

# *Algebra & Number Theory*

Volume 19  
2025  
No. 8

**Weyl sums with multiplicative coefficients  
and joint equidistribution**

Matteo Bordignon, Cynthia Bortolotto and Bryce Kerr

# Weyl sums with multiplicative coefficients and joint equidistribution

Matteo Bordignon, Cynthia Bortolotto and Bryce Kerr

We generalise a result of Montgomery and Vaughan regarding exponential sums with multiplicative coefficients to the setting of Weyl sums. As applications, we establish a joint equidistribution result for roots of polynomial congruences and polynomial values which generalises a result of Hooley. We also obtain some new results for mixed character sums.

1. Introduction	1549
2. Main results	1551
3. Applications	1552
4. Preliminary results	1554
5. Sums over bilinear forms	1558
6. Proof of Theorem 1	1564
7. Proof of Corollary 3	1566
8. Short mixed character sums	1567
9. On the correlation between roots of polynomial congruences and polynomial values	1568
10. Sharpness of Theorem 1	1578
Acknowledgements	1579
References	1579

## 1. Introduction

Let  $A \geq 1$ , and let  $f$  be a multiplicative function satisfying  $|f(p)| \leq A$  for any prime  $p$  and also  $\sum_{n \leq N} |f(n)|^2 \leq A^2 N$  for all natural numbers  $N$ . For  $\alpha \in \mathbb{R}$ , set

$$S(\alpha) := \sum_{1 \leq n \leq N} f(n)e(\alpha n),$$

where  $e(x) = \exp(2\pi i x)$ .

These sums appear to be considered first by Daboussi [1975], who showed that if  $|\alpha - a/q| \leq 1/q^2$ ,  $(a, q) = 1$  and  $3 \leq q \leq (N/\log N)^{1/2}$ , then

$$S(\alpha) \ll \frac{N}{(\log \log q)^{1/2}},$$

with the implied constant depending only on  $A$ .

MSC2020: 11N60, 11N75.

Keywords: Weyl sums, multiplicative functions.

This result was improved by Montgomery and Vaughan [1977, Corollary 1] who show that, assuming  $|\alpha - a/q| \leq 1/q^2$ ,  $(a, q) = 1$  and  $2 \leq R \leq q \leq N/R$ , we have

$$S(\alpha) \ll \frac{N}{\log N} + \frac{N(\log R)^{3/2}}{R^{1/2}}. \quad (1)$$

We refer the reader to [Montgomery and Vaughan 1977, Section 7] for a demonstration that the term  $N/\log N$  is sharp.

The optimal dependence on  $R$  in (1) is an open problem and has been the subject of several works (see for example [Bachman 2003; de la Bretèche 1998]), and it is expected the estimate (1) may be improved to

$$S(\alpha) \ll \frac{N}{\log N} + \frac{N}{R^{1/2}}. \quad (2)$$

Recently, de la Bretèche and Granville [2022] have studied in detail the sums  $S(\alpha)$  on major arcs. Their estimates suggest the following conjecture (see [de la Bretèche and Granville 2022, Equation 1.4]):

$$S(\alpha) \ll \frac{N}{\log N} + \frac{N}{q^{1/2}(1 + |\beta|x)}, \quad \alpha = \frac{a}{q} + \beta, \quad (a, q) = 1.$$

We also note that [de la Bretèche and Granville 2022] contains some nice applications to circle method-type problems.

The estimate (1) has important applications to Dirichlet  $L$ -functions. Montgomery and Vaughan [1977] have shown how it may be combined with the generalised Riemann hypothesis (GRH) to obtain a sharp upper bound for Dirichlet  $L$ -functions at the point  $s = 1$ . One may also combine (1) with estimates for short character sums to obtain unconditional variants of Montgomery and Vaughan's result. We refer the reader to [Granville and Soundararajan 2007; Hildebrand 1988b; 1988a] for progress in this direction.

Since the work of Montgomery and Vaughan, exponential sums with multiplicative coefficients have appeared in a number of different contexts, and a variety of techniques have been developed to facilitate the reduction to bilinear forms. Some examples include work of Karatsuba [2010] on short Kloosterman sums, which has been refined by Korolëv; see for example [Korolëv 2018]. Kátai [1986] and Indlekofer and Kátai [1989] have considered more general functions in the exponential factor. Bourgain, Sarnak and Ziegler [Bourgain et al. 2013] have established a finite version of Vinogradov's bilinear sum inequality. Gong and Jia [2015] have considered shifted character sums with multiplicative coefficients and Korolëv and Shparlinski [2020] dealt with sums over trace functions with multiplicative coefficients.

In this paper, we revisit the approach of Montgomery and Vaughan and generalise it to the setting of sums of the form

$$\sum_{n \leq N} f(n)e(F(n)), \quad (3)$$

where  $F$  is a polynomial with real coefficients and  $f$  is a multiplicative function satisfying

$$f(p) = O(1), \quad \sum_{n \leq N} |f(n)| = O(N), \quad \sum_{n \leq N} |f(n)|^2 = O(N(\log N)^A)$$

for any  $A \geq 0$ .

Problems of this sort have previously been considered by Jiang, Lü and Wang [Jiang et al. 2021], who showed that one may replace an assumption on the  $\ell_2$  norm,

$$\sum_{n \leq N} |f(n)|^2 \ll N,$$

with an assumption of the form

$$\sum_{\substack{p \leq N \\ p \text{ prime}}} |f(p)| |f(p+h)| \ll \frac{h}{\phi(h)} \frac{N}{(\log N)^2}.$$

Such a relaxation is significant in the context of  $\mathrm{GL}_m$   $L$ -functions in the absence of progress towards the Ramanujan conjectures.

Matthiesen [2018] considered sums of the form (3) over polynomial nilsequences with slightly weaker conditions on  $f$  than Montgomery and Vaughan. These results were later applied to linear correlations of multiplicative functions [Matthiesen 2020]. We also mention [Matomäki et al. 2023], which considers exponential sums with multiplicative functions over nilsequences on average over short intervals.

## 2. Main results

**Theorem 1.** *Let  $A > 0$  and  $c > 0$  be real numbers and  $f$  be a multiplicative function satisfying*

$$|f(p)| \leq C \quad \text{for each prime } p, \quad (4)$$

$$\sum_{n \leq N} |f(n)| = O(N), \quad (5)$$

$$\sum_{n \leq N} |f(n)|^2 = O(N(\log N)^A). \quad (6)$$

*Let  $F$  be a polynomial of degree  $d \geq 1$  with real coefficients given by*

$$F(x) = \alpha_d x^d + \cdots + \alpha_1 x.$$

*Let  $R \geq 1$ , and suppose there exist integers  $\ell$ ,  $a$  and  $q$ , with  $1 \leq q \leq R$ ,  $1 \leq \ell \leq d$ ,  $(a, q) = 1$  and*

$$\left| \alpha_\ell - \frac{a}{q} \right| \leq \frac{1}{Rq}.$$

*Write  $C = A/(2r)$ . Then, for any  $r > d(d+1)$ , we have*

$$\sum_{1 \leq n \leq N} f(n) e(F(n)) \ll N \left( \frac{1}{(\log N)^{1-C}} + (\log N)^C \left( \frac{q}{N^\ell} + \frac{1}{q} \right)^{1/(4r^2)} \right) + (NR^{1/\ell})^{1/2},$$

*where the implied constant depends on  $A$  and  $r$ . In particular, if we suppose that*

$$(\log N)^{4r^2} \leq q \leq \frac{N^\ell}{(\log N)^{4r^2}},$$

*then*

$$\sum_{1 \leq n \leq N} f(n) e(F(n)) \ll \frac{N}{(\log N)^{1-C}}. \quad (7)$$

To demonstrate the precision of the above estimate, in [Section 10](#) we prove that, for any polynomial  $F$  and integer  $N$ , there exists  $f = f_{F,N}$  such that

$$\left| \sum_{1 \leq n \leq N} f(n) e(F(n)) \right| \geq \frac{1}{10} \frac{N}{\log N}.$$

The proof of [Theorem 1](#) follows the outline of [[Montgomery and Vaughan 1977](#)] and starts with a combinatorial decomposition of multiplicative functions based on Möbius inversion. This reduces the problem to estimating bilinear forms over polynomials with summation restricted to points under the hyperbola. We then use Montgomery and Vaughan's partition of the parabola into disjoint rectangles to which techniques related to the Vinogradov mean value theorem may be applied. It will be fundamental to develop a version of the Vinogradov mean value theorem for primes in large translated intervals; this is [Lemma 10](#). We should note that we introduced the general condition [\(6\)](#) with the aim of using [Theorem 1](#) in the proof of [Theorem 2](#).

### 3. Applications

**3.1. Joint equidistribution.** As an application of [Theorem 1](#), we prove a joint equidistribution result. Throughout this section, we let  $p \in \mathbb{Z}[x]$  be irreducible over  $\mathbb{Q}$  of degree  $e \geq 2$ , and we consider the ratios  $v/n$ , where the  $v$  are the roots of the polynomial  $p$  modulo  $n$ :

$$p(v) \equiv 0 \pmod{n}.$$

Consider the sequence  $(g_k)_{k \geq 1}$  of these ratios, defined in such a way that the corresponding denominators are in ascending order. Hooley [[1964](#), Theorem 2] proved that this sequence is equidistributed in  $\mathbb{R}/\mathbb{Z}$ .

We now let

$$F(x) = \alpha_1 x + \cdots + \alpha_d x^d \in \mathbb{R}[x] \quad \text{with } d \geq 1$$

have an irrational coefficient and define

$$A(F, p)_k = (g_k, F(n))_{k \geq 1},$$

where  $g_k$  is as above and  $n$  is taken so that

$$g_k = v/n, \quad p(v) \equiv 0 \pmod{n}.$$

We prove the following result.

