J. Inst. Math. Jussieu (2025), **24**(5), 1765–1806
doi:10.1017/S1474748023000397

ENERGY BOUNDS FOR MODULAR ROOTS AND THEIR APPLICATIONS

BRYCE KERR[1,2], ILYA D. SHKREDOV[3], IGOR E. SHPARLINSKI[4] AND ALEXANDRU ZAHARESCU[5]

[1] *Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany*
[2] *School of Science, University of New South Wales, Canberra, ACT 2600, Australia*
(bryce.kerr89@gmail.com)
[3] *London Istitute for Mathematical Sciences, 21 Albemarle St., London W1S 4BS, UK*
(ilya.shkredov@gmail.com)
[4] *School of Mathematics and Statistics, University of New South Wales. Sydney, NSW 2052, Australia*
(igor.shparlinski@unsw.edu.au)
[5] *Department of Mathematics, University of Illinois at Urbana-Champaign 1409 West Green Street, Urbana, IL 61801, USA and Simon Stoilow Institute of Mathematics of the Romanian Academy, P.O. Box 1-764, RO-014700 Bucharest, Romania*
(zaharesc@illinois.edu)

(Received 28 January 2022; revised 9 October 2023; accepted 9 October 2023; first published online 4 March 2024)

Abstract We generalise and improve some recent bounds for additive energies of modular roots. Our arguments use a variety of techniques, including those from additive combinatorics, algebraic number theory and the geometry of numbers. We give applications of these results to new bounds on correlations between *Salié* sums and to a new equidistribution estimate for the set of modular roots of primes.

Contents

Keywords: Modular roots; arithmetic combinatorics; geometry of numbers

2020 Mathematics subject classification: Primary 11B30; 11L07
Secondary 11N69

1. Introduction

1.1. Background

For a prime q, we use $\mathbb{F}_q$ to denote the finite field of q elements. Given a set $\mathcal{N} \subseteq \mathbb{F}_q$ and an integer $k \geqslant 1$, let $T_{\nu,k}(\mathcal{N};q)$ be the number of solutions to the equation (in $\mathbb{F}_q$)

$$b_1 + \ldots + b_\nu = b_{\nu+1} + \ldots + b_{2\nu}, \qquad b_i^k \in \mathcal{N},\ i = 1,\ldots,2\nu.$$

For $\nu = 2$, we also denote

$$T_{\nu,k}(\mathcal{N};q) = E_k(\mathcal{N};q).$$

When $k = 1$, in additive combinatorics, this is the well–known quantity called the *additive energy* of $\mathcal{N}$. More generally, $E_k(\mathcal{N};q)$ is the additive energy of the set of k-th roots of elements of $\mathcal{N}$ (of those which are k-th power residues).

In the special case $\mathcal{N} = \{1,\ldots,N\}$ for an integer $1 \leqslant N < q$, we also write

$$T_{\nu,k}(j\mathcal{N};q) = \mathsf{T}_{\nu,k}(N;j,q), \qquad E_k(j\mathcal{N};q) = \mathsf{E}_k(N;j,q),$$

where the set $j\mathcal{N} = \{j,\ldots,jN\}$ is embedded in $\mathbb{F}_q$ in a natural way.

The quantity $\mathsf{E}_2(N;j,q)$ has been introduced and estimated in [13]. In particular, for any $j \in \mathbb{F}_q^*$, by [13, Lemmas 6.4 and 6.6] we have

$$\mathsf{E}_2(N;j,q) \leqslant \min\left\{N^4/q + N^{5/2}, N^{7/2}/q^{1/2} + N^{7/3}\right\} q^{o(1)}, \tag{1.1}$$

which has been used in [13, Theorem 1.7] to estimate certain bilinear sums and thus improve some results of [14] on correlations between *Salié* sums, which is important for applications to moments of L-functions attached to some modular forms. Furthermore, bounds of such bilinear sums have applications to the distribution of modular square roots of primes; see [13, 27] for details.

This line of research has been continued in [26] where it is shown that, for almost all primes q, for all $N < q$ and $j \in \mathbb{F}_q^*$ one has an essentially optimal bound

$$\mathsf{E}_2(N;j,q) \leqslant \left(N^4/q + N^2\right) q^{o(1)}. \tag{1.2}$$

We expect the bound (1.2) to hold for all primes q; however, this seems difficult to establish with current techniques.

As an application of the bound (1.2), it has been shown in [26] that on average over q one can significantly improve the error term in the asymptotic formula for twisted second moments of L-functions of half integral weight modular forms.

Furthermore, it is shown in [26] that methods of *additive combinatorics* can be used to estimate $E_2(\mathcal{N};q)$ for sets $\mathcal{N}$ with small doubling. Namely, for an arbitrary set $\mathcal{N}$ (of any algebraic domain equipped with addition), as usual, we denote

$$\mathcal{N} + \mathcal{N} = \{n_1 + n_2 : \ n_1, n_2 \in \mathcal{N}\}.$$

Then it is shown in [26], in particular, that if $\mathcal{N} \subseteq \mathbb{Z}_q$ is a set of cardinality N such that $\#(\mathcal{N} + \mathcal{N}) \leqslant LN$ for some real L, then

$$E_2(\mathcal{N};q) \leqslant q^{o(1)} \left(\frac{L^4 N^4}{q} + L^2 N^{11/4}\right). \tag{1.3}$$

Here, we extend and improve these results in several directions and obtain upper bounds on $T_{\nu,k}(\mathcal{N};q)$ and $\mathsf{T}_{\nu,k}(N;j,q)$ for other choices of (ν,k) besides $(\nu,k) = (2,2)$ along with improving the bound of [13, Lemma 6.6] for $T_{2,2}(N;j,q)$. Our estimate for $T_{2,2}(N;j,q)$ gives some improvement on exponential sums bounds from [13].

We believe the new ideas of this work include

- the use of higher-dimensional lattices and more advanced techniques from the geometry of numbers such as transference principles and should be considered a development of the arguments from [13] where only a two-dimensional lattice is used,
- applying so-called *decimations* of multivariate polynomials,
- the use of *Gowers norms.*

Such estimates have the potential for several new applications. One such application is to bilinear sums with some *multidimensional Salié sums* which by a result of Duke [10] can be reduced to one-dimensional sums over k-th roots (generalising the case of $k = 2$, see [19, Lemma 12.4] or [23, Lemma 4.4]). This result of Duke [10] combined with our present

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

results and also the approach of [14, 13, 26] may have a potential to lead to new asymptotic formulas for moments of L-functions with Fourier coefficients of automorphic forms over $\mathrm{GL}(k,\mathbb{Z})$ with $k \geqslant 3$. We refer to [10] for further references. For these applications, one has to extend our bound from $k = 2$ to arbitrary $k \geqslant 3$, which is of independent interest, and maybe achievable with our techniques.

Improved bounds on $\mathsf{T}_{\nu,k}(N;j,q)$ with $\nu > 2$ have a potential to obtain further improvements and extend the region in which there are nontrivial bounds of bilinear sums from [13, 26]. In turn, this can lead to further advances in their applications.

Furthermore, the new result on the distribution of modular roots of primes, (see Theorem 2.3) can be viewed as dual to celebrated result of Duke, Friedlander and Iwaniec [11, 12] on square roots of a fixed integer modulo distinct primes. In turn, this may have a similar range of 'dual' applications.

1.2. Notation

Throughout the paper, the notation $U = O(V)$, $U \ll V$ and $V \gg U$ are equivalent to $|U| \leqslant cV$ for some positive constant c, which throughout the paper may depend on the integer k.

For any quantity $V > 1$, we write $U = V^{o(1)}$ (as $V \to \infty$) to indicate a function of V which satisfies $|U| \leqslant V^{\varepsilon}$ for any $\varepsilon > 0$, provided V is large enough.

For complex weights $\boldsymbol{\beta} = \{\beta_n\}_{n\in\mathcal{N}}$, supported on a finite set $\mathcal{N}$, we define the norms

$$\|\boldsymbol{\beta}\|_\infty = \max_{n\in\mathcal{N}} |\beta_n| \qquad \text{and} \qquad \|\boldsymbol{\beta}\|_\sigma = \left(\sum_{n\in\mathcal{N}} |\alpha_n|^\sigma\right)^{1/\sigma},$$

where $\sigma > 1$, and similarly for other weights.

For a real $A > 0$, we write $a \sim A$ to indicate that a is in the dyadic interval $A/2 \leqslant a < A$.

We use $\#\mathcal{A}$ for the cardinality of a finite set $\mathcal{A}$.

Given two functions f,g on some algebraic domain $\mathcal{D}$ equipped with addition, we define the convolution

$$(f \circ g)(d) = \sum_{x\in\mathcal{D}} f(x)g(x-d).$$

We can then recursively define longer convolutions $(f_1 \circ \ldots \circ f_s)(d)$.

If f is the indicator function of a set $\mathcal{A}$, then we write

$$(f \circ f)(d) = (\mathcal{A} \circ \mathcal{A})(d).$$

In fact, we often use $\mathcal{A}(a)$ for the indicator function of a set $\mathcal{A}$, that is, $\mathcal{A}(a) = 1$ if $a \in \mathcal{A}$ and $\mathcal{A}(a) = 0$ otherwise.

Note that $(\mathcal{A} \circ \mathcal{A})(d)$ counts the number of the solutions to the equation $d = a_1 - a_2$, where a_1, a_2 run over $\mathcal{A}$, that is

$$(\mathcal{A} \circ \mathcal{A})(d) = \#\{(a_1,a_2) \in \mathcal{A}^2 : \ d = a_1 - a_2\}. \tag{1.4}$$

As usual, we also write

$$\mathcal{A} + \mathcal{A} = \{a_1 + a_2 : \ a_1, a_2 \in \mathcal{A}\}$$

and more generally

$$k\mathcal{A}-\ell\mathcal{A}=\{a_1+\ldots+a_k-b_1-\ldots-b_\ell:\ a_1,\ldots,a_k,b_1,\ldots,b_\ell\in\mathcal{A}\}.$$

Finally, we follow the convention that in summation symbols $\sum_{a\leqslant A}$ the sum is over positive integers $a\leqslant A$.

1.3. New results

We start with a new bound on $\mathsf{T}_{2,2}(N;j,q)=\mathsf{E}_2(N;j,q)$ which improves Equation (1.1).

Theorem 1.1. *Let q be prime. For any $j\in\mathbb{F}_q^*$ and integer $N\leqslant q$, we have*

$$\mathsf{T}_{2,2}(N;j,q)\ll\left(\frac{N^{3/2}}{q^{1/2}}+1\right)N^{2+o(1)}.$$

Note it is easy to show the following trivial inequality

$$\mathsf{T}_{4,2}(N;j,q)\leqslant N^4\mathsf{T}_{2,2}(N;j,q),$$

which combined with Theorem 1.1 implies that

$$\mathsf{T}_{4,2}(N;j,q)\leqslant\left(\frac{N^{3/2}}{q^{1/2}}+1\right)N^{6+o(1)}. \tag{1.5}$$

We now obtain a stronger bound for short intervals.

Theorem 1.2. *Let q be prime. For any $j\in\mathbb{F}_q^*$ and integer $N\leqslant q$, we have*

$$\mathsf{T}_{4,2}(N;j,q)\leqslant\left(\frac{N^{5/8}}{q^{1/8}}+\frac{N^{11/2}}{q^{1/2}}+\frac{N^3}{q^{1/4}}\right)N^{6+o(1)}+N^{5+o(1)}.$$

We see that Theorem 1.2 is sharper than Equation (1.5) provided $N\leqslant q^{1/12}$. Energies of the type considered in Theorem 1.2 have the potential for applications to new bilinear sum estimates considered in Section 2 below. However, the range of parameters $N\leqslant q^{1/12}$ does not seem strong enough for meaningful applications, except maybe to very skewed bilinear sums.

The proofs of Theorems 1.1 and 1.2 are based on the geometry of numbers and in particular on some properties of lattices. Although such ideas have been used before to estimate the number of solutions of various congruences (see [7, 20]), they have never been applied to estimate the additive energy of modular roots.

Next, we generalise Equation (1.2) to higher-order roots. In fact, as in [26] the methods allow us to also treat the natural extension of $\mathsf{E}_k(N;j,q)$ to composite moduli q, for which we consider equations in the residue ring $\mathbb{Z}_q$ modulo q, and estimate $\mathsf{E}_k(N;j,q)$ for almost all positive integers q. We, however, restrict ourselves to the case of prime moduli q.

Theorem 1.3. *For a fixed $k\geqslant 3$ and any positive integers $Q\geqslant N\geqslant 1$, we have*

$$\frac{\log Q}{Q}\sum_{\substack{q\sim Q\\ q\ \text{prime}}}\max_{j\in\mathbb{F}_q^*}\mathsf{E}_k(N;j,q)\ll N^2+N^4Q^{-1+o(1)}.$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

To establish Theorem 1.3, we use some arguments related to norms of algebraic integers. It is interesting to note that our construction of auxiliary polynomials resemble the so-called *decimation* procedure which appears in multiple contexts; we refer to [1] for further references.

We now extend the bound (1.3) to other values of k as follows.

Theorem 1.4. *Let $\mathcal{N} \subseteq \mathbb{F}_q$ be a set of cardinality $\#\mathcal{N} = N \leqslant q^{2/3}$ such that $\#(\mathcal{N}+\mathcal{N}) \leqslant LN$ for some real L. Then for $k \geqslant 3$, we have*

$$E_k(\mathcal{N};q) \leqslant L^{\vartheta_k} N^{3-\rho_k} q^{o(1)},$$

where

$$\rho_k = 1/(7\cdot 2^{k-1}-9) \quad \text{and} \quad \vartheta_k = \begin{cases} 2^{k+3}\rho_k, & \text{for } k \geqslant 5; \\ 64/47, & \text{for } k = 4; \\ 32/19, & \text{for } k = 3. \end{cases}$$

We remark that the exponent of L in Theorem 1.4 is $\vartheta_3 = 32/19$, $\vartheta_4 = 64/47$ and

$$\vartheta_k = \frac{2^{k+3}}{7\cdot 2^{k-1}-9} \leqslant \frac{256}{103}$$

for $k \geqslant 5$. For $k = 3,4$, the exponent of L is better than generic because of some additional saving in our application of the Plünnecke inequality; see [30, Corollary 6.29].

The proof is based on some ideas of Gowers [16, 17], in particular on the notion of the *Gowers norm*. Finally, we remark that it is easy to see that, actually, our method works for any polynomial not only for monomials. Also, it is possible, in principle, to insert the general weight $\boldsymbol{\beta}$, but the induction procedure requires complex calculations to estimate this more general quantity

$$E_k(\mathcal{N};\boldsymbol{\beta},q) = \sum_{\substack{u,v,x,y\in\mathbb{F}_q\\ u^k,v^k,x^k,y^k\in\mathcal{N}\\ u+v=x+y}} \beta_u\beta_v\beta_x\beta_y.$$

Nevertheless, we record a simple consequence of Theorem 1.4 with weights $\boldsymbol{\beta}$, which follows from the pigeonhole principle.

Corollary 1.5. *Let $\mathcal{N} \subseteq \mathbb{F}_q$ be a set of cardinality $\#\mathcal{N} = N$ such that $\#(\mathcal{N}+\mathcal{N}) \leqslant LN$ for some real L. Then for any weights $\boldsymbol{\beta}$ supported on $\mathcal{N}$, and with $\|\boldsymbol{\beta}\|_\infty \leqslant 1$ Then*

$$E_k(\mathcal{N};\boldsymbol{\beta},q) \leqslant L^{\vartheta_k} \|\boldsymbol{\beta}\|_1^{2-2\rho_k} \|\boldsymbol{\beta}\|_2^{2+2\rho_k} q^{o(1)},$$

where ϑ_k and ρ_k are as in Theorem 1.4.

