjecture', *Mathematical Surveys and Monographs* **210**, American Mathematical Society, Providence, RI, 2016. xiii+280 pp. 1

[BeBu14] M. A. Bennett and Y. Bugeaud, 'Perfect powers with three digits', *Mathematika*, **60** (2014), 66–84. 4

[BBM13] M. A. Bennett, Y. Bugeaud and M. Mignotte, 'Perfect powers with few binary digits and related Diophantine problems', *Ann. Sc. Norm. Super. Pisa Cl. Sci.*, **12** (2013), 941–953. 4

[CGSZ] P. Corvaja, D. Ghioca, T. Scanlon and U. Zannier, 'The Dynamical Mordell-Lang Conjecture for endomorphisms of semiabelian varieties defined over fields of positive characteristic', *J. Inst. Math. Jussieu*, 30 pp. (2019), to appear. 3

[CoZa13] P. Corvaja and U. Zannier, 'Finiteness of odd perfect powers with four nonzero binary digits', *Ann. Inst. Fourier (Grenoble)*, **63** (2013), 715–731. 3, 4

[ErMu96] P. Erdős and M. R. Murty, 'On the order of $a \pmod p$', *Number theory (Ottawa, ON, 1996)*, CRM Proc. Lecture Notes, **19**, Amer. Math. Soc., Providence, RI, 1999, 87–97, 9

[GOSS21] D. Ghioca, A. Ostafe, S. Saleh and I. E. Shparlinski, 'A sparsity result for the Dynamical Mordell-Lang Conjecture in positive characteristic', *Bull. Aust. Math. Soc.*, 2021, 8 pp., to appear. 1, 2

[H-B84] D. R. Heath-Brown, 'The square sieve and consecutive square-free numbers', *Math. Ann.*, **266** (1984), 251–259. 2, 3

[IwKo04] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004. 9, 11, 14, 19

[Kat02] N. Katz, 'Estimates for nonsingular multiplicative character sums', *Int. Math. Res. Not.*, **7** (2002), 333–349. 2, 12, 13

[Kea69] M. Keates, 'On the greatest prime factor of a polynomial, *Proc. Edinburgh Math. Soc.*, **16** (1969), 301–303. 3

[Kor70] N. M. Korobov, 'Trigonometric sums with exponential functions, and the distribution of the digits in periodic fractions', *Mat. Zametki*, **8** (1970) 641–652 (in Russian); Translation in English: *Mathem. Notes*, **8** (1970), 831–837. 15

[Kor72] N. Korobov, 'On the distribution of digits in periodic fractions', *Matem. Sbornik*, **89** (1972), 654–670; translation in English: *Mathem. USSR Sbornik*, **18** (1972), 659–676. 26

[KuPo05] P. Kurlberg and C. Pomerance, 'On the period of the linear congruential and power generators', *Acta Arith.*, **119** (2005), 149–169. 9

[Lau84] M. Laurent, 'Équations diophantiennes exponentielles', *Invent. Math.*, **78** (1984), 299–327. 2

[Li96] W.-C. W. Li, *Number theory with applications*, World Scientific, Singapore, 1996. 15

[LuSh09] F. Luca and I. E. Shparlinski, 'On quadratic fields generated by the Shanks sequence', *Proc. Edinb. Math. Soc.*, **52** (2009), 719–729. 4, 9

[Mos21] A. Moscariello, 'On sparse perfect powers', *Preprint*, 2021 (available from http://arxiv.org/abs/2101.10415). 4

[Wei74] A. Weil, *Basic number theory*, Springer-Verlag, New York, 1974. 14

Dragos Ghioca, Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada

E-mail address: dghioca@math.ubc.ca

Alina Ostafe, School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia
E-mail address: alina.ostafe@unsw.edu.au

Sina Saleh, Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada
E-mail address: sinas@math.ubc.ca

Igor E. Shparlinski, School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia
E-mail address: igor.shparlinski@unsw.edu.au