**Theorem 2.** *The sequence  $A(F, p)_k$  is equidistributed in  $(\mathbb{R}/\mathbb{Z})^2$ .*

This indicates that the sequence  $(F(n))_{n \geq 1}$  is somehow not correlated with the sequence  $(g_n)_{n \geq 1}$ .

**3.2. Mixed character sums.** We next explain how [Theorem 1](#) is related to sums considered in [[Enflo 1995](#); [Chang 2010](#); [Heath-Brown and Pierce 2015](#)]. [Theorem 1](#) implies large exponential sums must correspond to pretentious multiplicative functions.

**Corollary 3.** *With the notation and conditions as in [Theorem 1](#), suppose further that  $f$  is completely multiplicative. Let  $r \geq d(d+1)$ , and suppose that*

$$\left| \sum_{1 \leq n \leq N} f(n)e(F(n)) \right| \gg \frac{N}{(\log N)^{1-A/(2r)}}.$$

*There exists an integer*

$$\ell \leq (\log N)^{d(4r^2+4rA)}$$

*and a multiplicative character  $\psi \pmod{\ell}$  such that*

$$\sum_{1 \leq n \leq N} f(n)e(F(n)) \ll (\log N)^{4r^2+4rA} \max_{u \leq N} \left| \sum_{n \leq u} \psi(n)f(n) \right|.$$

[Corollary 3](#) implies one may bound character sums mixed by polynomials by reducing to pure character sums; we refer the reader to [Section 8](#) for more precise results. It is worth mentioning that, by combining [Corollary 3](#) with Halász's theorem, it's possible to show that sums satisfying the conditions of [Corollary 3](#) must be pretentious in the sense of [\[Granville and Soundararajan 2007\]](#).

**Corollary 4.** *Let  $F(n)$  be a polynomial of degree  $d$  with real coefficients and  $\chi$  a primitive character modulo  $q$ . Suppose that  $\delta$  and  $\varepsilon$  satisfy*

$$\max_{\substack{\ell \ll (\log q)^{100d^3} \\ \psi \pmod{\ell} \\ u \leq N}} \left| \sum_{n \leq u} \psi(n)\chi(n) \right| \leq Nq^{-\varepsilon} \quad \text{provided } N \geq q^\delta.$$

*Then we have*

$$\sum_{n \leq N} \chi(n)e(F(n)) \ll \frac{N}{(\log N)^{1-1/(d(d+1))}} \quad \text{provided } N \geq q^\delta. \quad (8)$$

In particular, estimate (8) holds under the following conditions:

- for arbitrarily small  $\delta$  assuming the generalised Riemann hypothesis,
- for  $\delta = \frac{1}{3}$  and an arbitrary integer  $q$ , which follows from the Burgess bound; see for example [\[Iwaniec and Kowalski 2004\]](#).

Let  $\varepsilon > 0$  be small. Enflo [\[1995\]](#) has previously established that, if  $q$  is prime,

$$\sum_{n \leq N} \chi(n)e(F(n)) \ll N^{1-\delta}, \quad \text{provided } N \geq q^{1/4+\varepsilon},$$

and we refer the reader to [\[Chang 2010; Heath-Brown and Pierce 2015\]](#) for quantitative improvements on Enflo's result. Chang [\[2014\]](#) has shown

$$\sum_{n \leq N} \chi(n)e(F(n)) \ll N^{1-\delta}, \quad \text{provided } N \geq q^\varepsilon,$$

provided  $q$  is suitably smooth/powerful.

[Corollary 4](#) provides some new instances where one may bound mixed character sums nontrivially. We refer the reader to [Section 8](#) for more details.

#### 4. Preliminary results

**4.1. Reduction to bilinear forms.** We proceed in a similar fashion to [Montgomery and Vaughan 1977, Section 2], which reduces the proof of Theorem 1 to bounding bilinear forms under the hyperbola.

**Lemma 5.** *Let  $f$  be a multiplicative function satisfying the conditions of Theorem 1,  $F$  be any real-valued function and  $\epsilon > 0$ . Then, for any integer  $N$ , we have*

$$\left| \sum_{1 \leq n \leq N} f(n)e(F(n)) \right| \ll \frac{N}{(\log N)^{1-\epsilon}} + \frac{1}{\log N} \left| \sum_{1 \leq np \leq N} f(n)f(p)(\log p)e(F(np)) \right|. \quad (9)$$

*Proof.* We follow the argument from [Montgomery and Vaughan 1977, Section 2] with some modifications to deal with the condition

$$\sum_{n \leq N} |f(n)|^2 \ll N(\log N)^A.$$

Consider

$$S = \sum_{n \leq N} f(n)e(F(n)) \log(N/n).$$

Since

$$S = \log N \sum_{n \leq N} f(n)e(F(n)) - \sum_{n \leq N} f(n)(\log n)e(F(n)),$$

it is sufficient to show

$$S \ll N(\log N)^\epsilon \quad (10)$$

and

$$\sum_{n \leq N} f(n)(\log n)e(F(n)) \ll \left| \sum_{1 \leq np \leq N} f(n)f(p)(\log p)e(F(np)) \right| + N(\log N)^\epsilon. \quad (11)$$

Let  $r$  be a large real number, and apply Hölder's inequality, (5) and (6) to get

$$|S|^{2r} \ll \left( \sum_{n \leq N} (\log(N/n))^{2r} \right) \left( \sum_{n \leq N} |f(n)|^2 \right) \left( \sum_{n \leq N} |f(n)| \right)^{2r-2} \ll \left( \sum_{n \leq N} (\log(N/n))^{2r} \right) N^{2r-1} (\log N)^A.$$

Since

$$\sum_{n \leq N} (\log(N/n))^{2r} \ll \sum_{\substack{j \\ 1 \leq 2^j \leq N}} j^{2r} \sum_{N/2^{j+1} \leq n \leq N/2^{j-1}} 1 \ll N \sum_{j \geq 1} \frac{j^{2r}}{2^j} \ll N,$$

we obtain (10) after taking  $r$  sufficiently large. Since

$$\log n = \sum_{d|n} \Lambda(d),$$

we have

$$\begin{aligned} \sum_{n \leq N} f(n)(\log n)e(F(n)) &= \sum_{nm \leq N} \Lambda(m) f(nm)e(F(nm)) \\ &= \sum_{mn \leq N} \Lambda(m) f(n)f(m)e(F(nm)) + O\left( \sum_{mn \leq N} \Lambda(m) |f(nm) - f(n)f(m)| \right). \end{aligned}$$



Using (4) and (5),

$$\begin{aligned}\sum_{mn \leq N} \Lambda(m) f(n) f(m) e(F(nm)) &= \sum_{pn \leq N} (\log p) f(p) f(n) e(F(np)) + O\left(N \sum_{k \geq 2} \sum_{p^k \leq N} \frac{|f(p^k)|}{p^k}\right) \\ &= \sum_{pn \leq N} (\log p) f(p) f(n) e(F(np)) + O(N),\end{aligned}$$

where we have used the Cauchy–Schwarz inequality and (6) to estimate

$$\sum_{k \geq 2} \sum_{p^k \leq N} \frac{|f(p^k)|}{p^k} \ll \left( \sum_{k \geq 2} \sum_p \frac{1}{p^{0.8k}} \right) \left( \sum_n \frac{|f(n)|^2}{n^{1.2}} \right) = O(1).$$

Hence it remains to show

$$\sum_{mn \leq N} \Lambda(m) |f(nm) - f(n)f(m)| = O(N(\log N)^\epsilon). \quad (12)$$

From (5),

$$\begin{aligned}\sum_{mn \leq N} \Lambda(m) |f(nm) - f(n)f(m)| &\ll \sum_{k \geq 1} \sum_{p^k \leq N} \sum_{\substack{n \leq N/p^k \\ p|n}} |f(p^k)| |f(n)| + |f(p^k n)| \\ &\ll \sum_{k, j \geq 1} \sum_{p^{k+j} \leq N} \sum_{\substack{n \leq N/p^{k+j} \\ (n, p)=1}} (|f(p^{k+j})| + |f(p^k)| |f(p^j)|) |f(n)| \\ &\ll N \sum_{k, j \geq 1} \sum_p \frac{|f(p^k)| |f(p^j)| + |f(p^{k+j})|}{p^{k+j}},\end{aligned}$$

and after applying the Cauchy–Schwarz inequality, (6) and partial summation over  $p$ ,  $k$  and  $j$  as above, we establish (12) and complete the proof.  $\square$

We require a generalisation of [Montgomery and Vaughan 1977, Section 3] for multiplicative functions  $f$  satisfying (6).