We also remark that Theorem 1.4 can be reformulated as a statement that for any set $\mathcal{A} \subseteq \mathbb{F}_q$ either the additive energy $\#\{a_1+a_2 = a_3+a_4 :\ a_1,a_2,a_3,a_4 \in \mathcal{A}\}$ of $\mathcal{A}$ is small or $\mathcal{A}^k$ has large doubling set $\mathcal{A}^k + \mathcal{A}^k = \{a_1^k + a_2^k :\ a_1,a_2 \in \mathcal{A}\}$.

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

2. Applications

Given weights $\boldsymbol{\alpha},\boldsymbol{\beta}$ and $a,h \in \mathbb{F}_q^*$, we define bilinear forms over modular square roots as in [13, Equation (1.6)]

$$W_{a,q}(\boldsymbol{\alpha},\boldsymbol{\beta};h,M,N) = \sum_{m\sim M}\sum_{n\sim N}\alpha_m\beta_n \sum_{\substack{x\in\mathbb{F}_q\\ x^2=amn}} \mathbf{e}_q(hx). \tag{2.1}$$

Using Theorem 1.1, we obtain a new estimate for $W_{a,q}(\boldsymbol{\alpha},\boldsymbol{\beta};h,M,N)$ which improves on [13, Theorem 1.7]. Assuming

$$\|\boldsymbol{\alpha}\|_\infty,\|\boldsymbol{\beta}\|_\infty \leqslant 1,$$

it follows from the proof of [13, Theorem 1.7] that

$$|W_{a,q}(\boldsymbol{\alpha},\boldsymbol{\beta};h,M,N)|^8 \leqslant q^{1+o(1)}(MN)^4 \mathsf{T}_{2,2}(M;1,q)\mathsf{T}_{2,2}(N;b,q),$$

for some b with $\gcd(b,q)=1$.

Applying Theorem 1.1, we obtain the following bound.

Corollary 2.1. *For any positive integers $M,N \leqslant q/2$ and any weights $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ satisfying*

$$\|\boldsymbol{\alpha}\|_\infty,\|\boldsymbol{\beta}\|_\infty \leqslant 1,$$

we have

$$|W_{a,q}(\boldsymbol{\alpha},\boldsymbol{\beta};h,M,N)| \leqslant q^{1/8+o(1)}(MN)^{3/4}\left(\frac{M^{3/16}}{q^{1/16}}+1\right)\left(\frac{N^{3/16}}{q^{1/16}}+1\right).$$

If the sequence $\boldsymbol{\beta}$ corresponds to values of a smooth function φ whose derivatives and support $\operatorname{supp}\varphi$ satisfy

$$\varphi^{(j)}(x) \ll \frac{1}{x^j} \qquad \text{and} \qquad \operatorname{supp}\varphi \subseteq [N,2N], \tag{2.2}$$

for any integer j (with implied constant allowed to depend on j), then we write

$$V_{a,q}(\boldsymbol{\alpha},\varphi;h,M,N) = \sum_{m\sim M}\sum_{n\in\mathbb{Z}}\alpha_m\varphi(n) \sum_{\substack{x\in\mathbb{F}_q\\ x^2=amn}} \mathbf{e}_q(hx). \tag{2.3}$$

We now give a new bound for $V_{a,q}(\boldsymbol{\alpha};h,M,N)$. This does not rely on energy estimates although may be of independent interest. It is also used in a combination with Corollary 2.1 to derive Theorem 2.3 below.

Theorem 2.2. *For any positive integers M,N satisfying $MN \ll q$ and $M<N$, any weight $\boldsymbol{\alpha}$ satisfying*

$$\|\boldsymbol{\alpha}\|_\infty \leqslant 1,$$

and a function φ satisfying Equation (2.2), for any fixed integer $r \geqslant 2$, we have

$$|V_{a,q}(\boldsymbol{\alpha},\varphi;h,M,N)| \leqslant q^{1/2-1/4r+o(1)}M^{1-1/2r}N^{1/2r}\left(1+\frac{(MN)^{1/2}}{q^{1/2-1/4r}}\right).$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

Corollary 2.1 may be used to improve various results from [13, Sections 1.3–1.4]. We present once such improvement to the distribution of modular roots of primes. Recall that the *discrepancy* $D(N)$ of a sequence in $\xi_1,\dots,\xi_N \in [0,1)$ is defined as

$$D_N = \sup_{0\leqslant \alpha<\beta\leqslant 1} \left|\#\{1\leqslant n\leqslant N:\ \xi_n \in [\alpha,\beta)\} - (\beta-\alpha)N\right|.$$

For a positive integer P, we denote the discrepancy of the sequence (multiset) of points

$$\{x/q:\ x^2 \equiv p \bmod q \text{ for some prime } p\leqslant P\}$$

by $\Gamma_q(P)$. Combining the Erdös-Turán inequality with the Heath–Brown identity reduces estimating $\Gamma_q(P)$ to sums of the form (2.1) and (2.3). Combining, Corollary 2.1 with Theorem 2.2, we obtain an improvement on [13, Theorem 1.10].

Theorem 2.3. *For any $P\leqslant q^{3/4}$, we have*

$$\Gamma_q(P) \leqslant \left(P^{15/16} + q^{1/8}P^{3/4} + q^{1/16}P^{69/80} + q^{13/88}P^{3/4}\right) q^{o(1)}.$$

Note that Theorem 2.3 is nontrivial provided $P\geqslant q^{13/22}$ and improves on the range $P\geqslant q^{13/20}$ from [13, Theorem 1.10].

3. Proof of Theorem 1.1

3.1. Lattices

We use $\mathrm{Vol}(B)$ to denote the volume of a body $B\subseteq \mathbb{R}^d$. For a lattice $\Gamma\subseteq\mathbb{R}^d$, we recall that the quotient space $\mathbb{R}^d/\Gamma$ (called the fundamental domain) is compact and so $\mathrm{Vol}(\mathbb{R}^d/\Gamma)$ is correctly defined; see also [30, Sections 3.1 and 3.5] for basic definitions and properties of lattices. In particular, we define the successive minima λ_i, $i=1,\dots,d$, of B with respect to Γ as

$$\lambda_i = \inf\{\lambda>0:\ \lambda B \text{ contains } i \text{ linearly independent elements of } \Gamma\},$$

where λB is the homothetic image of B with the coefficient λ.

The following is Minkowski's second theorem. For a proof see [30, Theorem 3.30].

Lemma 3.1. *Suppose $\Gamma\subseteq\mathbb{R}^d$ is a lattice of rank d, $B\subseteq\mathbb{R}^d$ a symmetric convex body, and let $\lambda_1,\dots,\lambda_d$ denote the successive minima of Γ with respect to B. Then we have*

$$\frac{1}{\lambda_1\dots\lambda_d} \leqslant \frac{d!}{2^d}\frac{\mathrm{Vol}(B)}{\mathrm{Vol}(\mathbb{R}^d/\Gamma)}.$$

For a proof of the following, see [4, Proposition 2.1].

Lemma 3.2. *Suppose $\Gamma\subseteq\mathbb{R}^d$ is a lattice, $B\subseteq\mathbb{R}^d$ a symmetric convex body, and let $\lambda_1,\dots,\lambda_d$ denote the successive minima of Γ with respect to B. Then we have*

$$\#(\Gamma\cap B) \leqslant \prod_{i=1}^{d}\left(\frac{2i}{\lambda_i}+1\right).$$

3.2. Reduction to counting points in lattices

It more convenient to estimate $\mathsf{T}_{2,2}(N;\overline{j},q)$ rather than $\mathsf{T}_{2,2}(N;j,q)$ for the multiplicative inverse $\overline{j}$ of j modulo q, which or course is an equivalent question.

Let $\mathcal{A}$ denote the set

$$\mathcal{A} = \{x \in \mathbb{F}_q^* : \ jx^2 \in \{1,\dots,N\}\}$$

so that

$$\mathsf{T}_{2,2}(N;\overline{j},q) = \sum_{d\in\mathbb{F}_q} (\mathcal{A}\circ\mathcal{A})(d)^2, \tag{3.1}$$

where $(\mathcal{A}\circ\mathcal{A})(d)$ is defined by Equation (1.4).

If $a_1,a_2 \in \mathcal{A}$ satisfy

$$a_1 - a_2 = d,$$

then elementary algebraic manipulations imply

$$(a_1^2 - a_2^2 - d^2)^2 = 4d^2a_2^2.$$

We have

$$ja_1^2 - ja_2^2, ja_2^2 \in \{-N,\dots,N\}.$$

Since for any $\lambda,\mu \in \mathbb{F}_q$ the number of solutions to

$$ja_1^2 - ja_2^2 = \lambda, \quad ja_2^2 = \mu, \qquad a_1,a_2 \in \mathcal{A},$$

is $O(1)$, we derive from Equation (3.1)

$$\mathsf{T}_{2,2}(N;\overline{j},q) \ll \sum_{d\in\mathbb{F}_q} J_0(d)^2,$$

where

$$J_0(d) = \#\{|m|,|n| \leqslant N : \ (n - jd^2)^2 \equiv 4jd^2m \bmod q\}.$$

If n,m satisfy

$$(n - jd^2)^2 \equiv 4jd^2m \bmod q,$$

then

$$n^2 + j^2d^4 \equiv 2jd^2(2m+n) \bmod q.$$

This implies

$$\mathsf{T}_{2,2}(N;\overline{j},q) \ll \sum_{d\in\mathbb{F}_q} J(d)^2, \tag{3.2}$$

where

$$J(d) = \#\{|m|,|n| \leqslant 6N : \ n^2 + j^2d^4 \equiv jd^2m \bmod q\}. \tag{3.3}$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

Let $\mathcal{L}(d)$ denote the lattice

$$\mathcal{L}(d) = \{(x,y) \in \mathbb{Z}^2 : \; x \equiv jd^2 y \bmod q\},$$

B the convex body

$$B = \{(x,y) \in \mathbb{R}^2 : \; |x| \leqslant 72N^2, \; |y| \leqslant 12N\},$$

and let $\lambda_1(d), \lambda_2(d)$ denote the first and second successive minima of $\mathcal{L}(d)$ with respect to B.

We now partition summation in Equation (3.2) according to the size of $\lambda_1(d)$ and $\lambda_2(d)$ to get

$$\mathsf{T}_{2,2}(N;\bar{j},q) \ll S_0 + S_1 + S_2, \tag{3.4}$$

where

$$S_0 = \sum_{\substack{d \in \mathbb{F}_q \\ \lambda_1(d) > 1}} J(d)^2, \qquad S_1 = \sum_{\substack{d \in \mathbb{F}_q \\ \lambda_1(d) \leqslant 1 \\ \lambda_2(d) > 1}} J(d)^2, \qquad S_2 = \sum_{\substack{d \in \mathbb{F}_q \\ \lambda_1(d), \lambda_2(d) \leqslant 1}} J(d)^2.$$

3.3. Concluding the proof

Consider first S_0. If $\lambda_1(d) > 1$, then

$$J(d) \leqslant 1,$$

which follows from the fact that for any distinct points (n_0,m_0), $(n_1.m_1)$ satisfying the conditions in Equation (3.3) we have

$$(n_0^2 - n_1^2, m_0 - m_1) \in \mathcal{L}(d) \cap B.$$

This implies that $J(d)^2 = J(d)$, and we derive

$$S_0 = \sum_{\substack{d \in \mathbb{F}_q \\ \lambda_1(d) > 1}} J(d) \ll N^2. \tag{3.5}$$

Consider next S_1. Suppose d satisfies $\lambda_1(d) \leqslant 1$ and $\lambda_2(d) > 1$. There exists n_d, m_d satisfying the conditions given in Equation (3.3) such that

$$J(d) \ll \# \left\{ |m|,|n| \leqslant 6N : \; (n^2 - n_d^2, m - m_d) \in \mathcal{L}(d) \cap B \right\}.$$

Since $\lambda_2(d) > 1$, there exists a unique point $(a_d, b_d) \in \mathcal{L}(d) \cap B$ satisfying

$$\gcd(a_d, b_d) = 1, \quad |a_d| \leqslant 72N^2, \quad |b_d| \leqslant 12N$$

such that

$$J(d) \ll \# \left\{ |m|,|n| \leqslant 6N : \; \frac{n^2 - n_d^2}{m - m_d} = \frac{a_d}{b_d} \right\} + 1.$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

This implies

$$S_1 \leqslant \sum_{d\in\mathbb{F}_q} J(d)\left(\#\left\{|m|,|n|\leqslant 6N:\ \frac{n^2-n_d^2}{m-m_d}=\frac{a_d}{b_d}\right\}+1\right) \tag{3.6}$$
$$\leqslant \sum_{(a,b)\in\mathcal{W}} J(a,b)K(a,b)+N^2,$$

where $\mathcal{W}$ is the following set of all pairs (a,b) satisfying

$$\mathcal{W}=\{(a,b)\in\mathbb{Z}^2:\ |a|\leqslant 72N^2,\ |b|\leqslant 12N,\ \gcd(a,b)=1\}, \tag{3.7}$$

and $K(a,b)$ is defined by

$$K(a,b)=\#\left\{(m,n)\in\mathbb{Z}^2:\ |m|,|n|\leqslant 6N,\ \frac{n^2-n_{a,b}^2}{m-m_{a,b}}=\frac{a}{b}\right\},$$

for some choice of integers $m_{a,b},n_{a,b}$ satisfying $|m_{a,b}|,|n_{a,b}|\leqslant 6N$ and $J(a,b)$ is defined by

$$J(a,b)=\#\left\{(m,n)\in\mathbb{Z}^2:\ |m|,|n|\leqslant 6N,\ n^2+(ab^{-1})^2\equiv ab^{-1}m \mod q\right\}.$$

Note that

$$\sum_{(a,b)\in\mathcal{W}} J(a,b)\leqslant \#\{(m,n,\lambda)\in\mathbb{Z}^3:\ |m|,|n|\leqslant 6N,\ 1\leqslant\lambda<q,$$
$$\lambda^2-\lambda m+n^2\equiv 0 \mod q\}$$
$$\ll N^2$$

since after fixing m,n with $O(N^2)$ choices there exists $O(1)$ solutions to

$$\lambda^2-\lambda m+n^2\equiv 0 \mod q$$

in the remaining variable λ. We also have

$$J(a,b)\ll K(a,b)+1. \tag{3.8}$$

Fix some a,b as in the sum in Equation (3.6), and consider $K(a,b)$. If n,m satisfy

$$\frac{n^2-n_{a,b}^2}{m-m_{a,b}}=\frac{a}{b}, \qquad |m|,|n|\leqslant 6N,$$

then, since $\gcd(a,b)=1$, we have

$$n^2-n_{a,b}^2\equiv 0 \bmod |a|, \tag{3.9}$$

and

$$m-m_{a,b}\equiv 0 \bmod |b|. \tag{3.10}$$

Furthermore, if one out of m or n is fixed, then the other number is defined in no more than two ways.