**Lemma 6.** *Let the notation and conditions be as in Theorem 1. Suppose  $s$  is a parameter and, for each  $0 \leq i \leq \log_2 N$ , write*

$$J_i = \min(i + 1, \lfloor \log_2 N \rfloor - i + 1, \lfloor \log_2 \frac{1}{2}(64N/s) \rfloor). \quad (13)$$

We partition the hyperbola into rectangles

$$\mathcal{R}_i = (0, 2^i] \times \left( \frac{N}{2^{i+1}}, \frac{N}{2^i} \right], \quad 0 \leq i \leq \log_2 N, \quad (14)$$

and

$$\mathcal{R}_{i,j,k} = \left( \frac{2^{i+j}}{k}, \frac{2^{i+j+1}}{2k-1} \right] \times \left( \frac{(k-1)N}{2^{i+j}}, \frac{(2k-1)N}{2^{i+j+1}} \right], \quad 0 \leq i \leq \log_2 N, \quad 1 \leq j \leq J_i, \quad 2^{j-1} \leq k \leq 2^j. \quad (15)$$

Then each  $\mathcal{R}_{i,j,k}$  is a rectangle of the form  $(P, P'] \times (N, N']$ , with  $P, P', N, N'$  satisfying

$$P' - P \geq \frac{1}{4}, \quad N' - N \geq \frac{1}{4}, \quad (P' - P)(N' - N) \gg s.$$



Let  $\mathcal{E}$  denote the set of points  $(p, n)$  satisfying  $1 \leq pn \leq N$  with  $p$  prime which do not lie in any of the rectangles (14) or (15). Then, for any fixed  $\epsilon > 0$ , we have

$$\sum_{(p,n) \in \mathcal{E}} f(p)(\log p)f(n)e(F(np)) \ll (\log N)^\epsilon (N + (Ns)^{1/2} \log(2N/s) \log s).$$

*Proof.* Our proof is similar to that of [Montgomery and Vaughan 1977, Section 3] with some minor modifications. Recall that  $\mathcal{E}$  denotes the set of points  $(p, n)$  satisfying  $1 \leq pn \leq N$  with  $p$  prime which do not lie in any of the rectangles (14) or (15). We write the partition

$$\mathcal{E} = \mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3,$$

where

$$\begin{aligned} \mathcal{E}_1 &= \left\{ (p, n) \in \mathcal{E} : pn \leq N, \frac{N}{2^{i+1}} < n \leq \frac{N}{2^i}, J_i > i + 1 \right\}, \\ \mathcal{E}_2 &= \left\{ (p, n) \in \mathcal{E} : pn \leq N, \frac{N}{2^{i+1}} < n \leq \frac{N}{2^i}, J_i = \lfloor \log_2 N \rfloor - i + 1 \right\}, \\ \mathcal{E}_3 &= \left\{ (p, n) \in \mathcal{E} : pn \leq N, \frac{N}{2^{i+1}} < n \leq \frac{N}{2^i}, J_i = \left\lfloor \frac{1}{2} \log_2(64N/s) \right\rfloor \right\}, \end{aligned}$$

which allows us to bound

$$\begin{aligned} \sum_{(p,n) \in \mathcal{E}} f(p)(\log p)f(n)e(F(np)) \\ \ll \sum_{(p,n) \in \mathcal{E}_1} |f(p)||f(n)| \log p + \sum_{(p,n) \in \mathcal{E}_2} |f(p)||f(n)| \log p + \sum_{(p,n) \in \mathcal{E}_3} |f(p)||f(n)| \log p. \end{aligned}$$

Consider first summation over  $\mathcal{E}_1$ . We apply Hölder's inequality twice; first with the exponents  $(2r, 2r/(2r-1))$  and second with the exponents  $(2r-1, (2r-2)/(2r-1))$ . Together with (4), this gives

$$\left( \sum_{(p,n) \in \mathcal{E}_1} |f(p)||f(n)| \log p \right)^{2r} \ll \left( \sum_{(p,n) \in \mathcal{E}_1} |f(n)| \right)^{2r-2} \left( \sum_{(p,n) \in \mathcal{E}_1} |f(n)|^2 \right) \left( \sum_{(p,n) \in \mathcal{E}_1} (\log p)^{2r} \right).$$

For each prime  $p$ ,

$$\#\{n : (p, n) \in \mathcal{E}_1\} \ll \frac{N}{p^2},$$

so that

$$\sum_{(p,n) \in \mathcal{E}_1} (\log p)^{2r} \ll N \sum_p \frac{(\log p)^{2r}}{p^2} \ll N.$$

For each  $n \in \mathbb{N}$ ,

$$\#\{p : (p, n) \in \mathcal{E}_1\} \ll 1,$$

and hence, by (5) and (6),

$$\sum_{(p,n) \in \mathcal{E}_1} |f(n)| \ll \sum_{n \leq N} |f(n)| \ll N, \quad \sum_{(p,n) \in \mathcal{E}_1} |f(n)|^2 \ll \sum_{n \leq N} |f(n)|^2 \ll N(\log N)^A.$$

Taking  $r$  sufficiently large, the above estimates combine to give

$$\sum_{(p,n) \in \mathcal{E}_1} |f(p)| |f(n)| \log p \ll N (\log N)^\epsilon.$$

Consider next  $\mathcal{E}_2$ . By the Cauchy–Schwarz inequality,

$$\left( \sum_{(p,n) \in \mathcal{E}_2} |f(p)| |f(n)| \log p \right)^2 \ll \sum_{(p,n) \in \mathcal{E}_2} |f(n)|^2 \sum_{(p,n) \in \mathcal{E}_2} (\log p)^2.$$

If  $(p, n) \in \mathcal{E}_2$  then  $n \ll N^{1/2}$  and, for fixed  $n$ , there exists some  $H$  such that

$$\{p : (p, n) \in \mathcal{E}_2\} \subseteq [H, H + N/n^2].$$

Hence, by Hölder's inequality and the Brun–Titchmarsh theorem, we get

$$\sum_{(p,n) \in \mathcal{E}_2} |f(p)| |f(n)| \log p \ll \left( N \sum_{n \leq N^{1/2}} \frac{|f(n)|^2}{n^2 \log(4N/n^2)} \right)^{1/2} \left( \sum_{(p,n) \in \mathcal{E}_2} (\log p)^2 \right)^{1/2}.$$

Note by (6) and partial summation,

$$\sum_{n \leq N^{1/2}} \frac{|f(n)|^2}{n^2 \log(4N/n^2)} \ll \int_1^{N^{1/2}} \left( \sum_{n \leq t} |f(n)|^2 \right) \frac{1}{t^3 (\log(4N/t))^2} dt \ll \int_1^{N^{1/2}} \frac{(\log t + 2)^A}{t^2 (\log(4N/t))} dt \ll \frac{1}{(\log N)}.$$

For each  $p$ ,

$$\#\{n : (p, n) \in \mathcal{E}_2\} \ll 1,$$

so that

$$\sum_{(p,n) \in \mathcal{E}_2} (\log p)^2 \ll \sum_{p \leq N} (\log p)^2 \ll N \log N.$$

The above estimates combine to give

$$\sum_{(p,n) \in \mathcal{E}_2} |f(p)| |f(n)| \log p \ll N.$$

Finally consider  $\mathcal{E}_3$ . By Hölder's inequality,

$$\left( \sum_{(p,n) \in \mathcal{E}_3} |f(p)| |f(n)| \log p \right)^{2r} \ll \left( \sum_{(N/q)^{1/2} \leq n \leq (Nq)^{1/2}} |f(n)|^{2r/(2r+1)} \log p \right)^{2r-1} \left( \sum_{(N/q)^{1/2} \leq p \leq (Nq)^{1/2}} \frac{\log p}{p} \right).$$

If  $(p, n) \in \mathcal{E}_3$ , then

$$\left( \frac{N}{s} \right)^{1/2} \leq p \leq (Ns)^{1/2},$$

and, for each  $p$ , there exists some  $H$  such that

$$\{n : (p, n) \in \mathcal{E}_3\} \subseteq [H, H + O((Ns)^{1/2}/p)]$$

and, for each  $n$ , there exists some  $H$  such that

$$\{p : (p, n) \in \mathcal{E}_3\} \subseteq [H, H + O((Ns)^{1/2}/n)].$$

Using the Brun–Titchmarsh inequality, we see that

$$\left( \sum_{(p,n) \in \mathcal{E}_3} |f(p)| |f(n)| \log p \right)^{2r} \ll (Ns)^{1/2} \left( \sum_{(N/s)^{1/2} \leq n \leq (Ns)^{1/2}} |f(n)|^{2r/(2r+1)} \frac{\log(2N/n)}{n \log(2Ns/n^2)} \right)^{2r-1} \left( \sum_{(N/s)^{1/2} \leq p \leq (Ns)^{1/2}} \frac{\log p}{p} \right).$$

We have

$$\sum_{(N/s)^{1/2} \leq p \leq (Ns)^{1/2}} \frac{\log p}{p} \ll \log s,$$

and Hölder's inequality combined with (5) and (6) gives

$$\begin{aligned} & \left( \sum_{(N/s)^{1/2} \leq n \leq (Ns)^{1/2}} |f(n)|^{2r/(2r+1)} \frac{\log(2N/n)}{n \log(2Ns/n^2)} \right)^{2r-1} \\ & \ll (\log(2N/s))^{2r-1} \left( \sum_{(N/s)^{1/2} \leq n \leq (Ns)^{1/2}} \frac{|f(n)|}{n} \right)^{2r-2} \left( \sum_{(N/s)^{1/2} \leq n \leq (Ns)^{1/2}} \frac{|f(n)|^2}{n} \right) \\ & \ll (\log(2N/s))^{2r-1} (\log N)^A (\log s)^{2r-1}, \end{aligned}$$

which, after taking  $r$  sufficiently large, results in

$$\sum_{(p,n) \in \mathcal{E}_3} |f(p)| |f(n)| \log p \ll (Ns)^{1/2} (\log N)^\varepsilon (\log s) \log(2N/s). \quad \square$$

## 5. Sums over bilinear forms

**5.1. The Vinogradov mean value theorem.** Given integers  $r$ ,  $d$  and  $V$ , we let  $J_{r,d}(V)$  count the number of solutions to the system of equations

$$v_1^j + \cdots + v_r^j - v_{r+1}^j - \cdots - v_{2r}^j = 0, \quad 1 \leq j \leq d,$$

with variables satisfying

$$1 \leq v_1, \dots, v_{2r} \leq V.$$

We will use a consequence of Bourgain, Demeter and Guth's work on the Vinogradov mean value theorem; see [Bourgain et al. 2016, Section 5].

**Lemma 7.** Assume  $d \geq 2$  and  $r > d(d+1)$ . Then we have

$$J_{r,d}(V) \ll V^{2r-d(d+1)/2}.$$

Combining Lemma 7 with the fact that the Vinogradov system is translation invariant, we obtain the following.

**Corollary 8.** Let  $d \geq 2$ ,  $r > d(d+1)$  be integers and  $\mathcal{M}(k)$ ,  $1 \leq k \leq K$ , be disjoint intervals satisfying

$$\mathcal{M}(k) = (M'(k), M''(k)], \quad M''(k) - M'(k) \leq Y.$$

Then the number of solutions to the system of equations

$$n_1^j + \cdots - n_{2r}^j = 0, \quad n_i \in \mathcal{M}(k), \quad 1 \leq k \leq K, \quad (16)$$

is bounded by

$$O(KY^{2r-d(d+1)/2}).$$

We will also require an estimate for the number of solutions to the Vinogradov system with prime variables in translated intervals; here it will be fundamental that the intervals will not be too short. To obtain such a result we need the following intermediary lemma that follows directly from [Hua 1965, Theorem 10]. Here it appears clear why it is important that the intervals we work with are quite large compared to their starting point. For convenience we set  $L = \log P$ .

**Lemma 9.** Let  $0 < Q \leq c_1(k)L^{\sigma_1}$ ,  $X \gg 1$  and

$$S(X, P) = \sum_{\substack{X < p \leq X+P \\ p \equiv t \pmod{Q}}} e(f(p)),$$

in which

$$P \gg \frac{X}{(\log X)^M}$$

for any  $M \gg 1$  and

$$f(x) = \frac{h}{q}x^k + \alpha_1 x^{k-1} + \cdots + \alpha_k, \quad (h, q) = 1,$$

the numbers  $\alpha_1, \dots, \alpha_{d-1}$  being real. Suppose that  $L^\sigma < q \leq P^k L^{-\sigma}$ . For arbitrary  $\sigma_0 > 0$ , when  $\sigma \leq 2^{6k}(\sigma_0 + \sigma_1 + 1)$ , we always have

$$|S(X, P)| \leq c_2(k) \frac{P}{QL^{\sigma_0-M}}.$$

This lemma allows us to prove the following estimate for the number of solutions to the Vinogradov system with prime variables in large translated intervals.

**Lemma 10.** Let  $d \geq 2$  be an integer and  $X, Y \gg 1$ . If  $r > d(d+1)$ , the number of solutions to the equation

$$p_1^j + \cdots - p_{2r}^j = 0, \quad 1 \leq j \leq d, \quad Y \leq p_i \leq Y + X, \quad X \gg \frac{Y}{(\log Y)^C}, \quad p_i \text{ prime},$$

for any  $C \gg 1$  is bounded by

$$O\left(\frac{X^{2r-d(d+1)/2}}{(\log X)^{2r}}\right),$$

with the implied constant depending on  $r$  and  $C$ .

*Proof.* The result follows in a straightforward way from [Hua 1965, Theorem 16] redefining in part (1)

$$S(\alpha_k, \dots, \alpha_1) = \sum_{Y \leq p \leq Y+X} e(f(p)), \quad f(x) = \alpha_d x^d + \dots + \alpha_1 x,$$

and introducing the two following changes which account for the translation in the set of primes and optimising the range of  $r$  in Hua's result: In part (3) of the proof we use our Lemma 9 instead of [Hua 1965, Theorem 10]; this is possible as  $s_1$  in [Hua 1965, Lemma 10.8] is of arbitrary size. While in part (5) of the proof we need to substitute [Hua 1965, Theorem 15] with [Bourgain et al. 2016, Theorem 1] for  $d \geq 4$  and [Wooley 2016] for  $d = 3$ . Doing this we need to be careful to isolate, in [Hua 1965, p. 144],  $|S(\alpha_k, \dots, \alpha_1)|^{d(d+1)-\epsilon}$  instead of  $|S(\alpha_k, \dots, \alpha_1)|^{s_0-1}$  and, in [Hua 1965, p. 145],  $|S(\alpha_k, \dots, \alpha_1)|^{s-\epsilon}$  instead of  $|S(\alpha_k, \dots, \alpha_1)|^{s-1}$ . Here  $\epsilon > 0$  is chosen so that  $s = d(d+1) + 2\epsilon$ .  $\square$

**5.2. Bounding bilinear forms.** It is well known that one may use Lemma 7 to estimate bilinear forms with Weyl sums over rectangles. We next show how one may obtain sharper results by averaging bilinear forms over a family of disjoint rectangles.

**Lemma 11.** *Let  $F \in \mathbb{R}[X]$  be a polynomial of degree  $d \geq 2$  of the form*

$$F(x) = \alpha_d x^d + \dots + \alpha_1 x.$$

*Let  $M$  and  $N$  be integers and  $\alpha(n)$  and  $\beta(m)$  two sequences of complex numbers satisfying*

$$|\beta(m)| \leq 1$$

*and*

$$\sum_{n \leq N} |\alpha(n)| \ll N, \quad \sum_{n \leq N} |\alpha(n)|^2 \ll N(\log N)^A \quad (17)$$

*for  $A \geq 0$ . For  $1 \leq k \leq K$ , let*

$$\mathcal{R}(k) = \mathcal{L}(k) \times \mathcal{M}(k) \quad (18)$$

*be a rectangle of the form*

$$\mathcal{L}(k) = (Q'(k), Q''(k)], \quad \mathcal{M}(k) = (M'(k) \times M''(k)]$$

*such that  $\mathcal{L}(k) \subseteq (0, Q)$ , with  $Q \gg 1$ , are disjoint and satisfy*

$$Q''(k) - Q'(k) \leq X \quad (19)$$

*or*

$$\frac{Q'(k)}{(\log Q'(k))^C} \ll Q''(k) - Q'(k) \ll X, \quad (20)$$

*and  $\mathcal{M}(k) \subseteq (0, M]$  are disjoint and satisfy*

$$M''(k) - M'(k) \leq Y, \quad M''(k) \leq 2M'(k)$$

*and  $K \ll M$ . Let  $I$  denote the sum*

$$I = \sum_{k=1}^K \sum_{(p,n) \in \mathcal{R}(k)} \alpha(n) \beta(p) e(F(np)). \quad (21)$$

Let  $R \geq 1$ , and suppose there exists  $q \leq R$  and  $1 \leq \ell \leq d$  such that

$$\left| \alpha_\ell - \frac{a}{q} \right| \leq \frac{1}{qR} \quad (22)$$

for some  $(a, q) = 1$ . For  $r > d(d+1)$ , we have

$$I^{4r^2} \ll m(X)(\log M)^{2rA} M^{4r^2} \left( \frac{X}{\log X} \right)^{4r^2} \left( \frac{M}{Y} \right)^{d(d-1)/2} \left( \frac{Q}{X} \right)^{d(d-1)/2} \\ \times \left( \frac{q}{XQ^{\ell-1}YM^{\ell-1}} + \frac{1}{XQ^{\ell-1}} + \frac{1}{YM^{\ell-1}} + \frac{1}{q} \right),$$

where

$$m(X) = \begin{cases} (\log X)^{4r} & \text{when (19) holds,} \\ 1 & \text{when (20) holds,} \end{cases}$$

and the implied constant depends on  $C$ .

*Proof.* Recall

$$F(x) = \alpha_d x^d + \cdots + \alpha_1 x,$$

and define

$$S_k = \sum_{(p,n) \in \mathcal{R}(k)} \alpha(n) \beta(p) e(F(np)), \quad (23)$$

so that

$$I = \sum_{k=1}^K S_k. \quad (24)$$

Fix some  $1 \leq k \leq K$  and consider (23). Recalling (18), by Hölder's inequality, for any integer  $r \geq 1$ ,

$$S_k \leq \left( \sum_{n \in \mathcal{M}(k)} |\alpha(n)|^{2r/(2r-1)} \right)^{1-1/(2r)} \left( \sum_{n \in \mathcal{M}(k)} \left| \sum_{p \in \mathcal{L}(k)} \beta(p) e(F(np)) \right|^{2r} \right)^{1/(2r)}.$$

After another application of Hölder's inequality,

$$I^{2r} \leq \left( \sum_{1 \leq k \leq K} \sum_{n \in \mathcal{M}(k)} |\alpha(n)|^{2r/(2r-1)} \right)^{2r-1} \sum_{1 \leq k \leq K} \sum_{n \in \mathcal{M}(k)} \left| \sum_{p \in \mathcal{L}(k)} \beta(p) e(F(np)) \right|^{2r}.$$

Hence, from assumptions on the  $\mathcal{M}(k)$ ,

$$I^{2r} \ll \left( \sum_{n \leq M} |\alpha(n)|^{2r/(2r-1)} \right)^{2r-1} \sum_{1 \leq k \leq K} \sum_{n \in \mathcal{M}(k)} \left| \sum_{p \in \mathcal{L}(k)} \beta(p) e(F(np)) \right|^{2r},$$

which combined with (17) implies that

$$I^{2r} \ll M^{2r-1} (\log M)^A \sum_{1 \leq k \leq K} \sum_{n \in \mathcal{M}(k)} \left| \sum_{p \in \mathcal{L}(k)} \beta(p) e(F(np)) \right|^{2r}.$$

Write  $\lambda = (\lambda_1, \dots, \lambda_d)$ , and let  $J_k(\lambda)$  count the number of solutions to

$$p_1^j + \dots - p_{2r}^j = \lambda_j, \quad 1 \leq j \leq d, \quad p_i \in \mathcal{L}(k), \quad p_i \text{ prime.}$$

Note by assumptions on  $\mathcal{L}(k)$ , if the  $p_1, \dots, p_{2r} \in \mathcal{L}(k)$  satisfy

$$p_1^j + \dots - p_{2r}^j = \lambda_j,$$

then

$$\lambda_j \ll XQ^{j-1}.$$

Expanding the  $2r$ -th power and interchanging summation gives

$$I^{2r} \ll M^{2r-1} (\log M)^A \sum_{1 \leq k \leq K} \sum_{\substack{\lambda \\ \lambda_j \ll XQ^{j-1} \\ 1 \leq j \leq d}} J_k(\lambda) \left| \sum_{n \in \mathcal{M}(k)} e(\alpha_d \lambda_d n^d + \dots + \alpha_1 \lambda_1 n) \right|.$$