Write Equation (3.9) as

$$(n-n_{a,b})(n+n_{a,b})\equiv 0 \bmod |a|.$$

Then we see that there are two integers a_1,a_2 satisfying

$$a_1a_2 = a, \qquad |a_1|,|a_2| \leqslant 12N$$

such that

$$n \equiv n_{a,b} \bmod |a_1|, \quad n \equiv -n_{a,b} \bmod |a_2|.$$

Hence, for each fixed pair (a_1,a_2) there are at most

$$\frac{N}{\mathrm{lcm}[a_1,a_2]} + 1 \ll \frac{N}{|a|}\gcd(a_1,a_2) + 1$$

possibilities for n. Hence, by a well-known bound

$$\tau(a) = a^{o(1)} \tag{3.11}$$

on the divisor function $\tau(a)$ for $a \neq 0$, see [19, Equation (1.81)], we have

$$K(a,b) \ll \sum_{a_1a_2=a}\left(\frac{N}{\mathrm{lcm}(a_1,a_2)} + 1\right) \ll \frac{N}{|a|}\sum_{a_1a_2=a}\gcd(a_1,a_2) + N^{o(1)}.$$

By the Cauchy–Schwarz inequality and Equation (3.11), we now derive

$$K(a,b)^2 \ll N^{2+o(1)}\sum_{a_1a_2=a}\frac{\gcd(a_1,a_2)^2}{|a|^2} + N^{o(1)}. \tag{3.12}$$

Similarly, using Equation (3.10) we obtain

$$K(a,b) \ll \frac{N}{|b|}. \tag{3.13}$$

Combining Equations (3.12), (3.13), (3.8) and substituting into Equations (3.6), we see that

$$S_1 \leqslant N^{2+o(1)}\sum_{(a,b)\in\mathcal{W}}\sum_{\substack{a_1a_2=a\\|a_1|,|a_2|\leqslant 12N}}\min\left\{\frac{1}{b^2},\frac{\gcd(a_1,a_2)^2}{a^2}\right\} + \sum_{(a,b)\in\mathcal{W}}J(a,b)N^{o(1)}.$$

Hence, recalling Equation (3.7), we derive

$$\begin{aligned} S_1 &\leqslant N^{2+o(1)}\sum_{\substack{|a|\leqslant 72N^2\\|b|\leqslant 12N}}\sum_{\substack{a_1a_2=a\\|a_1|,|a_2|\leqslant 12N}}\min\left\{\frac{1}{b^2},\frac{\gcd(a_1,a_2)^2}{a^2}\right\} + N^{2+o(1)}\\ &\leqslant N^{2+o(1)}\sum_{a_1,a_2,b\leqslant 12N}\min\left\{\frac{1}{b^2},\frac{\gcd(a_1,a_2)^2}{a_1^2a_2^2}\right\} + N^{2+o(1)} \end{aligned}$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

$$\leqslant N^{2+o(1)} \sum_{e \leqslant 12N} \sum_{b \leqslant 12N} \sum_{\substack{a_1,a_2 \leqslant 12N \\ \gcd(a_1,a_2)=e}} \min\left\{\frac{1}{b^2}, \frac{e^2}{a_1^2 a_2^2}\right\} + N^{2+o(1)}$$

$$\leqslant N^{2+o(1)} \sum_{e \leqslant 12N} \sum_{b \leqslant 12N} \sum_{a_1,a_2 \leqslant 12N/e} \min\left\{\frac{1}{b^2}, \frac{1}{a_1^2 a_2^2 e^2}\right\} + N^{2+o(1)}.$$

Using the bound on the divisor function (3.11) again, we obtain

$$\begin{aligned} S_1 &\leqslant N^{2+o(1)} \sum_{b \leqslant 12N} \sum_{a \leqslant 12^4 N^2} \min\left\{\frac{1}{b^2}, \frac{1}{a^2}\right\} + N^{2+o(1)} \\ &\leqslant N^{2+o(1)} \left(\sum_{b \leqslant 12N} \sum_{a \leqslant b} \frac{1}{b^2} + \sum_{a \leqslant 12^4 N^2} \sum_{b \leqslant a} \frac{1}{a^2} \right) + N^{2+o(1)} \\ &\leqslant N^{2+o(1)}. \end{aligned} \tag{3.14}$$

Finally, consider S_2. If d satisfies $\lambda_2(d) \leqslant 1$, then by Lemmas 3.1 and 3.2

$$\#\left(\mathcal{L}(d) \cap B\right) \ll \frac{N^3}{q}. \tag{3.15}$$

In particular, we see that for $N = o(q^{1/3})$ the bound (3.15) implies

$$1 \leqslant \#\left(\mathcal{L}(d) \cap B\right) = o(1),$$

which means that this case (that is, $\lambda_2(d) \leqslant 1$) never occurs for 'small' N.

For each $|n| \leqslant 6N$ there exists at most one value of m satisfying Equation (3.3) and for any two pairs $(n_1,m_1),(n_2,m_2)$ satisfying Equation (3.3) we have

$$n_1^2 - n_2^2 \equiv jd^2(m_1 - m_2) \bmod q.$$

This implies

$$J(d)^2 \ll \#\{|n_1|,|n_2|,|m| \leqslant 12N,\ n_1 \neq \pm n_2 :\ n_1^2 - n_2^2 \equiv jd^2 m \bmod q\}.$$

Since for any integer $r \neq 0$ the bound (3.11) on the divisor function implies

$$\#\{|n_1|,|n_2| \leqslant 8N :\ n_1^2 - n_2^2 = r\} \leqslant N^{o(1)},$$

we obtain

$$J(d)^2 \leqslant \#\left(\mathcal{L}(d) \cap B\right) N^{o(1)}.$$

By Equation (3.15)

$$J(d) \ll \frac{N^{3/2+o(1)}}{q^{1/2}},$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

which implies

$$S_2 = \sum_{\substack{d \in \mathbb{F}_q \\ \lambda_1(d),\lambda_2(d) \leqslant 1}} J(d)^2 \ll \frac{N^{3/2}}{q^{1/2}} \sum_{\substack{d \in \mathbb{F}_q \\ \lambda_1(d),\lambda_2(d) \leqslant 1}} J(d) \ll \frac{N^{7/2+o(1)}}{q^{1/2}}. \tag{3.16}$$

Combining Equations (3.5), (3.14) and (3.16) with Equation (3.4), we derive the desired bound on $\mathsf{T}_{2,2}(N;\overline{j},q))$.

4. Proof of Theorem 1.2

4.1. Lattices

For a lattice Γ and a convex body B, we define the dual lattice Γ^* and dual body B^* by

$$\Gamma^* = \{x \in \mathbb{R}^d : \langle x,y \rangle \in \mathbb{Z} \quad \text{for all} \quad y \in \Gamma\},$$

and

$$B^* = \{x \in \mathbb{R}^d : \langle x,y \rangle \leqslant 1 \quad \text{for all} \quad y \in B\},$$

respectively.

The following is known as a transference theorem and is due to Mahler [21] which we present in a form given by Cassels [8, Chapter VIII, Theorem VI].

Lemma 4.1. *Let $\Gamma \subseteq \mathbb{R}^d$ be a lattice, $B \subseteq \mathbb{R}^d$ a symmetric convex body, and let Γ^* and B^* denote the dual lattice and dual body. Let $\lambda_1,\ldots,\lambda_d$ denote the successive minima of Γ with respect to B and $\lambda_1^*,\ldots,\lambda_d^*$ the successive minima of Γ^* with respect to B^*. For each $1 \leqslant j \leqslant d$, we have*

$$\lambda_j \lambda_{d-j+1}^* \leqslant d!.$$

We apply Lemma 4.1 to lattices of a specific type whose dual may be easily calculated. For a proof of the following, see [6, Lemma 15].

Lemma 4.2. *Let $a_1,\ldots,a_d$ and $q \geqslant 1$ be integers satisfying $\gcd(a_i,q) = 1$, and let $\mathcal{L}$ denote the lattice*

$$\mathcal{L} = \{(n_1,\ldots,n_d) \in \mathbb{Z}^d : a_1 n_1 + \ldots + a_d n_d \equiv 0 \bmod q\}.$$

Then we have

$$\mathcal{L}^* = \Bigg\{ \left(\frac{m_1}{q},\ldots,\frac{m_d}{q} \right) \in \mathbb{Z}^d/q : \\ \exists\ \lambda \in \mathbb{Z} \ \ \textit{such that} \ \ a_j \lambda \equiv m_j \bmod q \Bigg\}.$$

Our next result should be compared with the case $\nu = 3$ of [7, Lemma 17]. It is possible to give a more direct variant of [7, Lemma 17] to estimate higher-order energies of modular square roots (see the proof of Corollary 4.4 below) although this seems to put tighter restrictions on the size of the parameter N.

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

Lemma 4.3. *Let q be prime, $a,b,c \not\equiv 0 \bmod q$ and L,M,N integers. Let $\mathcal{L}$ denote the lattice*

$$\mathcal{L} = \{(\ell,m,n) \in \mathbb{Z}^3: \ a\ell + bm + cn \equiv 0 \bmod q\},$$

and let B be the convex body

$$B = \{(x,y,z) \in \mathbb{R}^3: \ |x| \leqslant L, \quad |y| \leqslant M, \quad |z| \leqslant N\}.$$

Let

$$K = \#(\mathcal{L} \cap B),$$

and λ_1,λ_2 denote the first and second successive minima of $\mathcal{L}$ with respect to B. Then at least one of the following holds:

(i)

$$K < \max\left\{\frac{640LMN}{q}, 1\right\}.$$

(ii) $\lambda_1 \leqslant 1$ *and* $\lambda_2 > 1$.

(iii) *There exists some $\lambda \not\equiv 0 \bmod q$ and $\ell,m,n \in \mathbb{Z}$ satisfying*

$$|\ell| \leqslant \frac{4320MN}{K}, \quad |m| \leqslant \frac{4320LN}{K}, \quad |n| \leqslant \frac{4320LM}{K}$$

and

$$a\lambda \equiv \ell \bmod q, \quad b\lambda \equiv m \bmod q, \quad c\lambda \equiv n \bmod q.$$

Proof. Assume that (i) fails. Thus, we have

$$K \geqslant \max\left\{\frac{640LMN}{q}, 1\right\}. \tag{4.1}$$

Then $K \geqslant 1$. Hence, if $\lambda_1 \leqslant \lambda_2 \leqslant \lambda_3$ denote the successive minima of $\mathcal{L}$ with respect to B, then $\lambda_1 \leqslant 1$. We first show Equation (4.1) implies

$$\lambda_3 > 1.$$

Indeed, otherwise by Lemma 3.2

$$K \leqslant \left(\frac{2}{\lambda_1}+1\right)\left(\frac{4}{\lambda_2}+1\right)\left(\frac{6}{\lambda_3}+1\right) \leqslant \frac{3}{\lambda_1}\frac{5}{\lambda_2}\frac{7}{\lambda_3} = \frac{105}{\lambda_1\lambda_2\lambda_3}. \tag{4.2}$$

Since

$$\mathrm{Vol}(\mathbb{R}^3/\mathcal{L}) = q \qquad \text{and} \qquad \mathrm{Vol}(B) = 8LMN,$$

we see from Lemma 3.1 that

$$\frac{1}{\lambda_1\lambda_2\lambda_3} \leqslant \frac{3!}{8}\frac{8LMM}{q} = \frac{6LMN}{q}, \tag{4.3}$$

which together with Equation (4.2) contradicts Equation (4.1).

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

Hence, we have either

$$\lambda_1 \leqslant 1, \qquad \lambda_2, \lambda_3 > 1, \tag{4.4}$$

or

$$\lambda_1, \lambda_2 \leqslant 1, \qquad \lambda_3 > 1. \tag{4.5}$$

Clearly, Equation (4.4) is the same as (ii).

Next, suppose that we have Equation (4.5). By Lemma 3.2, a similar calculation as before, together with Equation (4.3) gives

$$K \leqslant \frac{7 \times 15}{\lambda_1 \lambda_2} = \frac{105\lambda_3}{\lambda_1 \lambda_2 \lambda_3}. \tag{4.6}$$

Applying Lemma 3.1 and using

$$\mathrm{Vol}(B) = 8NML, \quad \mathrm{Vol}(\mathbb{R}^3/\mathcal{L}) = q,$$

we derive from Equation (4.6) that

$$K \leqslant \frac{105 \cdot 3!\,\mathrm{Vol}(B)\lambda_3}{2^3\,\mathrm{Vol}(\mathbb{R}^3/\mathcal{L})} = \frac{630NML\lambda_3}{q}.$$

Let λ_1^* denote the first successive minima of the dual lattice $\mathcal{L}^*$ with respect to the dual body B^*. By Lemma 4.1,

$$\lambda_3 \leqslant \frac{6}{\lambda_1^*}.$$

The above estimates combined with Equation (4.6) implies

$$\lambda_1^* \leqslant \frac{4320NML}{qK}.$$

Hence, by the definition of λ_1^*

$$\mathcal{L}^* \cap \frac{4320NML}{qK} B^* \neq \{(0,0,0)\}. \tag{4.7}$$

Its remains to recall that by Lemma 4.2

$$\mathcal{L}^* = \left\{ \left(\frac{\ell}{q}, \frac{m}{q}, \frac{n}{q} \right) \in \mathbb{Z}^3/q : \ \exists\ \lambda \in \mathbb{Z} \text{ such that} \right.$$
$$\left. a\lambda \equiv \ell \bmod q,\ b\lambda \equiv m \bmod q,\ c\lambda \equiv n \bmod q \right\},$$

and also it is obvious that

$$B^* = \{(x,y,z) \in \mathbb{R}^3 : \ L|x| + M|y| + N|z| \leqslant 1\}.$$

By Equation (4.7), this implies there exists some $\lambda \not\equiv 0 \bmod q$ and ℓ, m, n satisfying (iii), which completes the proof. $\square$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

Corollary 4.4. *Let $\varepsilon > 0$ be a fixed real number. For $j \in \mathbb{F}_q^*$, integer $N \ll q$ and $\Delta \geqslant 1$, let $\mathcal{A}, \mathcal{D} \subseteq \mathbb{F}_q$ denote the sets*

$$\mathcal{A} = \{x \in \mathbb{F}_q^* : \; jx^2 \in [1, N]\}.$$

and

$$\mathcal{D} = \{d \in \mathbb{F}_q^* : \; (\mathcal{A} \circ \mathcal{A})(d) \geqslant \Delta\}.$$

Let K be sufficiently large, and suppose K and Δ satisfy

$$K \geqslant \left(\frac{N^{15/2}}{\Delta^{12} q^{1/2}} + \frac{N^5}{\Delta^8 q^{1/4}}\right) N^{\varepsilon} \tag{4.8}$$

and

$$\Delta \geqslant \left(\frac{N^{3/2}}{q^{1/2}} + \frac{N^{5/8}}{q^{1/8}}\right) N^{\varepsilon}. \tag{4.9}$$

Let $\mathcal{F} \subseteq \mathbb{F}_q^*$ denote the set of f satisfying

$$(\mathcal{D} \circ \mathcal{D})(f) \geqslant K. \tag{4.10}$$

Then either

$$K \ll 1, \tag{4.11}$$

or

$$K \# \mathcal{F} \ll \frac{N^{3+o(1)}}{\Delta^4}.$$

Proof. From Equation (4.10)

$$K \leqslant \#\{(d_1, d_2) \in \mathcal{D}^2 : \; d_1 - d_2 = f\}. \tag{4.12}$$

If $d_1, d_2 \in \mathcal{D}$ satisfy $d_1 - d_2 = f$, then

$$d_1^2 - d_2^2 - f^2 = (d_1 - d_2)^2 + 2d_1 d_2 - 2d_2^2 - f^2 = 2d_2(d_1 - d_2) = 2d_2 f$$

and some algebraic manipulations show

$$(2jd_1^2 - 2jd_2^2 - 2jf^2)^2 = 8jf^2(2jd_2^2).$$

Since $0 \notin \mathcal{D}$, for each $d \in \mathcal{D}$, by Equation (4.9) and [13, Lemma 6.4] there exists m_d, n_d satisfying

$$2jd^2 \equiv m_d^{-1} n_d \bmod q, \qquad |n_d| \ll \frac{N^2}{\Delta^2}, \tag{4.13}$$
$$|m_d| \ll \frac{N}{\Delta^2}, \qquad \gcd(m_d, n_d) = 1.$$

Let $I(f)$ count the number of solutions to the congruence

$$\left(n_{d_1} m_{d_1}^{-1} - n_{d_2} m_{d_2}^{-1} - 2jf^2\right)^2 \equiv 8jf^2 n_{d_2} m_{d_2}^{-1} \bmod q, \tag{4.14}$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

with $d_1, d_2 \in \mathcal{D}$. The above and Equation (4.12) imply

$$K \leqslant I(f). \tag{4.15}$$

Rearranging Equation (4.14), we obtain

$$\left(m_{d_2} n_{d_1} - m_{d_1} n_{d_2} - 2jf^2 m_{d_1} m_{d_2}\right)^2 \equiv 8jf^2 m_{d_1}^2 m_{d_2} n_{d_2} \bmod q.$$

This implies that $I(f)$ is bounded by the number of solutions to

$$\begin{aligned}(n_{d_1} m_{d_2} - n_{d_2} m_{d_1})^2 - 4jf^2 m_{d_1} m_{d_2}(n_{d_1} m_{d_2} + n_{d_2} m_{d_1})& \\ + 4j^2 f^4 (m_{d_1} m_{d_2})^2 \equiv 0 \bmod q,&\end{aligned} \tag{4.16}$$

with $d_1, d_2 \in \mathcal{D}$. Let $\mathcal{L}$ denote the lattice

$$\mathcal{L} = \{(m,n,\ell) \in \mathbb{Z}^3 : \; m + njf^2 + \ell j^2 f^4 \equiv 0 \bmod q\},$$

and B the convex body

$$B = \left\{(x,y,z) \in \mathbb{R}^3 : \; |x| \leqslant \frac{CN^6}{\Delta^8}, \; |y| \leqslant \frac{CN^5}{\Delta^8}, \; |z| \leqslant \frac{CN^4}{\Delta^8}\right\}$$

for a suitable absolute constant C. By Equations (4.13) and (4.16)

$$\begin{aligned}\big((n_{d_1} m_{d_2} - n_{d_2} m_{d_1})^2, -4m_{d_1} m_{d_2}(n_{d_1} m_{d_2} + n_{d_2} m_{d_1}),& \\ 4(m_{d_1} m_{d_2})^2\big) \in \mathcal{L} \cap B.&\end{aligned} \tag{4.17}$$

Let λ_1, λ_2 denote the first and second successive minima of $\mathcal{L}$ with respect to B. Assuming that $K \geqslant 1$, we have $\lambda_1 \leqslant 1$.