After another application of Hölder's inequality, we get

$$\begin{aligned} I^{4r^2} &\ll M^{4r^2-2r} (\log M)^{2rA} \left( \sum_{1 \leq k \leq K} \sum_{\lambda} J_k(\lambda) \right)^{2r-2} \left( \sum_{1 \leq k \leq K} \sum_{\lambda} J_k(\lambda)^2 \right) \\ &\quad \times \sum_{1 \leq k \leq K} \sum_{\substack{\lambda_j \ll XQ^{j-1} \\ 1 \leq j \leq d}} \left| \sum_{n \in \mathcal{M}(k)} e(\alpha_d \lambda_d n^d + \dots + \alpha_1 \lambda_1 n) \right|^{2r}. \end{aligned}$$

We have

$$\sum_{1 \leq k \leq K} \sum_{\lambda} J_k(\lambda) \leq \sum_{1 \leq k \leq K} |\{p_1, \dots, p_{2r} \in \mathcal{L}(k)\}|.$$

Since, for each  $1 \leq k \leq K$ ,  $\mathcal{L}(k)$  is an interval of length at most  $X$ , the Brun–Titchmarsh theorem implies

$$\sum_{1 \leq k \leq K} \sum_{\lambda} J_k(\lambda) \ll \frac{KX^{2r}}{(\log X)^{2r}}.$$

The term

$$\sum_{1 \leq k \leq K} \sum_{\lambda} J_k(\lambda)^2$$

counts the number of solutions to the system of equations

$$p_1^j + \dots - p_{4r}^j = 0, \quad 1 \leq j \leq d, \quad p_i \in \mathcal{L}(k), \quad p_i \text{ prime}, \quad 1 \leq k \leq K. \quad (25)$$

By [Corollary 8](#), ignoring the condition that  $p_i$  is prime if (19) holds and using [Lemma 10](#) when (20) holds, we get

$$\sum_{1 \leq k \leq K} \sum_{\lambda} J_k(\lambda)^2 \ll Km_1(X),$$

where

$$m_1(X) = \begin{cases} X^{4r-d(d+1)/2} & \text{when (19) holds,} \\ \frac{X^{4r-d(d+1)/2}}{(\log X)^{4r}} & \text{when (20) holds} \end{cases}$$



since  $r > d(d+1)$ . Combined with the observations above, this implies

$$I^{4r^2} \ll m(X) M^{4r^2-2r} (\log M)^{2rA} K^{2r-1} \left( \frac{X}{\log X} \right)^{4r^2} \frac{I_0}{X^{d(d+1)/2}}, \quad (26)$$

where

$$I_0 = \sum_{1 \leq k \leq K} \sum_{\substack{\lambda_j \ll X Q^{j-1} \\ 1 \leq j \leq d}} \left| \sum_{n \in \mathcal{M}(k)} e(\alpha_d \lambda_d n^d + \cdots + \alpha_1 \lambda_1 n) \right|^{2r}.$$

Let

$$S(x) = \left( \frac{\sin \pi x}{\pi x} \right)^2,$$

so that

$$\hat{S}(x) = \max\{0, 1 - |x|\} \quad (27)$$

and

$$S(x) \gg 1 \quad \text{if } |x| \leq \frac{1}{4}.$$

There exists a constant  $c_0$  such that

$$I_0 \ll \sum_{1 \leq k \leq K} \sum_{\substack{\lambda_j \ll X Q^{j-1} \\ 1 \leq j \leq d \\ j \neq \ell}} \sum_{\lambda_\ell \in \mathbb{Z}} S\left(\frac{c_0 \lambda_\ell}{X Q^{\ell-1}}\right) \left| \sum_{n \in \mathcal{M}(k)} e(\alpha_d \lambda_d n^d + \cdots + \alpha_1 \lambda_1 n) \right|^{2r}.$$

Expanding the  $2r$ -th power and interchanging summation,

$$I_0 \ll \sum_{\substack{1 \leq k \leq K \\ \mu_j \ll Y N^{j-1}}} L_k(\mu) \prod_{\substack{j=1 \\ j \neq \ell}}^d \left| \sum_{\lambda \ll X Q^{j-1}} e(\alpha_j \lambda \mu_j) \right| \left| \sum_{\lambda \in \mathbb{Z}} S\left(\frac{c_0 \lambda}{X Q^{\ell-1}}\right) e(\alpha_\ell \lambda \mu_\ell) \right|,$$

where  $\mu = (\mu_1, \dots, \mu_d)$  and  $L_k(\mu)$  counts the number of solutions to

$$n_1^j + \cdots - n_{2r}^j = \mu_j, \quad n_i \in \mathcal{M}(k), \quad 1 \leq k \leq K, \quad 1 \leq j \leq d.$$

Using that

$$L_k(\mu) \leq L_k(0)$$

and applying [Corollary 8](#), we obtain

$$I_0 \ll K Y^{2r-d(d+1)/2} \sum_{\substack{\mu \\ \mu_j \ll Y M^{j-1}}} \prod_{\substack{j=1 \\ j \neq \ell}}^d \left| \sum_{\lambda \ll X Q^{j-1}} e(\alpha_j \lambda \mu_j) \right| \left| \sum_{\lambda \in \mathbb{Z}} S\left(\frac{c_0 \lambda}{X Q^{\ell-1}}\right) e(\alpha_\ell \lambda \mu_\ell) \right|.$$

Combining the inequality above with [\(26\)](#), we have

$$I^{4r^2} \ll m(X) (\log M)^{2rA} M^{4r^2} \left( \frac{X}{\log X} \right)^{4r^2} \frac{I_1}{(XY)^{d(d+1)/2}}, \quad (28)$$

where

$$I_1 = \sum_{\mu_j \ll Y M^{j-1}} \prod_{\substack{j=1 \\ j \neq \ell}}^d \left| \sum_{\lambda \ll X Q^{j-1}} e(\alpha_j \lambda \mu_j) \right| \left| \sum_{\lambda \in \mathbb{Z}} S\left(\frac{c_0 \lambda}{X Q^{\ell-1}}\right) e(\alpha_\ell \lambda \mu_\ell) \right|.$$

In  $I_1$ , we bound every term trivially except the one with index  $\ell$  to obtain

$$I_1 \ll \left(\frac{Y}{M}\right)^d \left(\frac{X}{Q}\right)^d (QM)^{d(d+1)/2} \frac{1}{XQ^{\ell-1}} \frac{1}{YM^{\ell-1}} \sum_{\mu \ll YM^{\ell-1}} \left| \sum_{\lambda \in \mathbb{Z}} S\left(\frac{c_0 \lambda}{Xq^{\ell-1}}\right) e(\alpha_\ell \lambda \mu_\ell) \right|. \quad (29)$$

By Poisson summation,

$$\sum_{\lambda \in \mathbb{Z}} S\left(\frac{c_0 \lambda}{XQ^{\ell-1}}\right) e(\alpha_\ell \lambda \mu) = \frac{XQ^{\ell-1}}{c_0} \sum_{\lambda \in \mathbb{Z}} \hat{S}\left(\frac{XQ^{\ell-1}(\lambda - \alpha_\ell \mu)}{c_0}\right),$$

and hence from (27)

$$\begin{aligned} \sum_{\mu \ll YM^{\ell-1}} \left| \sum_{\lambda \in \mathbb{Z}} S\left(\frac{c_0 \lambda}{XQ^{\ell-1}}\right) e(\alpha_\ell \lambda \mu) \right| &\ll XQ^{\ell-1} \sum_{\mu \ll YM^{\ell-1}} \sum_{\lambda \in \mathbb{Z}} \max\left\{0, 1 - \left| \frac{XQ^{\ell-1}(\lambda - \alpha_\ell \mu)}{c_0} \right| \right\} \\ &\ll XQ^{\ell-1} \left| \left\{ \mu \ll YM^{\ell-1} : \|\alpha_\ell \mu\| \leq \frac{100c_0}{XQ^{\ell-1}} \right\} \right|. \end{aligned}$$

There exists some real number  $\beta$  such that

$$\left| \left\{ \mu \ll YM^{\ell-1} : \|\alpha_\ell \mu\| \leq \frac{100c_0}{XQ^{\ell-1}} \right\} \right| \ll \left(1 + \frac{YM^{\ell-1}}{q}\right) \left| \left\{ 0 \leq \mu \leq q : \|\alpha_\ell \mu + \beta\| \leq \frac{100c_0}{XQ^{\ell-1}} \right\} \right|.$$

Recalling (22),

$$\left| \left\{ \mu \ll YM^{\ell-1} : \|\alpha_\ell \mu\| \leq \frac{100c_0}{XQ^{\ell-1}} \right\} \right| \ll \left(1 + \frac{YM^{\ell-1}}{q}\right) \left| \left\{ 0 \leq \mu \leq q : \left\| \frac{a\mu}{q} + \beta \right\| \leq \frac{100c_0}{XQ^{\ell-1}} + \frac{1}{R} \right\} \right|,$$

which implies that

$$\left| \left\{ \mu \ll YM^{\ell-1} : \|\alpha_\ell \mu\| \leq \frac{100c_0}{XQ^{\ell-1}} \right\} \right| \ll \left(1 + \frac{YM^{\ell-1}}{q}\right) \left(1 + \frac{q}{XQ^{\ell-1}}\right),$$

and hence

$$\sum_{\mu \ll YM^{\ell-1}} \left| \sum_{\lambda \in \mathbb{Z}} S\left(\frac{c_0 \lambda}{Xq^{\ell-1}}\right) e(\alpha_\ell \lambda \mu_\ell) \right| \ll XQ^{\ell-1} YM^{\ell-1} \left( \frac{1}{YM^{\ell-1}} + \frac{1}{q} \right) \left(1 + \frac{q}{XQ^{\ell-1}}\right).$$

Combined with (28) and (29), this gives

$$\begin{aligned} I^{4r^2} &\ll m(X)(\log M)^{2rA} M^{4r^2} \left(\frac{X}{\log X}\right)^{4r^2} \left(\frac{M}{Y}\right)^{d(d-1)/2} \left(\frac{Q}{X}\right)^{d(d-1)/2} \\ &\quad \times \left( \frac{q}{XQ^{\ell-1}YM^{\ell-1}} + \frac{1}{XQ^{\ell-1}} + \frac{1}{YM^{\ell-1}} + \frac{1}{q} \right). \quad \square \end{aligned}$$

## 6. Proof of Theorem 1

We apply Lemma 5 and Lemma 6 with

$$s = \frac{q^{1/\ell}}{(\log N)^4}$$

to get

$$\sum_{1 \leq n \leq N} f(n) e(F(n)) \ll \frac{N}{(\log N)^{1-\varepsilon}} + (Nq^{1/\ell})^{1/2} + \sum_{0 \leq i \leq \log_2 N} \frac{i}{\log N} S_i + \sum_{0 \leq i \leq \log_2 N} \frac{i}{\log N} \sum_{1 \leq j \leq J_i} S_{i,j},$$

where

$$S_i = \sum_{(p,n) \in \mathcal{R}_i} \frac{\log p}{i} f(p) f(n) e(F(pn))$$

and

$$S_{i,j} = \sum_{2^{j-1} \leq k \leq 2^j} \sum_{(p,n) \in \mathcal{R}_{i,j,k}} \frac{\log p}{i} f(p) f(n) e(F(pn)).$$

Note if  $(p, n) \in \mathcal{R}_i$  or  $(p, n) \in \mathcal{R}_{i,j,k}$  then

$$\frac{\log p}{i} \ll 1.$$

By [Lemma 11](#), observing that in this case condition (20) holds, we have

$$S_i \ll (\log N)^{A/(2r)} \frac{N}{i} \left( \frac{q}{N^\ell} + \frac{1}{2^{\ell i}} + \frac{2^{\ell i}}{N} + \frac{1}{q} \right)^{1/(4r^2)},$$

which implies that

$$\sum_{0 \leq i \leq \log_2 N} \frac{i}{\log N} S_i \ll \frac{N}{(\log N)^{1-A/(2r)}} \left( 1 + \log N \left( \frac{q}{N^\ell} + \frac{1}{q} \right)^{1/(4r^2)} \right). \quad (30)$$

Consider next the sums  $S_{i,j}$ . We apply [Lemma 11](#) with parameters

$$K = 2^{j-1}, \quad M = \frac{N}{2^i}, \quad Q = 2^{i+1}, \quad X = 2^{i-j+1}, \quad Y = 32N2^{-i-j}.$$

We first focus on the case when  $j \geq \log i^c$  for a fixed  $c \gg 1$ . Here we use [Lemma 11](#) with condition (19), which easily gives

$$S_{i,j} \ll \frac{N}{i^{c_1} 2^{j/8}} \left( \frac{q}{N^\ell} + \frac{1}{2^{\ell i}} + \left( \frac{2^i}{N} \right)^\ell + \frac{1}{q} \right)^{1/(4r^2)}$$

for some  $c_1 \gg 1$ . For fixed  $i \leq \log_2 N$ , recalling that  $J_i$  is given by (13), we have

$$\sum_{\log i^c \leq j \leq J_i} S_{i,j} \ll \frac{N}{i^{c_1}} \left( \frac{q}{N^\ell} + \frac{1}{2^{\ell i}} + \left( \frac{2^i}{N} \right)^\ell + \frac{1}{q} \right)^{1/(4r^2)},$$

and hence

$$\begin{aligned} \sum_{0 \leq i \leq \log_2 N} \frac{i}{\log N} \sum_{\log i^c \leq j \leq J_i} S_{i,j} &\ll \frac{N}{\log N} \sum_{i \leq \log_2 N} \frac{1}{i^{c_1-1}} \left( \frac{q}{N^\ell} + \frac{1}{2^{\ell i}} + \left( \frac{2^i}{N} \right)^\ell + \frac{1}{q} \right)^{1/(4r^2)} \\ &\ll N \left( \frac{1}{\log N} + \frac{q}{N^\ell} + \frac{1}{q} \right). \end{aligned}$$

Write  $C = A/(2r)$ . We then focus on the case when  $j \leq \log i^c$ . Here we use [Lemma 11](#) with condition (20), which easily gives

$$S_{i,j} \ll \frac{1}{(i-j+1)^{1-C}} \frac{N}{2^{j(1-d(d-1)/(4r^2))}} \left( \frac{2^{2j}q}{N^\ell} + \frac{2^j}{2^{\ell i}} + 2^j \left( \frac{2^i}{N} \right)^\ell + \frac{1}{q} \right)^{1/(4r^2)},$$

with the implied constant depending on the fixed real number  $c$ . For  $i \leq \log_2 N$ , we have

$$\sum_{1 \leq j \leq \log i^c} S_{i,j} \ll \frac{N}{i^{1-c}} \left( \frac{q}{N^\ell} + \frac{1}{2^{\ell i}} + \left( \frac{2^i}{N} \right)^\ell + \frac{1}{q} \right)^{1/(4r^2)},$$

and hence

$$\begin{aligned} \sum_{0 \leq i \leq \log_2 N} \frac{i}{\log N} \sum_{1 \leq j \leq \log i^c} S_{i,j} &\ll \frac{N}{\log N} \sum_{i \leq \log_2 N} i^c \left( \frac{q}{N^\ell} + \frac{1}{2^{\ell i}} + \left( \frac{2^i}{N} \right)^\ell + \frac{1}{q} \right)^{1/(4r^2)} \\ &\ll N \left( \frac{1}{(\log N)^{1-c}} + \frac{q(\log N)^c}{N^\ell} + \frac{(\log N)^c}{q} \right). \end{aligned}$$

Combining the above estimates, we complete the proof. □

## 7. Proof of Corollary 3

Suppose

$$F(x) = \alpha_1 x + \cdots + \alpha_d x^d.$$

By Dirichlet's theorem, for each  $1 \leq \ell \leq d$ , there exists integers  $r_\ell$  and  $s_\ell$ , with  $(r_\ell, s_\ell) = 1$  and

$$r_\ell \leq \frac{N^\ell}{(\log N)^{4r^2+4rA}},$$

such that

$$\left| \alpha_\ell - \frac{r_\ell}{s_\ell} \right| \leq \frac{(\log N)^{4r^2+4rA}}{q_\ell N^\ell}.$$

By Theorem 1, we may suppose, for each  $1 \leq \ell \leq d$ ,

$$s_\ell \leq (\log N)^{4r^2+4rA}.$$

By partial summation, we have

$$\left| \sum_{n \leq N} f(n) e(F(n)) \right| \ll (\log N)^{4r^2+4rA} \max_{u \leq N} T(u),$$

with

$$T(u) := \sum_{n \leq u} f(n) e(F_1(n))$$

and

$$F_1(x) := \frac{r_d}{s_d} x^d + \cdots + \frac{r_1}{s_1} x.$$

Defining  $k := \text{lcm}(s_d, \dots, s_1)$ , we have

$$T(u) = \sum_{a \leq k} e(F_1(a)) S(a),$$

with

$$S(a) := \sum_{\substack{n \leq u \\ n \equiv a \pmod k}} f(n).$$

Let  $e = (a, k)$ , and write

$$a' = \frac{a}{e}, \quad k' = \frac{k}{e},$$

so that

$$S(a) = \sum_{\substack{n \leq u \\ n \equiv a \pmod k \\ n \equiv 0 \pmod e}} f(n) = \sum_{\substack{n \leq u/e \\ n \equiv a' \pmod{k'}}} f(en),$$

which after expanding into multiplicative characters gives

$$S(a) = \sum_{\substack{n \leq u \\ n \equiv a \pmod k \\ n \equiv 0 \pmod e}} f(n) = \frac{f(e)}{\phi(k')} \sum_{\psi \pmod{k'}} \bar{\psi}(a') \sum_{n \leq u/e} \psi(n) f(n),$$

where we have used the assumption that  $f$  is completely multiplicative. Hence

$$|S(a)| \leq \frac{1}{\phi(k')} \sum_{\psi \pmod{k'}} \left| \sum_{n \leq u/e} \psi(n) f(n) \right|.$$

Thus, observing that

$$k = \text{lcm}(s_d, \dots, s_1) \leq \prod_{1 \leq i \leq d} s_i \leq (\log N)^{d(4r^2 + 4rA)},$$

we conclude the proof. □

## 8. Short mixed character sums

We next use [Corollary 3](#) to show how one may estimate short mixed character sums assuming GRH.

**Corollary 12.** *Assume the GRH, and let  $\varepsilon > 0$ . Uniformly over all primitive characters  $\chi \pmod q$  and polynomials  $F$  of degree  $d$  with real coefficients, if  $N$  satisfies*

$$\log N \geq B \log \log q \tag{31}$$

*for a suitable fixed constant  $B$  depending only on  $\varepsilon$ , then*

$$\left| \sum_{n \leq N} \chi(n) e(F(n)) \right| \ll \frac{N}{(\log N)^{1-\varepsilon}}.$$

We need the following lemma on convolution of Dirichlet characters, which follows from Theorem 2 in [\[Granville and Soundararajan 2001\]](#) and Corollary 1.3 in [\[Hildebrand and Tenenbaum 1993\]](#), remembering that there they have  $u = \log x / \log y$ .