Suppose that

$$\lambda_1 \leqslant 1, \quad \lambda_2 > 1.$$

Then there exists some $(a_0, b_0, c_0) \in \mathcal{L} \cap B$ such that for any $d_1, d_2 \in \mathcal{D}$ satisfying Equation (4.17) we have

$$\begin{aligned}\big((n_{d_1} m_{d_2} - n_{d_2} m_{d_1})^2, -4m_{d_1} m_{d_2}(n_{d_1} m_{d_2} + n_{d_2} m_{d_1}), 4(m_{d_1} m_{d_2})^2\big)& \\ = m(a_0, b_0, c_0),&\end{aligned}$$

for some $m \in \mathbb{Z}$. Note from Equation (4.13) for each $d_1, d_2 \in \mathcal{D}$ we have $m_{d_1} m_{d_2} \neq 0$ and hence $c_0 \neq 0$. This implies

$$\begin{aligned}\left(\frac{n_{d_1}}{m_{d_1}} - \frac{n_{d_2}}{m_{d_2}}\right)^2 &= \frac{a_0}{c_0}, \\ \frac{n_{d_1}}{m_{d_1}} + \frac{n_{d_2}}{m_{d_2}} &= \frac{b_0}{c_0}.\end{aligned}$$

Hence,

$$\begin{aligned}K \leqslant \#\Bigg\{(d_1, d_2) \in \mathcal{D} \times \mathcal{D} : \; \frac{n_{d_1}}{m_{d_1}} - \frac{n_{d_2}}{m_{d_2}} = \pm \left(\frac{a_0}{c_0}\right)^{1/2},& \\ \frac{n_{d_1}}{m_{d_1}} + \frac{n_{d_2}}{m_{d_2}} = \frac{b_0}{c_0}\Bigg\} \leqslant 8&\end{aligned}$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

since once n_{d_1}/m_{d_1} is fixed, due to the coprimality condition in Equation (4.13), d_1^2 is uniquely defined and similarly for d_2^2. This implies Equation (4.11).

Suppose next that

$$\lambda_1 \leqslant 1, \quad \lambda_2 \leqslant 1. \tag{4.18}$$

Let $J(\ell,m,n)$ count the number of solutions to

$$m_1m_2 = \ell, \quad n_1m_2 + n_2m_1 = m, \quad n_1m_2 - n_2m_1 = n,$$

with

$$|m_1|,|m_2| \ll \frac{N}{\Delta^2}, \quad |n_1|,|n_2| \ll \frac{N^2}{\Delta^2}, \qquad m_1m_2n_1n_2 \neq 0 \tag{4.19}$$

so that

$$I(f) \ll \sum_{\substack{|m|,|n|\leqslant CN^3/\Delta^4 \\ |\ell|\leqslant CN^2/\Delta^4 \\ 4j^2f^4\ell^2-4jf^2\ell m+n^2\equiv 0 \bmod q}} J(\ell,m,n), \tag{4.20}$$

for some absolute constant C. We next show that

$$J(\ell,m,n) = N^{o(1)}. \tag{4.21}$$

Estimates for the divisor function (3.11) imply the number of solutions to

$$m_1m_2 = \ell, \quad m_1,m_2 \text{ satisfying Equation (4.19)}$$

is at most $N^{o(1)}$. For each such m_1,m_2, there exists at most one solution to the system

$$n_1m_2 - n_2m_1 = n, \quad n_1m_2 + n_2m_1 = m, \quad n_1,n_2 \text{ satisfying Equation (4.19)},$$

which establishes Equation (4.21). By Equations (4.15) and (4.20)

$$\begin{aligned} K \leqslant \#\{(\ell,m,n)\in\mathbb{Z}^3 : \ &|\ell|\leqslant CN^2/\Delta^4,\ |m|,|n|\leqslant CN^3/\Delta^4, \\ &n^2 - 4jf^2\ell m + 4j^2f^4\ell^2 \equiv 0 \bmod q\}N^{o(1)}, \end{aligned}$$

and hence

$$\begin{aligned} K \leqslant \#\Big\{&(\ell,m,n)\in\mathbb{Z}^3 : \\ &|\ell|\leqslant 2CN^2/\Delta^4,\ |m|\leqslant 4C^2N^5/\Delta^8,\ |n|\leqslant CN^3/\Delta^4, \\ &n^2 + jf^2m + j^2f^4\ell^2 \equiv 0 \bmod q\Big\}N^{o(1)}. \end{aligned} \tag{4.22}$$

By Equation (4.9), for each $\ell,n\in\mathbb{Z}$, there exists at most one value of $|m| \ll N^5/\Delta^8$ satisfying

$$n^2 + jf^2m + j^2f^4\ell^2 \equiv 0 \bmod q.$$

For any (ℓ_1,m_1,n_1) and (ℓ_2,m_2,n_2) satisfying the conditions of Equation (4.22), there exists some $|m| \ll N^5/\Delta^8$ such that

$$n_1^2 + n_2^2 - 2jf^2m + j^2f^4(\ell_1^2+\ell_2^2) \equiv 0 \bmod q. \tag{4.23}$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

Define the lattice

$$\mathcal{L} = \{(n, m, \ell) \in \mathbb{Z}^3 : \ n + jf^2m + j^2f^4\ell \equiv 0 \bmod q\},$$

and the convex body

$$B = \{(n, m, \ell) \in \mathbb{R}^3 : \ |n| \leqslant C_0N^6/\Delta^8, \\ |m| \leqslant C_0N^5/\Delta^8, \ |\ell| \leqslant C_0N^4/\Delta^8\},$$

for a suitable constant C_0. Since for any integer r

$$\#\{n_1, n_2 \in \mathbb{Z} : \ n_1^2 + n_2^2 = r\} \leqslant r^{o(1)},$$

we see that Equation (4.23) implies

$$K^2 \leqslant \#(\mathcal{L} \cap B)\, N^{o(1)}.$$

By Equation (4.8), Equation (4.18) and Lemma 4.3, there exists $(\ell, m, n) \neq (0, 0, 0)$ satisfying

$$|\ell| \leqslant \frac{N^{11+o(1)}}{\Delta^{16}K^2}, \qquad |m| \leqslant \frac{N^{10+o(1)}}{\Delta^{16}K^2}, \qquad |n| \leqslant \frac{N^{9+o(1)}}{\Delta^{16}K^2}, \tag{4.24}$$

and

$$jf^2n \equiv m \bmod q, \quad j^2f^4n \equiv \ell \bmod q. \tag{4.25}$$

Note we may assume

$$\gcd(\ell, m, n) = 1. \tag{4.26}$$

Recall Equation (4.16)

$$\begin{aligned} I(f) \leqslant \#\{(d_1, d_2) \in \mathcal{D}^2 : \ & (n_{d_1}m_{d_2} - n_{d_2}m_{d_1})^2 \\ & - 4jf^2m_{d_1}m_{d_2}(n_{d_1}m_{d_2} + n_{d_2}m_{d_1}) \\ & + 4j^2f^4(m_{d_1}m_{d_2})^2 \equiv 0 \bmod q\}. \end{aligned} \tag{4.27}$$

If d_1, d_2 satisfy the conditions in Equation (4.27), then by Equation (4.25)

$$n(n_{d_1}m_{d_2} - n_{d_2}m_{d_1})^2 - 4mm_{d_1}m_{d_2}(n_{d_1}m_{d_2} + n_{d_2}m_{d_1}) \\ + 4\ell(m_{d_1}m_{d_2})^2 \equiv 0 \bmod q,$$

and hence from Equation (4.8), assuming that N is large enough, we derive

$$n(n_{d_1}m_{d_2} - n_{d_2}m_{d_1})^2 - 4mm_{d_1}m_{d_2}(n_{d_1}m_{d_2} + n_{d_2}m_{d_1}) \\ + 4\ell(m_{d_1}m_{d_2})^2 = 0. \tag{4.28}$$

Similarly by Equations (4.24) and (4.25) we have $m^2 \equiv n\ell \bmod q$ and again Equation (4.8) ensures that

$$m^2 = n\ell.$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

Therefore, Equation (4.28) implies the following equation

$$\left(\frac{n_{d_1}}{m_{d_1}}-\frac{n_{d_2}}{m_{d_2}}\right)^2-4\left(\frac{n_{d_1}}{m_{d_1}}+\frac{n_{d_2}}{m_{d_2}}\right)\left(\frac{m}{n}\right)+4\left(\frac{m}{n}\right)^2=0.$$

We see that

$$\frac{m}{n}=\frac{1}{2}\left(\frac{n_{d_1}}{m_{d_1}}+\frac{n_{d_2}}{m_{d_2}}\right)\pm\frac{\sqrt{n_{d_1}m_{d_1}n_{d_2}m_{d_2}}}{m_{d_1}m_{d_2}}. \tag{4.29}$$

Hence, from Equations (4.13) and (4.27), there exists some constant C such that

$$\begin{aligned}I(f)\leqslant \#\Big\{&(m_{d_1},m_{d_2},n_{d_1},n_{d_2})\in\mathbb{Z}^4:\\ &|m_{d_1}|,|m_{d_2}|\leqslant\frac{CN}{\Delta^2},\ |n_{d_1}|,|n_{d_2}|\leqslant\frac{CN^2}{\Delta^2},\\ &m_{d_1}m_{d_2}n_{d_1}n_{d_2}\neq 0,\text{ and (4.29) holds}\Big\}.\end{aligned}$$

Summing the above over $f\in\mathcal{F}$, using Equation (4.15) and noting that for each ℓ,m,n satisfying Equation (4.26) there exists $O(1)$ values of f satisfying Equation (4.25), we see that $K\#\mathcal{F}$ is bounded by the number of solutions to the Equation (4.29) with integer variables satisfying

$$|m_{d_1}|,|m_{d_2}|\leqslant\frac{CN}{\Delta^2},\qquad |n_{d_1}|,|n_{d_2}|\leqslant\frac{CN^2}{\Delta^2},\qquad n_{d_1}n_{d_2}m_{d_1}m_{d_2}\neq 0.$$

We see from Equation (4.29) that $n_{d_1}m_{d_1}n_{d_2}m_{d_2}=r^2$ for some $r\in\mathbb{Z}$ and hence a bound (3.11) on the divisor function implies

$$K\#\mathcal{F}\leqslant N^{o(1)}\#\left\{\ell\leqslant C^4\frac{N^6}{\Delta^8}:\ \ell=r^2\text{ for some } r\in\mathbb{Z}\right\}\leqslant\frac{N^{3+o(1)}}{\Delta^4},$$

which completes the proof. □

4.2. Concluding the proof

As in Section 3.2, here we work again with $\mathsf{T}_{4,2}(N;\overline{j},q)$ for the multiplicative inverse $\overline{j}$ of j modulo q rather than with $\mathsf{T}_{4,2}(N;j,q)$. Let notation be as in Corollary 4.4 so that

$$\mathsf{T}_{4,2}(N;\overline{j},q)=\sum_{x\in\mathbb{F}_q}(\mathcal{A}\circ\mathcal{A}\circ\mathcal{A}\circ\mathcal{A})(x)^2,$$

where we recall that

$$\mathcal{A}=\{x\in\mathbb{F}_q^*\ :\ jx^2\in[1,N]\}.$$

By Equation (1.5), we may assume that

$$N\leqslant q^{1/3}. \tag{4.30}$$

Applying the dyadic pigeonhole principle, there exist $\Delta_1,\Delta_2\geqslant 1$ and $\mathcal{D}_1,\mathcal{D}_2\subseteq\mathbb{F}_q$ given by

$$\mathcal{D}_j=\{x\in\mathbb{F}_q:\ \Delta_j\leqslant(\mathcal{A}\circ\mathcal{A})(x)<2\Delta_j\},\qquad j=1,2$$

such that

$$\mathsf{T}_{4,2}(N;\bar{j},q) \leqslant N^{o(1)}(\Delta_1\Delta_2)^2 E(\mathcal{D}_1,\mathcal{D}_2),$$

where

$$E(\mathcal{D}_1,\mathcal{D}_2) = \sum_{x\in\mathbb{F}_q}(\mathcal{D}_1 \circ \mathcal{D}_2)(x)^2.$$

By the Cauchy–Schwarz inequality,

$$E(\mathcal{D}_1,\mathcal{D}_2) \leqslant E(\mathcal{D}_1)^{1/2}E(\mathcal{D}_2)^{1/2},$$

and hence there exists some Δ and $\mathcal{D}$ given by

$$\mathcal{D} = \{x \in \mathbb{F}_q : \ \Delta \leqslant (\mathcal{A}\circ\mathcal{A})(x) < 2\Delta\}$$

such that

$$\mathsf{T}_{4,2}(N;\bar{j},q) \leqslant N^{o(1)}\Delta^4 E(\mathcal{D}). \tag{4.31}$$

It is also obvious from Equationi (3.1) that

$$\Delta^2(\#\mathcal{D}) \leqslant \mathsf{T}_{2,2}(N;\bar{j},q), \tag{4.32}$$

and

$$\#\mathcal{D} \leqslant \Delta\#\mathcal{D} \ll N^2. \tag{4.33}$$

Isolating the diagonal contribution in $E(\mathcal{D})$, we write

$$E(\mathcal{D}) = (\#\mathcal{D})^2 + \sum_{f\in\mathbb{F}_q^*}(\mathcal{D}\circ\mathcal{D})(f)^2.$$

We may assume

$$E(\mathcal{D}) \leqslant 2\sum_{f\in\mathbb{F}_q^*}(\mathcal{D}\circ\mathcal{D})(f)^2 \tag{4.34}$$

since otherwise we have $E(\mathcal{D}) \leqslant 2(\#\mathcal{D})^2$ and it follows from the bounds (4.31) and (4.32) that

$$\mathsf{T}_{4,2}(N;\bar{j},q) \leqslant \Delta^4(\#\mathcal{D})^2N^{o(1)} \leqslant \mathsf{T}_{2,2}(N;\bar{j},q)^2N^{o(1)}.$$

Now, recalling the condition (4.30) and using Theorem 1.1, we derive

$$\mathsf{T}_{4,2}(N;\bar{j},q) \leqslant N^{4+o(1)}.$$

By Equation (4.34) and the dyadic pigeonhole principle, there exists some K and a set $\mathcal{F} \subseteq \mathbb{F}_q^*$ given by

$$\mathcal{F} = \{f \in \mathbb{F}_q^* : \ K \leqslant (\mathcal{D}\circ\mathcal{D})(f) < 2K\}$$

such that

$$E(\mathcal{D}) \leqslant K^2\#\mathcal{F}N^{o(1)}. \tag{4.35}$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

Combining with Equations (4.31) and (4.35) gives

$$\mathsf{T}_{4,2}(N;\overline{j},q) \leqslant \Delta^4 K^2 \# \mathcal{F} N^{o(1)}. \tag{4.36}$$

We apply Corollary 4.4 to estimate the right-hand side of Equation (4.36).