**Lemma 13.** *Let  $\chi$  be a nonprincipal character modulo  $q$ . Assuming the GRH, for any  $x$  such that*

$$\frac{\log x}{\log \log q} \geq B$$

*for a sufficiently large constant  $B$ , we have*

$$\left| \sum_{n \leq x} \chi(n) \right| \ll x (\log q)^{-(1+o(1))} \frac{\log x \log \left( \frac{\log x}{2 \log \log q} \right)}{2 (\log \log q)^2}.$$

We can thus prove [Corollary 12](#) in a similar fashion to [\[Hildebrand 1988b, Lemma 3\]](#) and [\[Kerr 2020, Lemma 7\]](#).

*Proof of Corollary 12.* Clearly we may suppose

$$\left| \sum_{n \leq N} \chi(n) e(F(n)) \right| \gg \frac{N}{(\log N)^{1-\varepsilon}}.$$

Let  $k$  be as in [Corollary 3](#).

For any  $\psi$  with modulus smaller than or equal to  $k$ , by [Lemma 13](#), we have

$$\max_{u \leq N} \left| \sum_{n \leq u} \psi(n) \chi(n) \right| \ll N (\log q)^{-(1+o(1)) \frac{\log N \log \left( \frac{\log N}{2 \log \log q} \right)}{2 (\log \log q)^2}}.$$

Therefore, by [Corollary 3](#), taking  $r$  large enough in terms of  $\varepsilon$ ,

$$\left| \sum_{n \leq N} \chi(n) e(F(n)) \right| \ll N (\log x)^{d^5} (\log q)^{-(1+o(1)) \frac{\log N \log \left( \frac{\log N}{2 \log \log q} \right)}{2 (\log \log q)^2}} \ll \frac{N}{(\log N)^{1-\varepsilon}}. \quad \square$$

## 9. On the correlation between roots of polynomial congruences and polynomial values

We now prove [Theorem 2](#). Let  $p \in \mathbb{Z}[x]$  be irreducible over  $\mathbb{Q}$  of degree  $e \geq 2$ , and consider the ratios  $v/n$ , where  $v$  are the roots of the polynomial  $p$  modulo  $n$ . In particular,  $v$  and  $n$  satisfy

$$p(v) \equiv 0 \pmod{n}.$$

Define the sequence  $(g_k)_{k \geq 1}$  of these ratios in such a way that the corresponding denominators are in ascending order.

Hooley [\[1964, Theorem 1\]](#) proved that  $(g_k)_{k \geq 1}$  is equidistributed in  $\mathbb{R}/\mathbb{Z}$ . Even stronger than that, he showed

$$\lim_{x \rightarrow \infty} \frac{1}{x} \sum_{n \leq x} \left| \sum_{\substack{v \in \mathbb{Z}/n\mathbb{Z} \\ p(v) \equiv 0 \pmod{n}}} e\left(\frac{hv}{n}\right) \right| = 0 \quad (32)$$

for every  $h \in \mathbb{Z} \setminus \{0\}$ . To prove [Theorem 2](#), by the Weyl equidistribution criteria, it suffices to prove that, for any  $(h_1, h_2) \neq 0$ , we have

$$\sum_{n \leq N} e(h_1 F(n)) \sum_{\substack{v \in \mathbb{Z}/n\mathbb{Z} \\ p(v) \equiv 0 \pmod{n}}} e\left(\frac{h_2 v}{n}\right) = o(N).$$

If  $h_2 \neq 0$  this is true by (32). Thus, the only cases that need to be considered are  $h_2 = 0$  and  $h_1 \neq 0$ . If we let

$$\varrho(n) = |\{v \in \mathbb{Z}/n\mathbb{Z} : p(v) \equiv 0 \pmod{n}\}|, \quad (33)$$

then the problem is therefore to show that

$$\sum_{n \leq N} \varrho(n) e(F(n)) = o(N).$$

We first prove some properties of  $\varrho$ .

**Lemma 14.** *The function  $\varrho$  is multiplicative and satisfies the following:*

(1) *For all  $\epsilon > 0$ ,  $\varrho(n) \leq_\epsilon n^\epsilon$  for  $n \rightarrow \infty$ .*

(2) *There exists a constant  $\lambda > 0$  such that*

$$\sum_{n=1}^N \varrho(n) \sim \lambda N.$$

(3) *There exists a constant  $A \geq 0$  such that*

$$\sum_{n=1}^N \varrho(n)^2 \ll N(\log N)^A$$

*for  $N \geq 2$ .*

(4) *There exists a constant  $D \geq 1$  such that*

$$\varrho(mn) \leq D^{\text{disc}(f)} \varrho(m) \varrho(n)$$

*for all  $m, n \in \mathbb{Z}_{>0}$ .*

*Proof.* The Chinese remainder theorem implies that  $\varrho$  is a multiplicative function. From Wirsing's theorem [1961, Satz 1] we conclude the second item. The proof of the third item is standard (see, e.g., [Crişan and Pollack 2020, Lemma 2.7]).

To conclude the fourth item, we observe that  $\varrho(p^\alpha) = \varrho(p)$  for all primes  $p$ ,  $p \nmid \text{disc}(f)$  and  $\alpha \in \mathbb{Z}_{\geq 1}$ , and  $\varrho(p^\alpha) \leq D$  for all primes  $p$  and a constant  $D > 0$  (for a proof, see, e.g., [Crişan and Pollack 2020, Lemma 2.4]). We also note that if  $p \mid \text{disc}(f)$  and  $\varrho(p^\alpha) \neq 0$  then  $\varrho(p^\beta) \neq 0$  for all  $\beta \leq \alpha$ , and we can conclude the result by factoring  $m$  and  $n$  in primes. Note this also implies the first item, since if  $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  then

$$\varrho(n) \ll D^k \ll D^{\log n / \log \log n}.$$

□

From now on, we fix  $r^* = 2 \max(d(d+1), A)$ ,  $B = 4r^{*2} + 4rA + 1$  and the constants  $\lambda$ ,  $D$  and  $A$  as in Lemma 14.

From Dirichlet's theorem, we can find  $a_i$  and  $1 \leq q_i \leq N^i / (\log N)^B$  coprime integers satisfying

$$\left| \alpha_i - \frac{a_i}{q_i} \right| \leq \frac{(\log N)^B}{q_i N^i} \quad (34)$$

for  $1 \leq i \leq d$ . We also let

$$q = \text{lcm}(q_1, \dots, q_d).$$

**Proposition 15.** *If there exists an  $l \in \{1, \dots, d\}$  such that  $q_l$  satisfies  $q_l \geq (\log N)^B$  then*

$$\sum_{n=1}^N \varrho(n) e(F(n)) \ll \frac{N}{(\log N)^{1/2}}.$$

*Proof.* This follows directly from Theorem 1 applied to  $f = \rho$ ,  $r = r^*$  and  $R = N^\ell / (\log N)^B$ . □

We next focus on establishing the following result.



**Proposition 16.** *Let  $\varepsilon > 0$ , and suppose that  $q_i < (\log N)^B$  for all  $1 \leq i \leq d$ . Then we*

$$\sum_{n=1}^N \varrho(n) e(F(n)) \ll \frac{N}{q^{1/(2d(d+1))-\varepsilon}},$$

where the implied constant depends on  $\varepsilon$ .

Combining [Proposition 16](#) with [Proposition 15](#), one may deduce [Theorem 2](#). Indeed, since at least one of the  $\alpha_i$  is irrational, as  $N \rightarrow \infty$ , the integers  $q_i$  in [\(34\)](#) must satisfy  $q_i \rightarrow \infty$ , which implies

$$\sum_{n=1}^N \varrho(n) e(F(n)) = o(N).$$

To prove [Proposition 16](#) we will proceed with an algebraic approach. We split the task into four subsections: First we make some reductions and provide a proof of the proposition, conditional to further analysis of a different sum. This new sum will be analysed using a Dirichlet series. In the next subsection, we write the Dirichlet series that we want to analyse in terms of better understood  $L$ -functions and in the third subsection we state some of its properties. At last, we gather all the results and conclude the proof.

**9.1. First reductions.** We assume  $q_i < (\log N)^B$  for all  $1 \leq i \leq d$ , and we set, for  $r|q$  and  $Q \in \mathbb{Z}[x]$ ,

$$S_r(N, F) = \sum_{\substack{n=1 \\ (n,q)=r}}^N \varrho(n) e(F(n));$$

we omit  $r$  from the notation when the sum is over all integers  $1 \leq n \leq N$ .

We can split  $S(N, F)$  into two sums as follows:

$$S(N, F) = \sum_{r|q} S_r(N, F) = \sum_{\substack{r|q \\ r < q^{1/(d(d+1))}}} S_r(N, F) + \sum_{\substack{r|q \\ r \geq q^{1/(d(d+1))}}} S_r(N, F). \quad (35)$$

We can bound trivially the second sum of the right-hand side of [\(35\)](#) using [Lemma 14](#). Indeed,

$$\left| \sum_{r|q, r \geq q^{1/(d(d+1))}} S_r(N, F) \right| \leq \sum_{\substack{r|q \\ r \geq q^{1/(d(d+1))}}} \sum_{\substack{n=1 \\ (n,q)=r}}^N \varrho(n) = \sum_{\substack{r|q \\ r \geq q^{1/(d(d+1))}}} \sum_{\substack{n=1 \\ (n,q/r)=1}}^{N/r} \varrho(rn) \ll_{\varepsilon} \frac{N}{q^{1/(d(d+1))-\varepsilon}}. \quad (36)$$

We turn our attention to  $S_r(N, F)$  when  $r \leq 1/(d(d+1))$ . Let

$$\tilde{F}(x) = \sum_{j=1}^d (a_j/q_j) x^j \quad \text{and} \quad Q(x) = F(x) - \tilde{F}(x).$$

Observe that integration by parts yields

$$S_r(N, F) = e(Q(N)) S_r(N, \tilde{F}) - 2\pi i \sum_{j=1}^d j \beta_j \int_1^N u^{j-1} e(Q(u)) S_r(u, \tilde{F}) du, \quad (37)$$

where  $\beta_j$  is defined by

$$\alpha_j = \frac{a_j}{q_j} + \beta_j. \quad (38)$$

In particular, from (34),

$$|\beta_j| \leq \frac{(\log N)^B}{q_j N^j}. \quad (39)$$

The above reduces to analysing  $S_r(N, \tilde{F})$  instead of  $S_r(N, F)$ .