We now fix some $\varepsilon > 0$ and suppose first that one of Equation (4.8) or Equation (4.9) does not hold. In particular, assume

$$K < \left(\frac{N^{15/2}}{\Delta^{12} q^{1/2}} + \frac{N^5}{\Delta^8 q^{1/4}} \right) N^{\varepsilon} \tag{4.37}$$

or

$$\Delta < \frac{N^{5/8+\varepsilon}}{q^{1/8}}, \tag{4.38}$$

where we have use the assumption (4.30) to ignore the term $N^{3/2}/q^{1/2}$ in Equation (4.9). If Equation (4.37) holds, then using the trivial bounds

$$K\#\mathcal{F} \leqslant (\#\mathcal{D})^2 \qquad \text{and} \qquad \Delta \# \mathcal{D} \ll N^2,$$

we derive from Equation (4.36)

$$\begin{aligned} \mathsf{T}_{4,2}(N;\overline{j},q) &\leqslant \Delta^4 (\#\mathcal{D})^2 K N^{o(1)} \leqslant \Delta^2 K N^{4+o(1)} \\ &\leqslant \left(\frac{N^{15/2}}{\Delta^{10} q^{1/2}} + \frac{N^5}{\Delta^6 q^{1/4}} \right) N^{4+\varepsilon+o(1)} \\ &\leqslant \left(\frac{N^{15/2}}{q^{1/2}} + \frac{N^5}{q^{1/4}} \right) N^{4+\varepsilon+o(1)} \\ &\leqslant \left(\frac{N^{11/2}}{q^{1/2}} + \frac{N^3}{q^{1/4}} \right) N^{6+\varepsilon+o(1)}. \end{aligned} \tag{4.39}$$

If Equation (4.38) holds, then from Equation (4.36)

$$\begin{aligned} \mathsf{T}_{4,2}(N;\overline{j},q) &\leqslant N^{o(1)} \Delta^4 (\#\mathcal{D})^3 \leqslant N^{6+o(1)} \Delta \\ &\leqslant \frac{N^{6+5/8+o(1)}}{q^{1/8}}. \end{aligned} \tag{4.40}$$

Hence, if one of the conditions (4.8) or (4.9) does not hold then combining Equations (4.39) and (4.40) we obtain

$$\mathsf{T}_{4,2}(N;\overline{j},q) \leqslant \left(\frac{N^{5/8}}{q^{1/8}} + \frac{N^8}{q^{1/2}} \right) N^{6+\varepsilon+o(1)}. \tag{4.41}$$

Suppose next that Equations (4.37) and (4.38) both fail and thus both Equation (4.8) and Equation (4.9) hold. By Corollary 4.4, we have either

$$K \ll 1, \tag{4.42}$$

or

$$K\#\mathcal{F} \leqslant \frac{N^{3+o(1)}}{\Delta^4}. \tag{4.43}$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

If Equation (4.42) holds, then from Equation (4.36) and the trivial bound $K\#\mathcal{F} \leqslant (\#\mathcal{D})^2$, we derive

$$\mathsf{T}_{4,2}(N;\overline{j},q) \leqslant \Delta^4 K^2 \#\mathcal{F} N^{o(1)} \leqslant \Delta^4 K \#\mathcal{F} N^{o(1)} \leqslant \Delta^4 (\#\mathcal{D})^2 N^{o(1)}.$$

Now, the bound (4.32) and Theorem 1.1 (under the condition (4.30)) yield

$$\mathsf{T}_{4,2}(N;\overline{j},q) \leqslant T_{2,2}(N;j,q)^2 N^{o(1)} \leqslant N^{4+o(1)}.$$

If Equation (4.43) holds, then using Equation (4.33)

$$\mathsf{T}_{4,2}(N;\overline{j},q) \leqslant N^{3+o(1)} K \leqslant N^{3+o(1)} \#\mathcal{D} \leqslant N^{5+o(1)}. \tag{4.44}$$

Combining Equations (4.41) and (4.44), since $\varepsilon > 0$ is arbitrary, we complete the proof.

5. Proof of Theorem 1.3

5.1. Product polynomials

In the proof of [26, Lemma 5.1], a certain polynomial in four variables with integer coefficients played a key role. More precisely, it has been found in [26] that the polynomial

$$\begin{aligned} F(U,V,X,Y) &= 64UVXY \\ &\qquad - \left(4UV + 4XY - (X+Y-U-V)^2\right)^2 \end{aligned}$$

has the following property. Letting $U = u^2$, $V = v^2$, $X = x^2$ and $Y = y^2$, one has that $F(u^2,v^2,x^2,y^2) = 0$ for any u,v,x,y for which $u+v = x+y$ (over any commutative ring). We now proceed to discuss this property in a more general context.

Denote $\mathcal{U}_k = \{\omega \in \mathbb{C} : \ \omega^k = 1\}$, and consider the polynomial

$$G_k(X_1,X_2,X_3,X_4) = \prod_{\omega_1,\omega_2,\omega_3 \in \mathcal{U}_k} (\omega_1 X_1 + \omega_2 X_2 - \omega_3 X_3 - X_4)$$

defined over the cyclotomic field $K_k = \mathbb{Q}(\exp(2\pi i/k))$. Since the Galois group $\mathrm{Gal}(K_k/\mathbb{Q})$ of K is cyclic and any automorphism σ of K_k over $\mathbb{Q}$ is a multiplication by some $\omega \in \mathcal{U}_k$, we see that

$$\begin{aligned} &\sigma(G_k(X_1,X_2,X_3,X_4)) \\ &\quad = \prod_{\omega_1,\omega_2,\omega_3 \in \mathcal{U}_k} (\sigma(\omega_1) X_1 + \sigma(\omega_2) X_2 - \sigma(\omega_3) X_3 - \sigma(1) X_4) \\ &\quad = \prod_{\omega_1,\omega_2,\omega_3 \in \mathcal{U}_k} (\omega\omega_1 X_1 + \omega\omega_2 X_2 - \omega\omega_3 X_3 - \omega X_4) \\ &\quad = \omega^{k^3} \prod_{\omega_1,\omega_2,\omega_3 \in \mathcal{U}_k} (\omega_1 X_1 + \omega_2 X_2 - \omega_3 X_3 - X_4) \\ &\quad = G_k(X_1,X_2,X_3,X_4). \end{aligned}$$

Hence, G_k has rational coefficients. Since obviously these coefficients are algebraic integers, we see that $G_k(X_1,X_2,X_3,X_4) \in \mathbb{Z}[X_1,X_2,X_3,X_4]$.

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

We also see that

$$\begin{aligned}
&\prod_{\omega_1,\omega_2,\omega_3\in\mathcal{U}_k}(\omega_1X_1+\omega_2X_2-\omega_3X_3-X_4)\\
&\qquad=\prod_{\omega_1,\omega_2,\omega_3\in\mathcal{U}_k}(\omega_1X_1+\omega_1\omega_2X_2-\omega_1\omega_3X_3-X_4)\\
&\qquad=\prod_{\omega_2,\omega_3\in\mathcal{U}_k}\prod_{\omega_1\in\mathcal{U}_k}(\omega_1(X_1+\omega_2X_2-\omega_3X_3)-X_4)\\
&\qquad=(-1)^k\prod_{\omega_2,\omega_3\in\mathcal{U}_k}\left((X_1+\omega_2X_2-\omega_3X_3)^k-X_4^k\right).
\end{aligned}$$

Therefore, $G_k(X_1,X_2,X_3,X_4)$ is a polynomial in X_4^k. Similarly,

$$\begin{aligned}
&\prod_{\omega_1,\omega_2,\omega_3\in\mathcal{U}_k}(\omega_1X_1+\omega_2X_2-\omega_3X_3-X_4)\\
&\qquad=\prod_{\omega_2,\omega_3\in\mathcal{U}_k}\prod_{\omega_1\in\mathcal{U}_k}\left(X_1+\omega_1^{-1}(\omega_2X_2-\omega_3X_3-X_4)\right)\\
&\qquad=\prod_{\omega_2,\omega_3\in\mathcal{U}_k}\left(X_1^k+(\omega_3X_3+X_4-\omega_2X_2)^k\right).
\end{aligned}$$

Thus, it is also a polynomial in X_1^k and of course also in X_2^k and X_3^k. Hence, we can write

$$G_k(X_1,X_2,X_3,X_4)=F_k\left(X_1^k,X_2^k,X_3^k,X_4^k\right)$$

for some polynomial $F_k(X_1,X_2,X_3,X_4)\in\mathbb{Z}[X_1,X_2,X_3,X_4]$.

Remark 5.1. It is clear that this construction can be extended in several directions, in particular to polynomials $F_{\nu,k}\in\mathbb{Z}[X_1,\ldots,X_{2\nu}]$ such that

$$F_{\nu,k}\left(x_1^k,\ldots,x_{2\nu}^k\right)=0$$

whenever $x_1+\ldots+x_\nu=x_{\nu+1}+\ldots+x_{2\nu}$.

5.2. The zero set of $F_k(X_1,\ X_2,\ X_3,\ X_4)$

We now need the following bound on the number of integer zeros of F_k in a box. Define by $T_k(N)$ by

$$\begin{aligned}
T_k(N)=\#\{(n_1,n_2,n_3,n_4)\in\mathbb{Z}^4:\ &1\leqslant n_1,n_2,n_3,n_4\leqslant N,\\
&F_k(n_1,n_2,n_3,n_4)=0\}.
\end{aligned}$$

Our next result gives a bound for $T_k(N)$.

Lemma 5.2. *Fix an integer $k\geqslant 3$. For any positive integer N, we have $T_k(N)\ll N^2$.*

Proof. Take a solution (n_1,n_2,n_3,n_4) to $F_k(n_1,n_2,n_3,n_4)=0$ satisfying $1\leqslant n_1,n_2,n_3,n_4\leqslant N$. Denote by t_1,t_2,t_3,t_4 the positive real numbers that are roots of order k of n_1,n_2,n_3,n_4, respectively.

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

Therefore, there exist roots of unity $\omega_1,\omega_2,\omega_3 \in \mathcal{U}_k$ such that

$$\omega_1 t_1 + \omega_2 t_2 - \omega_3 t_3 - t_4 = 0. \tag{5.1}$$

We now distinguish two cases.

Case 1. At least one of the roots of unity ω_1, ω_2, ω_3 is not real. Complex conjugation then provides a second linear equation,

$$\bar{\omega}_1 t_1 + \bar{\omega}_2 t_2 - \bar{\omega}_3 t_3 - t_4 = 0. \tag{5.2}$$

which is different from Equation (5.1). Then using Equations (5.1) and (5.2) to eliminate t_4, one obtains a nontrivial linear equation in t_1,t_2 and t_3 which obviously has at most $O(N^2)$ solutions, after which t_4 is uniquely defined.

Thus, the total number of solutions in Case 1 is $O(N^2)$.

Case 2. All three of $\omega_1,\omega_2,\omega_3$ are real, that is, $\omega_1,\omega_2,\omega_3 \in \{-1,1\}$, and Equation (5.1) reduces to

$$t_1 \pm t_2 \pm t_3 \pm t_4 = 0. \tag{5.3}$$

We observe that *Case 2* also covers the $2N^2 + O(N)$ diagonal solutions.

To treat the nondiagonal solutions, one can now apply results of Besicovitch [3], Mordell [22], Siegel [28] or the more recent results of Carr and O'Sullivan [9]. For instance, [9, Theorem 1.1] shows that a set of real k-th roots of integers that are pairwise linearly independent over the rationals must also be linearly independent. Applying this to the set t_1,t_2,t_3,t_4, which by Equation (5.3) is not linearly independent over $\mathbb{Q}$, it follows that two of them, for example, t_1 and t_2, are linearly dependent over $\mathbb{Q}$. We derive that there are positive integers a_1,a_2,b such that

$$t_1^k = n_1 = b a_1^k \qquad \text{and} \qquad t_2^k = n_2 = b a_2^k,$$

where b is not divisible by a k-th power of a prime. That is, a_1^k is the largest k-th power that divides n_1, and a_2^k is the largest k-th power that divides n_2.

Then letting t_5 denote the positive k-th root of b, Equation (5.3) becomes

$$(a_1 \pm a_2) t_5 \pm t_3 \pm t_4 = 0. \tag{5.4}$$

Without loss of generality, we can assume that $a_1 \geqslant a_2$. Hence, for any fixed $1 \leqslant a_2 \leqslant a_1 \leqslant N^{1/k}$ there are at most N/a_1^k possible values for b and thus for t_5. After a_1, a_2 and t_5 are fixed, there are obviously at most N pairs (t_3,t_4) satisfying Equation (5.4). Hence, the total contribution from such solutions is

$$\sum_{1 \leqslant a_2 \leqslant a_1 \leqslant N^{1/k}} N^2/a_1^k \leqslant \sum_{1 \leqslant a_1 \leqslant N^{1/k}} N^2/a_1^{k-1} \ll N^2$$

which concludes the proof. □

We remark that the case of $k=2$ can also be included in Lemma 5.2; however, this case is already fully covered by the results of [26].

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

5.3. Concluding the proof

Clearly, the congruence

$$u+v \equiv x+y \bmod q, \qquad ju^k, jv^k, jx^k, jy^k \in [1,N]$$

implies that

$$F_k(u^k,v^k,x^k,y^k) \equiv 0 \bmod q$$

for the above polynomial F_k. Since F_k is homogeneous, this implies that

$$F_k(ju^k,jv^k,jx^k,jy^k) \equiv 0 \bmod q.$$

Since for a prime $q \sim Q$, $a \in \mathbb{F}_q$ and $j \in \mathbb{F}_q^*$, there are at most k solutions to the congruence $jz^k \equiv a \bmod q$ in variable $z \in \mathbb{F}_q$, and thus at most $2k$ solution in variable $z \in [1,N]$ (since $N \leqslant Q \leqslant 2q$) we have

$$\begin{aligned}\sum_{\substack{q\sim Q\\ q \text{ prime}}} \max_{j\in\mathbb{F}_q^*} \mathsf{E}_k(N;j,q) &= \sum_{\substack{q\sim Q\\ q \text{ prime}}} \max_{j\in\mathbb{F}_q^*} \mathsf{E}_k(N;\overline{j},q)\\ &\leqslant 16k^4 \sum_{\substack{q\sim Q\\ q \text{ prime}}} \sum_{\substack{U,V,X,Y\in[1,N]\\ F_k(U,V,X,Y)\equiv 0 \bmod q}} \!\!\cdots\!\! \sum 1,\end{aligned}$$

where, as before, $\overline{j}$ denotes the multiplicative inverse of j modulo q. Changing the order of summation and separating the sum over the variables U,V,X,Y into two parts depending on whether $F_k(U,V,X,Y) = 0$ or not, we derive

$$\begin{aligned}\sum_{\substack{q\sim Q\\ q \text{ prime}}} \max_{j\in\mathbb{F}_q^*} \mathsf{E}_k(N;j,q) &\ll \sum_{U,V,X,Y\in[1,N]} \!\!\cdots\!\! \sum \sum_{\substack{q\sim Q\\ q \text{ prime}\\ q\mid F_k(U,V,X,Y)}} 1\\ &\ll \frac{Q}{\log Q} \sum_{\substack{U,V,X,Y\in[1,N]\\ F_k(U,V,X,Y)=0}} \!\!\cdots\!\! \sum 1 + \sum_{\substack{U,V,X,Y\in[1,N]\\ F_k(U,V,X,Y)\neq 0}} \!\!\cdots\!\! \sum \sum_{\substack{q\sim Q\\ q \text{ prime}\\ q\mid F_k(U,V,X,Y)}} 1.\end{aligned}$$

Recall that F_k is a polynomial with constant coefficients of degree k^3. Hence, $F_k(U,V,X,Y) \ll N^{k^3}$, and thus trivially has at most $O(\log N)$ prime divisors. Hence, we derive

$$\sum_{\substack{q\sim Q\\ q \text{ prime}}} \max_{j\in\mathbb{F}_q^*} \mathsf{E}_k(N;j,q) \ll \frac{Q}{\log Q} T_k(N) + N^{4+o(1)},$$

and applying Lemma 5.2 we conclude the proof.

Remark 5.3. Furthermore, it is easy to see that there is a constant $C > 0$ such that if $N \leqslant Cq^{1/k^3}$, then $F_k(n_1,n_2,n_3,n_4) \equiv 0 \bmod q$ with $1 \leqslant n_1,n_2,n_3,n_4 \leqslant N$ implies $F_k(n_1,n_2,n_3,n_4) = 0$. Hence, in this range of N, using Lemma 5.2, we obtain $\mathsf{E}_k(N;j,q) \ll N^2$ for every q.

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

6. Proof of Theorem 1.4

6.1. Preliminary discussion

We need some facts about the *Gowers norms*, introduced in the celebrated work of Gowers [16, 17] on the first quantitative bound for the famous Szemerédi Theorem [29] about sets avoiding arithmetic progressions of length four and longer. As an important step in the proof, Gowers [16, 17] observes that there are very random sets having an unexpected number of arithmetic progressions of length $l \geqslant 4$. An example is, basically, the set

$$\mathcal{A}^{(k)} = \left\{x \in \mathbb{Z}_N : \ x^k \in \{1, \ldots, c_k N\}\right\}, \tag{6.1}$$

where $c_k > 0$ is an appropriate constant, depending on $k \geqslant 2$ only (see the beginning of [17, Section 4] and also [18]). Then the set $\mathcal{A}^{(k)}$ has an enormous number of arithmetic progressions of length $k+2$ but the expected number of shorter progressions. In Theorem 1.4, we consider the sets $\mathcal{N}^{1/k}$, where $\mathcal{N}$ is a set with small doubling. Clearly, such sets generalise the construction (6.1). Below, we show that these sets are random in the sense that they all have small additive energy. Actually, we obtain a stronger property that Gowers norms of its characteristic functions are small and thus this has even more parallels to the Gowers construction (6.1). On the other hand, sets $\mathcal{N}^{1/k}$ preserve all essential combinatorial properties of the sets $\mathcal{A}^{(k)}$. For example, for $k = 2$ and any $s \neq 0$ we have for an arbitrary $x \in \mathcal{N}^{1/2} \cap (\mathcal{N}^{1/2} + s)$

$$x^2 \in \mathcal{N} \qquad \text{and} \qquad (x-s)^2 \in \mathcal{N}.$$

Thus, $2sx - s^2 \in \mathcal{N} - \mathcal{N}$ or $x \in (\mathcal{N} - \mathcal{N} + s^2)/2s$. Hence, all intersections $\mathcal{N}^{1/2} \cap (\mathcal{N}^{1/2} + s)$ are additively rich sets exactly as in construction (6.1) (we literally use such facts in the proof of Theorem 1.4 below).

6.2. Gowers norms

Now, we are ready to give general definitions. Suppose that G is an abelian group with the group operation $+$ and $\mathcal{A} \subseteq G$ is a finite set. Having a sequence of elements $s_1, \ldots, s_l \in G$, we define the set

$$\mathcal{A}_{s_1,\ldots,s_l} = \mathcal{A} \cap (\mathcal{A} - s_1) \cap \ldots \cap (\mathcal{A} - s_l).$$

Let $\|\mathcal{A}\|_{\mathcal{U}^k}$ be the Gowers nonnormalised kth-norm [17] of the characteristic function of $\mathcal{A}$ (in additive form). We have (see, for example, [25]):

$$\|\mathcal{A}\|_{\mathcal{U}^k} = \sum_{x_0, x_1, \ldots, x_k \in G} \ \prod_{\varepsilon \in \{0,1\}^k} \mathcal{A}\left(x_0 + \sum_{j=1}^{k} \varepsilon_j x_j\right),$$

where $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_k)$ (we also recall that we use $\mathcal{A}(a)$ for the indicator function of $\mathcal{A}$). In particular,

$$\|\mathcal{A}\|_{\mathcal{U}^2} = \sum_{x_0, x_1, x_2 \in G} \mathcal{A}(x_0)\mathcal{A}(x_0 + x_1)\mathcal{A}(x_0 + x_2)\mathcal{A}(x_0 + x_1 + x_2) = E(\mathcal{A})$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

is the additive energy of $\mathcal{A}$, that is

$$E(\mathcal{A}) = \#\{(a_1,a_2,a_3,a_4) \in \mathcal{A}^4 : \ a_1+a_2 = a_3+a_4\},$$

and

$$\|\mathcal{A}\|_{\mathcal{U}^3} = \sum_{s\in\mathcal{A}-\mathcal{A}} E(\mathcal{A}_s).$$

Moreover, the induction property for Gowers norms holds; see [17]

$$\|\mathcal{A}\|_{\mathcal{U}^{k+1}} = \sum_{s\in\mathcal{A}-\mathcal{A}} \|\mathcal{A}_s\|_{\mathcal{U}^k}$$

and

$$\|\mathcal{A}\|_{\mathcal{U}^k} = \sum_{s_1,\ldots,s_k\in G} \#\mathcal{A}_{\pi(s_1,\ldots,s_k)}, \tag{6.2}$$

where $\pi(s_1,\ldots,s_k)$ is a vector with 2^k components, namely,

$$\pi(s_1,\ldots,s_k) = \left(\sum_{j=1}^k s_j\varepsilon_j\right)_{(\varepsilon_1,\ldots,\varepsilon_k)\in\{0,1\}^k}.$$

Notice also

$$\|\mathcal{A}\|_{\mathcal{U}^{k+1}} = \sum_{s_1,\ldots,s_k\in G} \left(\#\mathcal{A}_{\pi(s_1,\ldots,s_k)}\right)^2. \tag{6.3}$$

It is proved in [17] that kth-norms of the characteristic function of any set are connected to each other. It is shown in [25] that the connection for the nonnormalised norms does not depend on size of the group G. Here, we formulate a particular case of [25, Proposition 35], which relates $\|\mathcal{A}\|_{\mathcal{U}^k}$ and $\|\mathcal{A}\|_{\mathcal{U}^2}$.

Lemma 6.1. *Let $\mathcal{A}$ be a finite subset of an abelian group G with the group operation $+$. Then for any integer $k\geqslant 1$, we have*

$$\|\mathcal{A}\|_{\mathcal{U}^{k+1}} \geqslant \frac{\|\mathcal{A}\|_{\mathcal{U}^k}^{(3k-2)/(k-1)}}{\|\mathcal{A}\|_{\mathcal{U}^{k-1}}^{2k/(k-1)}}.$$

Next, we have to relate $\|\mathcal{A}\|_{\mathcal{U}^k}$ and $E(\mathcal{A})$; see [25, Remark 36].

Lemma 6.2. *Let $\mathcal{A}$ be a finite subset of an abelian group G with the group operation $+$. Then for any integer $k\geqslant 1$, we have*

$$\|\mathcal{A}\|_{\mathcal{U}^k} \geqslant E(\mathcal{A})^{2^k-k-1}(\#\mathcal{A})^{-(3\cdot 2^k-4k-4)}.$$

6.3. Concluding the proof

Let $\mathcal{A} = \mathcal{N}^{1/k}$.

6.3.1. Case $k=3$. Let us start with the case $k=3$. Below, we can assume that the quantity L is sufficiently small because otherwise the result is trivial.

For any $s \neq 0$, consider the set $\mathcal{A}_s = \mathcal{A} \cap (\mathcal{A} - s)$ and let $x \in \mathcal{A}_s$. Then $x^3, (x+s)^3 \in \mathcal{N}$ and hence

$$3s(x+s/2)^2 + s^3/4 = 3sx^2 + 3s^2x + s^3 \in \mathcal{N} - \mathcal{N}.$$

Put $\mathcal{B}_s = \mathcal{A}_s + s/2$, so $\#\mathcal{B}_s = \#\mathcal{A}_s$. Furthermore, let $\mathcal{C}_s = \{x^2 : \ x \in \mathcal{B}_s\}$. Clearly, by the Plünnecke inequality (see [30, Corollary 6.29]),

$$\#(\mathcal{C}_s + \mathcal{C}_s) \leqslant \#(2\mathcal{N} - 2\mathcal{N}) \leqslant L^4 N = L_s \#\mathcal{A}_s,$$

where

$$L_s = \frac{L^4 N}{\#\mathcal{A}_s}.$$

Then, after applying estimate (1.3) with our restriction $N \leqslant q^{2/3}$, we obtain

$$\begin{aligned} E(\mathcal{A}_s) = E(\mathcal{B}_s) &\ll E_2(\mathcal{C}_s; q) \\ &\leqslant \left(L_s^4 (\#\mathcal{A}_s)^4 / q + L_s^2 (\#\mathcal{A}_s)^{11/4}\right) q^{o(1)}. \end{aligned} \tag{6.4}$$

We now assume that

$$\#\mathcal{A}_s \geqslant N^{4/5} L^{32/5}. \tag{6.5}$$

We also observe that we can always assume that $L \leqslant N^{1/32}$ as otherwise the result is trivial. Further, to show that the second term in Equation (6.4) dominates the first one, we need to check that

$$L_s^4 (\#\mathcal{A}_s)^4 / q \leqslant L_s^2 (\#\mathcal{A}_s)^{11/4} \tag{6.6}$$

or $L_s^2 (\#\mathcal{A}_s)^{5/4} \leqslant q$, which in turn is equivalent to $(\#\mathcal{A}_s)^3 \geqslant L^{32} N^8 q^{-4}$. Since for $L \leqslant N^{1/32}$ and $N \leqslant q^{2/3}$, we have

$$N^{12/5} L^{96/5} \geqslant L^{32} N^8 q^{-4},$$

we see that under the assumption (6.5) we have Equation (6.6) and hence the bound (6.4) becomes

$$E(\mathcal{A}_s) \leqslant L_s^2 (\#\mathcal{A}_s)^{11/4} q^{o(1)} \leqslant L^8 N^2 (\#\mathcal{A}_s)^{3/4} q^{o(1)}. \tag{6.7}$$

By the definition of the sets $\mathcal{A}_s$, we have

$$\sum_{s \in \mathcal{A} - \mathcal{A}} \#\mathcal{A}_s = (\#\mathcal{A})^2. \tag{6.8}$$

Furthermore, using the definition of $\mathcal{U}_3$–norm we write

$$\|\mathcal{A}\|_{\mathcal{U}^3} = \sum_{s \in \mathcal{A} - \mathcal{A}} E(\mathcal{A}_s) = \sum_{s:\, \#\mathcal{A}_s \leqslant T} E(\mathcal{A}_s) + \sum_{s:\, \#\mathcal{A}_s > T} E(\mathcal{A}_s). \tag{6.9}$$

First, we observe that

$$\begin{aligned} \sum_{s:\, \#\mathcal{A}_s \leqslant T} E(\mathcal{A}_s) = \#\{(a_1, a_2, a_3, a_4, s) \in \mathcal{A}^4 \times (\mathcal{A} - \mathcal{A}) :& \\ a_1 + a_2 = a_3 + a_4,\ \#\mathcal{A}_s \leqslant T,& \\ a_i - s \in \mathcal{A},\ i = 1, \ldots, 4\}.& \end{aligned}$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

Thus, for each of $E(\mathcal{A})$ choices of quadruples $(a_1,a_2,a_3,a_4)\in\mathcal{A}^4$ with $a_1+a_2=a_3+a_4$, there are at most T possibilities for s with $\#\mathcal{A}_s\leqslant T$ and we derive

$$\sum_{s:\,\#\mathcal{A}_s\leqslant T} E(\mathcal{A}_s)\leqslant TE(\mathcal{A}). \tag{6.10}$$

We now choose

$$T=27E(\mathcal{A})^{-4/5}L^{32/5}N^{16/5} \tag{6.11}$$

and note that the trivial upper bound $E(\mathcal{A})\leqslant(\#\mathcal{A})^3\leqslant 27N^3$ implies that $T\geqslant N^{4/5}L^{32/5}$. Hence, for any s with $\#\mathcal{A}_s>T$ the condition (6.5) is satisfied and so the bound (6.7) holds.

Hence, by identity (6.8), we obtain

$$\begin{aligned}\sum_{s:\,\#\mathcal{A}_s>T} E(\mathcal{A}_s) &\leqslant L^8N^2q^{o(1)}\sum_{s:\,\#\mathcal{A}_s>T}(\#\mathcal{A}_s)^{3/4}\\ &\leqslant L^8N^2T^{-1/4}q^{o(1)}\sum_{s:\,\#\mathcal{A}_s>T}\#\mathcal{A}_s \\ &\leqslant L^8N^2\cdot N^2T^{-1/4}q^{o(1)}=L^8N^4T^{-1/4}q^{o(1)}.\end{aligned} \tag{6.12}$$

The value of T in Equation (6.11) is chosen to balance the bounds (6.10) and (6.12) and thus from Equation (6.9) we derive

$$\|\mathcal{A}\|_{\mathcal{U}^3}\leqslant E(\mathcal{A})^{1/5}L^{32/5}N^{16/5}q^{o(1)}.$$

Finally, applying Lemma 6.2, we obtain

$$E(\mathcal{A})\leqslant N^2\|\mathcal{A}\|_{\mathcal{U}^3}^{1/4}\leqslant L^{8/5}N^{14/5}E(\mathcal{A})^{1/20}q^{o(1)},$$

and whence

$$E(\mathcal{A})\leqslant L^{32/19}N^{56/19}q^{o(1)},$$

which gives the desired result for $k=3$.

6.3.2. Case $k=4$.

Next, we consider the case $k=4$. Let

$$\mathcal{A}_{\pi(s,t)}=\mathcal{A}\cap(\mathcal{A}-s)\cap(\mathcal{A}-t)\cap(\mathcal{A}-s-t),$$

and let $x\in\mathcal{A}_{\pi(s,t)}$. Then $x^4,(x+s)^4,(x+t)^4,(x+t+s)^4\in\mathcal{N}$ and hence $\mathcal{N}-\mathcal{N}$ contains

$$4ux^3+6u^2x^2+4u^3x+u^4,\qquad u\in\{s,t,s+t\}.$$

Subtracting the expressions with s and t from the expression with $s+t$, we see that $3\mathcal{N}-3\mathcal{N}$ contains $12stx^2+12(t^2s+ts^2)x+(t+s)^4-s^4-t^4$ and we can apply a version of previous arguments. Actually, in our particular case $k=4$ one can write exact identity

$$(x+t+s)^4+x^4-(x+s)^4-(x+t)^4=12stx^2+12(t^2s+ts^2)x+(t+s)^4-s^4-t^4$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

and thus even it is enough to consider the set $2\mathcal{N}-2\mathcal{N}$. In particular, since by the Plünnecke inequality (see [30, Corollary 6.29])

$$\#(2\mathcal{N}-2\mathcal{N})\leqslant L^4N,$$

the role of L_s is now played by

$$L_{s,t}=\frac{L^8N}{\#\mathcal{A}_{\pi(s,t)}}.$$

We also set

$$T=(E(\mathcal{A})N^2L^{16}\|\mathcal{A}\|_{\mathcal{U}^3}^{-1})^{4/5}$$

and note that we have the trivial bound $\|\mathcal{A}\|_{\mathcal{U}^3}\leqslant NE(\mathcal{A})$. We also have

$$T\geqslant N^{4/5}L^{64/5}.$$

We now verify that $T^3\geqslant L^{64}N^8q^{-4}$ or

$$N^{12/5}L^{192/5}\geqslant L^{64}N^8q^{-4}$$

which is equivalent to $N^{28}L^{128}\leqslant q^{20}$. Since we can clearly assume that $L\leqslant N^{1/64}$ as otherwise the result is trivial, the last inequality hold under our assumption $N\leqslant q^{2/3}$.

Hence, similar to the case $k=3$ after simple calculations, one verifies that for $\#\mathcal{A}_{s,t}>T$, we have $L_{s,t}^2\left(\#\mathcal{A}_{\pi(s,t)}\right)^{5/4}\leqslant q$ which in turn is equivalent to

$$\left(\#\mathcal{A}_{\pi(s,t)}\right)^3\geqslant T^3\geqslant L^{64}N^8q^{-4}.$$

Therefore, by Equation (1.3), we have

$$\begin{aligned}E(\mathcal{A}_{\pi(s,t)})&\leqslant\left(L_{s,t}^4\left(\#\mathcal{A}_{\pi(s,t)}\right)^4/q+L_{s,t}^2\left(\#\mathcal{A}_{s,t}\right)^{11/4}\right)q^{o(1)}\\&\leqslant L_{s,t}^2\left(\#\mathcal{A}_{s,t}\right)^{11/4}q^{o(1)}\\&=L^{16}N^2\left(\#\mathcal{A}_{\pi(s,t)}\right)^{3/4}q^{o(1)}.\end{aligned}$$

Using Equations (6.2) and (6.3) and the arguments as above, we get

$$\begin{aligned}\|\mathcal{A}\|_{\mathcal{U}^4}&=\sum_{s,t}E(\mathcal{A}_{\pi(s,t)})\\&\leqslant T\|\mathcal{A}\|_{\mathcal{U}^3}+L^{16}N^2q^{o(1)}\sum_{(s,t):\,\#\mathcal{A}_{\pi(s,t)}>T}\#(\mathcal{A}_{\pi(s,t)})^{3/4}\\&\leqslant T\|\mathcal{A}\|_{\mathcal{U}^3}+L^{16}N^2E(\mathcal{A})T^{-1/4}q^{o(1)}\\&\leqslant L^{64/5}N^{8/5}E^{4/5}(\mathcal{A})\|\mathcal{A}\|_{\mathcal{U}^3}^{1/5}q^{o(1)}\end{aligned}\tag{6.13}$$

since again we have chosen T to optimise the above bound.

On the other hand, applying Lemma 6.1 and then Lemma 6.2, we derive

$$\|\mathcal{A}\|_{\mathcal{U}^4}\geqslant\frac{\|\mathcal{A}\|_{\mathcal{U}^3}^{7/2}}{\|\mathcal{A}\|_{\mathcal{U}^2}^3}=\frac{\|\mathcal{A}\|_{\mathcal{U}^3}^{7/2}}{E^3(\mathcal{A})}\geqslant\|\mathcal{A}\|_{\mathcal{U}^3}^{1/5}\cdot\frac{E^{51/5}(\mathcal{A})}{N^{132/5}}.\tag{6.14}$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

Comparing Equations (6.13) and (6.14)

$$E(\mathcal{A}) \leqslant L^{64/47} N^{3-1/47} q^{o(1)},$$

which gives the desired result for $k=4$.

6.3.3. Case $k \geqslant 5$. Finally, consider the general case, which we treat with a version of *Weyl differencing*. Now,

$$\mathcal{A}_s = \mathcal{A}_{\pi(s_1,\dots,s_{k-2})}$$

and let $x \in \mathcal{A}_{\pi(s_1,\dots,s_{k-2})}$. Indeed, we start with $\mathcal{A}_{s_1}$ and reduce the main term in $x^k, (x+s_1)^k \in \mathcal{N}$ deriving that $p_{k-1}(x) \in \mathcal{N} - \mathcal{N}$, where $\deg p_{k-1} = k-1$. After that consider $(\mathcal{A}_{s_1})_{s_2} = \mathcal{A}_{\pi(s_1,s_2)}$ and reduce degree of the polynomial by one, and so on. We also note that by the Plünnecke inequality (see [30, Corollary 6.29])

$$\#\left(2^{k-1}\mathcal{N} - 2^{k-1}\mathcal{N}\right) \leqslant L^{2^k} N,$$

the role of L_s or $L_{s,t}$ is now played by

$$L_s = \frac{L^{2^k} N}{\#\mathcal{A}_{\pi(s)}}.$$

We now set

$$T = \left(N^2 L^{2^{k+1}} \|\mathcal{A}\|_{\mathcal{U}^{k-2}} \|\mathcal{A}\|_{\mathcal{U}^{k-1}}^{-1}\right)^{4/5}.$$

Using the same arguments as above, after somewhat tedious calculations to verify all necessary conditions such as

$$N^8 L^{2^{k+3}} q^{-4} \leqslant \left(\#\mathcal{A}_{\pi(s_1,\dots,s_{k-2})}\right)^3 \tag{6.15}$$

to obtain

$$E(\mathcal{A}_{\pi(s_1,\dots,s_{k-2})}) \leqslant L^{2^{k+1}} N^2 \left(\#\mathcal{A}_{\pi(s_1,\dots,s_{k-2})}\right)^{3/4} q^{o(1)}.$$

In particular, to check Equation (6.15) we note that for the above choice of T we have

$$T \geqslant N^{4/5} L^{2^{k+3}/5}$$

and then derive

$$N^8 L^{2^{k+3}} q^{-4} \leqslant N^{12/5} L^{3 \cdot 2^{k+3}/5} \leqslant T^3$$

which is true because $N \leqslant q^{2/3}$ and $L \leqslant N^{1/2^{k+3}}$ (which we can assume as otherwise the bound is trivial).

Using the formula (6.2) and Equation (6.3), we obtain

$$\begin{aligned}
\|\mathcal{A}\|_{\mathcal{U}^k} &\leqslant T \|\mathcal{A}\|_{\mathcal{U}^{k-1}} + L^{2^{k+1}} N^2 q^{o(1)} \sum_{s:\, \#\mathcal{A}_{\pi(s)} > T} \#(\mathcal{A}_{\pi(s)})^{3/4} \\
&\leqslant T \|\mathcal{A}\|_{\mathcal{U}^{k-1}} + L^{2^{k+1}} N^2 \|\mathcal{A}\|_{\mathcal{U}^{k-2}} T^{-1/4} q^{o(1)} \\
&\leqslant L^{2^{k+1} \cdot 4/5} N^{8/5} \|\mathcal{A}\|_{\mathcal{U}^{k-2}}^{4/5} \|\mathcal{A}\|_{\mathcal{U}^{k-1}}^{1/5} q^{o(1)}
\end{aligned}$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

and hence by induction and Lemma 6.2

$$E(\mathcal{A})^{7\cdot 2^{k-1}-9} \leqslant L^{2^{k+3}} N^{21\cdot 2^{k-1}-28} q^{o(1)}.$$

In other words,

$$E(\mathcal{A}) \leqslant L^{2^{k+3}/(7\cdot 2^{k-1}-9)} N^{3-1/(7\cdot 2^{k-1}-9)} q^{o(1)},$$

which completes the proof.

7. Proof of Theorem 2.2

Given a function $f : \mathbb{F}_q \to \mathbb{C}$, we define the Fourier transform of f by

$$\widehat{f}(n) = \frac{1}{q^{1/2}} \sum_{\lambda \in \mathbb{F}_q} f(\lambda)\, \mathbf{e}_q(\lambda n).$$

Define

$$f_m(n) = \sum_{\substack{x \in \mathbb{F}_q \\ x^2 = amn}} \mathbf{e}_q(hx) \tag{7.1}$$

so that

$$V_{a,q}(\boldsymbol{\alpha}, \varphi; h, M, N) = \sum_{m \sim M} \alpha_m \sum_{n \in \mathbb{Z}} \varphi(n) f_m(n).$$

Recall that φ satisfies Equation (2.2).

Applying Poisson summation to the sum over n gives

$$V_{a,q}(\boldsymbol{\alpha}, \varphi; h, M, N) = \frac{N}{q^{1/2}} \sum_{m \sim M} \alpha_m \sum_{n \in \mathbb{Z}} \widehat{\varphi}\left(-\frac{n}{q}\right) \widehat{f}_m(n), \tag{7.2}$$

where

$$\widehat{f}_m(n) = \frac{1}{q^{1/2}} \sum_{\lambda \in \mathbb{F}_q} f_m(\lambda)\, \mathbf{e}_q(\lambda n).$$

Using Equation (7.1) and interchanging summation

$$\begin{aligned} \widehat{f}_m(n) &= \frac{1}{q^{1/2}} \sum_{x \in \mathbb{F}_q} \sum_{\substack{\lambda \in \mathbb{F}_q \\ x^2 = am\lambda}} \mathbf{e}_q(hx)\, \mathbf{e}_q(\lambda n) \\ &= \frac{1}{q^{1/2}} \sum_{x \in \mathbb{F}_q} \mathbf{e}_q(\overline{am} n x^2 + hx), \end{aligned}$$

where $\overline{am}$ denotes multiplicative inverse modulo q. Summation over x is a quadratic Gauss sum which has evaluation (see [5, Theorem 1.52])

$$\widehat{f}_m(n) = \varepsilon_q \chi(amn)\, \mathbf{e}_q(-am\overline{4n}h^2),$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

for some $|\varepsilon_q|=1$, where χ is the quadratic character mod q. Therefore, there exists some integer c with $\gcd(c,q)=1$ depending on a and h such that

$$\widehat{f}_m(n)=\varepsilon_q\chi(amn)\,\mathbf{e}_q(cm\overline{n}).$$

Substituting this into Equation (7.2) and applying the triangle inequality, we obtain

$$|V_{a,q}(\boldsymbol{\alpha},\varphi;h,M,N)|\ll\frac{1}{q^{1/2}}\sum_{m\sim M}\left|\sum_{n\in\mathbb{Z}}\widehat{\varphi}\left(-\frac{n}{q}\right)\chi(n)\,\mathbf{e}_q(cm\overline{n})\right|.$$

Our next step is to apply linear shifts in a similar fashion to Friedlander and Iwaniec's generalisation of the Burgess bound for character sums [15]. Define

$$U=\frac{q}{MN}, \tag{7.3}$$

so by assumption on M,N we have $U\gg 1$. For fixed $m\sim M$ apply shifts $n\to n+um$ to the inner summation over n. Averaging this over $1\leqslant u\leqslant U$ gives

$$\begin{aligned}&V_{a,q}(\boldsymbol{\alpha},\varphi;h,M,N)\\&\quad\ll\frac{1}{q^{1/2}U}\sum_{m\sim M}\sum_{n\in\mathbb{Z}}\\&\qquad\left|\sum_{1\leqslant u\leqslant U}\widehat{\varphi}\left(-\frac{n+mu}{q}\right)\chi(n+mu)\,\mathbf{e}_q(cm(\overline{n+mu}))\right|.\end{aligned}$$

Let $\varepsilon>0$ be small. Note by Equation (2.2) and partial integration, for any $m\sim M$, $1\leqslant u\leqslant U$ and constant $C>0$ we have

$$\widehat{\varphi}\left(-\frac{n+mu}{q}\right)\ll\frac{1}{n^C},\quad\text{provided}\quad n\geqslant\frac{q^{1+\varepsilon}}{N}.$$

Therefore,

$$\begin{aligned}&V_{a,q}(\boldsymbol{\alpha},\varphi;h,M,N)\\&\quad\ll\frac{1}{q^{1/2}U}\sum_{m\sim M}\sum_{|n|\leqslant q^{1+\varepsilon}/N}\\&\qquad\left|\sum_{1\leqslant u\leqslant U}\widehat{\varphi}\left(-\frac{n+mu}{q}\right)\chi(n+mu)\,\mathbf{e}_q(cm(\overline{n+mu}))\right|.\end{aligned}$$

Applying partial summation to u and using

$$\frac{\partial\widehat{\varphi}\left(-\frac{n+mu}{q}\right)}{\partial u}\ll\frac{N}{|u|},$$

we obtain

$$V_{a,q}(\boldsymbol{\alpha},\varphi;h,M,N) \ll \frac{N^{1+o(1)}}{q^{1/2}U} \sum_{m\sim M} \sum_{|n|\leqslant q^{1+\varepsilon}/N} \left| \sum_{1\leqslant u\leqslant U_0} \chi(n\overline{m}+u)\,\mathbf{e}_q(c\overline{(n\overline{m}+u)}) \right|,$$

for some $U_0 \leqslant U$. Let $I(\lambda)$ count the number of solutions to

$$\lambda \equiv nm^{-1} \bmod q, \quad |n| \leqslant \frac{q^{1+o(1)}}{N}, \quad m \sim M$$

so that

$$V_{a,q}(\boldsymbol{\alpha},\varphi;h,M,N) \leqslant \frac{N^{1+o(1)}}{q^{1/2}U} \sum_{\lambda\in\mathbb{F}_q} I(\lambda) \left| \sum_{1\leqslant u\leqslant U_0} \chi(\lambda+u)\,\mathbf{e}_q(c\overline{(\lambda+u)}) \right|. \tag{7.4}$$

Note

$$\sum_{\lambda\in\mathbb{F}_q} I(\lambda) \ll \frac{q^{1+\varepsilon}M}{N}, \tag{7.5}$$

and

$$\sum_{\lambda\in\mathbb{F}_q} I(\lambda)^2 = \#\{(m_1,m_2,n_1,n_2)\in\mathbb{Z}^4 : \ n_1m_2 \equiv n_2m_2 \bmod q, \quad |n_1|,|n_2| \leqslant \frac{q^{1+\varepsilon}}{N},\ m_1,m_2 \sim M\}.$$

It is known (see, for example, [2]) that

$$\sum_{\lambda\in\mathbb{F}_q} I(\lambda)^2 \leqslant q^{2\varepsilon+o(1)} \left(\frac{1}{q}\left(\frac{qM}{N}\right)^2 + \frac{qM}{N} + M^2 \right),$$

and by assumptions on M,N the above simplifies to

$$\sum_{\lambda\in\mathbb{F}_q} I(\lambda)^2 \ll \frac{q^{1+2\varepsilon}M}{N}. \tag{7.6}$$

Applying the Hölder inequality to summation in Equation (7.4) gives

$$V_{a,q}(\boldsymbol{\alpha},\varphi;h,M,N)^{2r} \ll \frac{N^{2r+o(1)}}{q^rU^{2r}} \left(\sum_{\lambda\in\mathbb{F}_q} I(\lambda)\right)^{2r-2} \left(\sum_{\lambda\in\mathbb{F}_q} I(\lambda)^2\right) \times \sum_{\lambda\in\mathbb{F}_q} \left| \sum_{1\leqslant u\leqslant U_0} \chi(\lambda+u)\,\mathbf{e}_q(c\overline{(\lambda+u)}) \right|^{2r}.$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

Using Equations (7.5) and (7.6)

$$V_{a,q}(\boldsymbol{\alpha},\varphi;h,M,N)^{2r} \leqslant q^{r-1+4r\varepsilon+o(1)}NM^{2r-1}\frac{1}{U^{2r}}\sum_{\lambda\in\mathbb{F}_q}\left|\sum_{1\leqslant u\leqslant U_0}\chi(\lambda+u)\,\mathbf{e}_q(c\overline{(\lambda+u)})\right|^{2r}.$$

Expanding the $2r$-th power, interchanging summation, isolating the diagonal contribution and using the Weil bound (see [24, pg. 45, Theorem 2G]) gives

$$\sum_{\lambda\in\mathbb{F}_q}\left|\sum_{1\leqslant u\leqslant U_0}\chi(\lambda+u)\mathbf{e}_q(c\overline{(\lambda+u)})\right|^{2r} \ll q^{1/2}U^{2r}+qU^r.$$

Using the above and recalling Equation (7.3), we get

$$\begin{aligned}V_{a,q}(\boldsymbol{\alpha},\varphi;h,M,N)^{2r} &\ll q^{r-1+4r\varepsilon+o(1)}NM^{2r-1}\left(q^{1/2}+\frac{q}{U^r}\right)\\ &\ll q^{r-1/2+4r\varepsilon+o(1)}NM^{2r-1}\left(1+\frac{(MN)^r}{q^{r-1/2}}\right),\end{aligned}$$

from which the result follows after taking ε sufficiently small.

8. Proof of Theorem 2.3

8.1. Preliminaries

Our argument follows the proof of [13, Theorem 1.10], the only difference being our use of Corollary 2.1 and Theorem 2.2. We refer the reader to [13, Section 7] for more complete details.

Let $\widetilde{S}_q(h,P)$ denote the sum

$$\widetilde{S}_q(h,P)=\sum_{k=1}^{P}\Lambda(k)\sum_{\substack{x\in\mathbb{F}_q\\ x^2=k}}\mathbf{e}_q(hx).$$

By partial summation, it is sufficient to show

$$\widetilde{S}_q(h,P)\ll q^{o(1)}(P^{15/16}+q^{1/8}P^{3/4}+q^{1/16}P^{69/80}+q^{13/88}P^{3/4}).$$

Let $J\geqslant 1$ be an integer. Using the Heath–Brown identity and a smooth partition of unity as in [13, Section 1.7], there exist some

$$\mathbf{V}=(M_1,\ldots,M_J,N_1,\ldots,N_J)\in[1/2,2P]^{2J}$$

$2J$-tuple of parameters satisfying

$$N_1\geqslant\ldots\geqslant N_J,\quad M_1,\ldots,M_J\leqslant P^{1/J},\quad P\ll Q\ll P,$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

(implied constants are allowed to depend on J),

$$Q = \prod_{i=1}^{J} M_i \prod_{j=1}^{J} N_j, \tag{8.1}$$

and

- the arithmetic functions $m_i \mapsto \gamma_i(m_i)$ are bounded and supported in $[M_i/2, 2M_i]$;
- the smooth functions $x_i \mapsto V_i(x)$ have support in $[1/2, 2]$ and satisfy

  $$V_i^{(j)}(x) \ll q^{j\varepsilon}$$

  for all integers $j \geqslant 0$, where the implied constant may depend on j and ε

such that defining

$$\Sigma(\mathbf{V}) = \sum_{m_1,\ldots,m_J=1}^{\infty} \gamma_1(m_1)\cdots\gamma_J(m_J) \sum_{n_1,\ldots,n_J=1}^{\infty}$$

$$V_1\left(\frac{n_1}{N_1}\right)\cdots V_J\left(\frac{n_J}{N_J}\right) \sum_{\substack{x\in\mathbb{F}_q \\ x^2 = m_1\cdots m_J n_1\cdots n_J}} \mathbf{e}_q(hx),$$

we have

$$\widetilde{S}_q(h,P) \ll P^{o(1)}\Sigma(\mathbf{V}).$$

We proceed on a case-by-case basis depending on the size of N_1. We first note a general estimate for the multilinear sums. Let $\mathcal{I},\mathcal{J} \subseteq \{1,\ldots,J\}$, and write

$$M = \prod_{i\in\mathcal{I}} M_i \prod_{j\in\mathcal{J}} N_j, \quad N = Q/M.$$

Grouping variables in $\Sigma(\mathbf{V})$ according to $\mathcal{I},\mathcal{J}$, there exists α,β satisfying

$$\|\alpha\|_\infty, \|\beta\|_\infty = Q^{o(1)}$$

such that

$$\Sigma(\mathbf{V}) = \sum_{\substack{m\leqslant 2^J M \\ n\leqslant 2^J N}} \alpha(m)\beta(n) \sum_{\substack{x\in\mathbb{F}_q \\ x^2 = mn}} \mathbf{e}_q(hx).$$

By Corollary 2.1,

$$\begin{aligned}\Sigma(\mathbf{V}) &\\ &\leqslant q^{1/8+o(1)}P^{3/4}\left(\frac{P^{3/16}}{q^{1/16}M^{3/16}}+1\right)\left(\frac{M^{3/16}}{q^{1/16}}+1\right) \\ &\leqslant q^{o(1)}\left(P^{15/16}+\frac{q^{1/16}P^{15/16}}{M^{3/16}}+q^{1/16}P^{3/4}M^{3/16}+q^{1/8}P^{3/4}\right).\end{aligned} \tag{8.2}$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

We proceed on a case by case basis depending on the size of N_1. Let $P^{1/2} \geqslant H \geqslant P^{\varepsilon}$ be some parameters and take

$$J = \lceil \log P / \log H \rceil.$$

8.2. Small N_1

Suppose first $N_1 \leqslant H$, then arguing as in [13, Equation (7.13)] we can choose two arbitrary sets $\mathcal{I}, \mathcal{J} \subseteq \{1, \ldots, J\}$ such that for

$$M = \prod_{i \in \mathcal{I}} M_i \prod_{j \in \mathcal{J}} N_j \qquad \text{and} \qquad N = Q/M,$$

where Q is given by Equation (8.1) and we have

$$P^{1/2} \ll M \ll H^{1/2} P^{1/2}.$$

Hence, by Equation (8.2)

$$\Sigma(\mathbf{V}) \leqslant q^{o(1)} \left(P^{15/16} + q^{1/16} P^{27/32} H^{3/32} + q^{1/8} P^{3/4} \right). \tag{8.3}$$

8.3. Medium N_1

Let L be a parameter satisfying $H \leqslant L$, and suppose next that

$$H \leqslant N_1 \leqslant L.$$

We may also suppose

$$H \leqslant N_2 \leqslant N_1 \leqslant L,$$

as otherwise we may argue as before to obtain the bound (8.3). In this case, we define M, N as

$$N = \prod_{i=1}^{J} M_i \prod_{j=3}^{J} N_j \quad \text{and} \quad M = N_1 N_2$$

so that

$$H^2 \leqslant M \leqslant L^2.$$

By Equation (8.2)

$$\Sigma(\mathbf{V}) \leqslant q^{o(1)} \left(P^{15/16} + \frac{q^{1/16} P^{15/16}}{H^{3/8}} + q^{1/16} P^{3/4} L^{3/8} + q^{1/8} P^{3/4} \right). \tag{8.4}$$

https://doi.org/10.1017/S1474748023000397 Published online by Cambridge University Press

8.4. Large N_1

Let R be a parameter to be chosen later and satisfying $R \geqslant cP^{1/2}$ for some sufficiently large constant $c > 0$. Suppose next that

$$L^2 \leqslant N_1 \leqslant R.$$

Taking $M = N_1$ as above, we derive from Equation (8.2)

$$\Sigma(\mathbf{V}) \leqslant q^{o(1)} \left(P^{15/16} + \frac{q^{1/16} P^{15/16}}{L^{3/8}} + q^{1/16} P^{3/4} R^{3/16} + q^{1/8} P^{3/4} \right). \tag{8.5}$$

8.5. Very large N_1

Finally, consider when $N_1 \geqslant R$. We now intend to apply Theorem 2.2 with $P/N_1 \ll M \ll P/N_1$ and $N = N_1$, where we notice that the condition $R \geqslant cP^{1/2}$ ensures that $M < N$, provided that c is large enough. Choosing $r = 2$, we obtain

$$\begin{aligned} \Sigma(\mathbf{V}) &\leqslant q^{3/8+o(1)} (P/N_1)^{3/4} N_1^{1/4} \left(1 + \frac{P^{1/2}}{q^{3/8}} \right) \\ &= q^{3/8+o(1)} P^{3/4} N_1^{-1/2} \left(1 + \frac{P^{1/2}}{q^{3/8}} \right). \end{aligned}$$

Using the assumption $P \leqslant q^{3/4}$, we obtain

$$\Sigma(\mathbf{V}) \leqslant q^{3/8+o(1)} \frac{P^{3/4}}{R^{1/2}}. \tag{8.6}$$

8.6. Optimisation

Combining all previous bounds (8.3), (8.4), (8.5) and (8.6) results in

$$\begin{aligned} \widetilde{S}_q(h,P) \leqslant\ & q^{o(1)} (P^{15/16} + q^{1/8} P^{3/4}) \\ & + q^{o(1)} \left(q^{1/16} P^{27/32} H^{3/32} + \frac{q^{1/16} P^{15/16}}{H^{3/8}} \right) \\ & + q^{o(1)} \left(q^{1/16} P^{3/4} L^{3/8} + \frac{q^{1/16} P^{15/16}}{L^{3/8}} \right) \\ & + q^{o(1)} \left(q^{1/16} P^{3/4} R^{3/16} + q^{3/8+o(1)} \frac{P^{3/4}}{R^{1/2}} \right). \end{aligned}$$

Taking parameters

$$H = P^{1/5}, \quad L = P^{1/4}, \quad R = q^{5/11},$$

gives

$$\widetilde{S}_q(h,P) \leqslant q^{o(1)} (P^{15/16} + q^{1/8} P^{3/4} + q^{1/16} P^{69/80} + q^{13/88} P^{3/4}),$$

which completes the proof.

Acknowledgement. We would like to thank Christian Bagshaw for pointing out a gap in the initial proof of Equation (3.14) and his help with fixing it and Alexander Dunn for some useful discussions and in particular for pointing out the paper of Duke [10] regarding multidimensional Salié sums. We are also very grateful to the referee for the very careful reading of the manuscript and very helpful comments.

During the preparation of this work, B.K. was supported by the Academy of Finland Grant 319180 and by the Max Planck Institute for Mathematics, I.D.S. by the Ministry of Science and Higher Education of the Russian Federation (agreement no. 075-02-2023-934), and I.E.S. by the Australian Research Council Grants DP170100786 and DP200100355.

Competing interests. The authors have no competing interest to declare.

References

[1] E. Arzhakova, D. Lind, K. Schmidt and E. Verbitskiy, 'Decimation limits of principal algebraic $\mathbb{Z}^d$-actions', Preprint, 2021, arxiv.org/abs/2104.04408.

[2] A. Ayyad, T. Cochrane and Z. Zheng, 'The congruence $x_1x_2 \equiv x_3x_4 (mod p)$, the equation $x_1x_2 = x_3x_4$ and mean values of character sums', *J. Number Theory* **59** (1996), 398–413.

[3] A. S. Besicovitch, 'On the linear independence of fractional powers of integers', *J. London Math. Soc.* **15** (1940), 3–6.

[4] U. Betke, M. Henk and J. M. Wills, 'Successive-minima-type inequalities', *Discr. Comput. Geom.* **9** (1993), 165–175.

[5] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums* (John Wiley, New York, 1998).

[6] M. Bordignon and B. Kerr, 'An explicit Pólya–Vinogradov inequality via partial Gaussian sums', *Trans. Amer. Math. Soc.* **373** (2020), 6503–6527.

[7] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'On congruences with products of variables from short intervals and applications', *Proc. Steklov Math. Inst.* **280** (2013), 67–96.

[8] J. W. S. Cassels, *An Introduction to the Geometry of Numbers* (Springer, Berlin, 1971).

[9] R. Carr and C. O'Sullivan, 'On the linear independence of roots', *Int. J. Number Theory* **5** (2009), 161–171.

[10] W. Duke, 'On multiple Salié sums', *Proc. Amer. Math. Soc.* **114** (1992), 623–625.

[11] W. Duke, J. Friedlander and H. Iwaniec, 'Equidistribution of roots of a quadratic congruence to prime moduli', *Ann. of Math.* **141** (1995), 423–441.

[12] W. Duke, J. Friedlander and H. Iwaniec, 'Weyl sums for quadratic roots', *Int. Math. Res. Not.* 2012 (**2012**), 2493–2549.

[13] A. Dunn, B. Kerr, I. E. Shparlinski and A. Zaharescu, 'Bilinear forms in Weyl sums for modular square roots and applications', *Adv. Math.* **375** (2020), Art.107369.

[14] A. Dunn and A. Zaharescu, 'The twisted second moment of modular half integral weight L-functions', Preprint, 2019, arxiv.org/abs/1903.03416.

[15] J. B. Friedlander and H. Iwaniec, 'Incomplete Kloosterman sums and a divisor problem', *Ann. Math.* **121**(2) (1985), 319–344.

[16] W. T. Gowers, 'A new proof of Szemerédi's theorem for arithmetic progressions of length four', *Geom. Funct. Anal.* **8** (1998), 529–551.

[17] W. T. Gowers, 'A new proof of Szemerédi's theorem', *Geom. Funct. Anal.* **11** (2001), 465–588.

[18] W. T. Gowers, 'A uniform set with fewer than expected arithmetic progressions of length 4', *Acta Math. Hungar.* **161** (2020), 756–767.
[19] H. Iwaniec and E. Kowalski, *Analytic Number Theory* (Amer. Math. Soc., Providence, RI, 2004).
[20] B. Kerr and A. Mohammadi, 'Points on polynomial curves in small boxes modulo an integer', *J. Number Theory* **223** (2021), 64–78.
[21] K. Mahler, 'Ein Übertragungsprinzip für konvexe Körper', *Math. Časopis* **68** (1939), 93–102.
[22] J. L. Mordell, 'On the linear independence of algebraic numbers', *Pacific J. Math.* **3** (1953), 625–630.
[23] P. Sarnak, *Some Applications of Modular Forms*, Cambridge Tracts in Math., vol. **99** (Cambridge Univ. Press, Cambridge, 1990).
[24] W. M. Schmidt, *Equations over Finite Fields*, Lecture Notes in Mathematics, vol. **536** (Springer Berlin, Heidelberg, 1976).
[25] I. D. Shkredov, 'Energies and structure of additive sets', *Electronic J. Combin.* **21** (2014), #P3.44, 1–53.
[26] I. D. Shkredov, I. E. Shparlinski and A. Zaharescu, 'Bilinear forms with modular square roots and averages of twisted second moments of half integral weight L-functions', *Intern. Math. Res. Notices* 2022 (**2022**), 17431–17474.
[27] I. D. Shkredov, I. E. Shparlinski and A. Zaharescu, 'On the distribution of modular square roots of primes', Preprint, 2020, arxiv.org/abs/2009.03460.
[28] C. L. Siegel, 'Algebraische Abhängigkeit von Wurzeln', *Acta Arith.* **21** (1972) 59–64.
[29] E. Szemerédi, 'On sets of integers containing no four elements in arithmetic progression', *Acta Math. Acad. Sci. Hungar.* **20** (1969), 89–104.
[30] T. Tao and V. Vu, *Additive Combinatorics, Cambridge*, Stud. Adv. Math., vol. **105** (Cambridge Univ. Press, Cambridge, 2006).