Observe that, since we are summing over multiples of  $r$ , we can rewrite  $e(\tilde{F}(n))$  as  $e(\tilde{F}_r(n))$ , where  $\tilde{F}_r(n) := \tilde{F}(rn)$ , so that the latter is a periodic function modulo  $q/r$ . We let  $q/r = r'$ , and we decompose  $S_r(u, \tilde{F}_r)$  using Dirichlet characters modulo  $r'$  as follows:

$$S_r(N, \tilde{F}) = \sum_{x \bmod r'} e(\tilde{F}_r(x)) \sum_{\substack{m \leq N/r \\ (m, r')=1 \\ m \equiv x \bmod r'}} \varrho(rm) = \frac{1}{\varphi(r')} \sum_{x \bmod r'} e(\tilde{F}_r(x)) \sum_{\chi \bmod r'} \overline{\chi(x)} \sum_{m \leq N/r} \chi(m) \varrho(rm).$$

We will prove the following.

**Proposition 17.** *Let  $\chi$  be a Dirichlet character mod  $r'$ . There exist constants  $c > 0$  and  $0 \leq \delta(\chi) \leq \lambda r$  such that*

$$\sum_{m \leq N/r} \chi(m) \varrho(rm) = \delta(\chi) \frac{N}{r} + O(Ne^{-\frac{1}{c}\sqrt{\log N}}). \quad (40)$$

Moreover, if  $\delta(\chi) \neq 0$  then  $\chi$  has conductor  $h | \text{disc}(p)$ .

We next show that Proposition 17 implies we can conclude the proof of Proposition 16. Indeed, we obtain

$$S_r(N, \tilde{F}) = \frac{N}{r\varphi(r')} \sum_{x \bmod r'} e(\tilde{F}_r(x)) \sum_{\chi \bmod r'} \overline{\chi(x)} \delta(\chi) + O(Ne^{-\frac{1}{c}\sqrt{\log N}}),$$

which substituted into (37) and using (39) implies

$$S_r(N, F) = e(Q(N)) S_r(N, \tilde{F}) - C \int_1^N u \left( 2\pi i \sum_{j=1}^d j \beta_j u^{j-1} \right) e(Q(u)) du + O(Ne^{-\frac{1}{c}\sqrt{\log N}}),$$

with

$$C = \frac{1}{r\varphi(r')} \sum_{x \bmod r'} e(\tilde{F}_r(x)) \sum_{\chi \bmod r'} \overline{\chi(x)} \delta(\chi).$$

Note that integrating by parts yields

$$\int_1^N u \left( 2\pi i \sum_{j=1}^d j \beta_j u^{j-1} \right) e(Q(u)) du \ll N,$$

and since if  $\delta(\chi) \neq 0$  then  $\chi$  has conductor  $h | \text{disc}(p)$ , the above implies

$$S_r(N, F) \ll \frac{N}{r} \frac{1}{\phi(r')} \sum_{x \bmod r'} \chi(x) e(\tilde{F}_r(x)) + O(Ne^{-\frac{1}{c}\sqrt{\log N}}) \quad (41)$$

for some  $\chi$  with conductor  $h | \text{disc}(p)$ . Recall that

$$\tilde{F}_r(x) = \tilde{F}(rx) = \sum_{j=1}^d \frac{a_j r^j}{q_j} x^j = \frac{\sum_{j=1}^d (q a_j r^j / q_j) x^j}{q}.$$

Let  $q'$  denote the smallest divisor of  $q$  such that the polynomial

$$P(x) = \sum_{j=1}^d (qa_j r^j / q_j) x^j$$

is constant mod  $q/q'$ . Note that, for each  $1 \leq j \leq d$ ,

$$\frac{qa_j r^j}{q_j} \equiv 0 \pmod{q/q'}.$$

Since  $(a_j, q_j) = 1$ , this implies

$$q' > \frac{q_j}{r^j} \geq \left( \prod_{j=1}^d \frac{q_j}{r^j} \right)^{1/d} \geq \frac{q^{1/d}}{r^{(d+1)/2}} \geq q^{1/(2d)},$$

provided  $r \leq q^{1/(d(d+1))}$ .

It follows from [Cochrane and Zheng 1999, Corollary 1.1] and the Chinese remainder theorem that

$$\sum_{x \bmod r'} \chi(x) e(\tilde{F}_r(x)) \ll \frac{r'}{q'} (q')^{1-1/d} \ll \frac{r'}{q^{1/(2d(d+1))}}.$$

Combining the above with (41) gives

$$S_r(N, F) \leq \frac{N}{q^{1/(2d(d+1))}} \quad \text{provided } r \leq q^{1/(d(d+1))}.$$

Summing over  $r < q^{1/(d(d+1))}$ , we get

$$\sum_{\substack{r|q \\ r < q^{1/(d(d+1))}}} S_r(N, \tilde{F}) \leq \frac{N}{q^{1/(2d(d+1))+o(1)}}.$$

Together with (35) and (36) this concludes the proof of Proposition 16. We will now focus on the proof of Proposition 17. In order to understand the sum

$$\sum_{n \leq N/r} \varrho(rn) \chi(n), \tag{42}$$

we study the Dirichlet series for  $\chi \bmod r'$ :

$$D_r(s, \chi) = \sum_{n=1}^{\infty} \varrho(rn) \chi(n) n^{-s}.$$

**9.2. Decomposing  $D_r(s, \chi)$ .** Observe that  $D_r(s, \chi)$  is absolutely convergent for  $\operatorname{Re}(s) > 1$ . Our next goal is to extend  $D_r(s, \chi)$  to the left of  $\operatorname{Re}(s) > 1$  so that we can use contour integration to estimate the sum (42). We will do this by decomposing  $D_r$  in terms of well-known Artin  $L$ -functions. With this in mind, we fix some notation.

Denote by  $K_f$  the splitting field of  $f$  in  $\mathbb{C}$ , by  $G$  the Galois group of  $K_f$  over  $\mathbb{Q}$  and by  $\mathbb{Q}(e(1/r'))$  the cyclotomic field generated by  $r'$ -roots of unity. Observe that the latter is a Galois extension of  $\mathbb{Q}$ , with Galois group  $C_{r'}$  isomorphic to  $(\mathbb{Z}/r'\mathbb{Z})^\times$ .

We also consider the compositum of  $K_f$  and  $\mathbb{Q}(e(1/r'))$  and denote it by  $K_{f,r'}$  and its Galois group over  $\mathbb{Q}$  by  $G_{r'}$ . Observe that there is a natural injection

$$G_{r'} \rightarrow G \times C_{r'} \simeq G \times (\mathbb{Z}/r'\mathbb{Z})^\times.$$

Moreover, observe that, from the extension theorem for field automorphism, it follows that the projections  $p_1 : G_{r'} \rightarrow G$  and  $p_2 : G_{r'} \rightarrow (\mathbb{Z}/r'\mathbb{Z})^\times$  are surjective.

We denote by  $\hat{G}$  the finite set of isomorphism classes of complex irreducible representations of  $G$  and, for  $\pi \in \hat{G}$ , we write  $\chi_\pi$  for the character of  $\pi$ .

Note that  $\chi$  can be viewed as a character of  $(\mathbb{Z}/r'\mathbb{Z})^\times$  and consequently as a character  $\eta : C_{r'} \rightarrow \mathbb{C}^\times$ . It is known that  $\eta(\sigma_p) = \chi(p)$  for  $p \nmid r'$  and  $\sigma_p$  the Frobenius automorphism at  $p$ .

So, we consider the representations  $p_1^* \pi = \pi \circ p_1$  and  $p_2^* \eta = \eta \circ p_2$  of  $G_{r'}$  and observe that their tensor product satisfies

$$\mathrm{tr}(p_1^* \pi \otimes p_2^* \eta(\sigma_p)) = \chi_\pi(\sigma_p) \chi(p) \quad (43)$$

for  $p \nmid \mathrm{disc}(f)$  and  $p \nmid r'$ .

**Proposition 18.**  $D_r(s, \chi)$  has an expression

$$D_r(s, \chi) = F_r(s, \chi) \prod_{\pi \in \hat{G}} E_{r,\pi}(s, \chi) (L(s, K_{f,r'}/\mathbb{Q}, p_1^* \pi \otimes p_2^* \eta))^{m_\pi}$$

for  $m_\pi \geq 0$  an integer and, for any  $\epsilon > 0$ ,  $F_r \ll_\epsilon q^\epsilon$  and  $E_{r,\pi} \ll q^\epsilon$  for  $\mathrm{Re}(s) \geq \frac{3}{4}$ .

To prove the proposition we will need the following lemma.

**Lemma 19.** Denote by  $\pi_f$  the permutation representation of  $G$  acting on the set of roots of  $f$  in  $\mathbb{C}$ , and let

$$\pi_f = \bigoplus_{\pi \in \hat{G}} m_\pi \pi$$

be its decomposition in irreducible representations, where  $m_\pi \geq 0$  are integers. For all  $p \nmid \mathrm{disc}(f)$ , we have

$$\varrho(p) = \sum_{\pi} m_\pi \cdot \chi_\pi(\sigma_p) \quad (44)$$

for  $\sigma_p \in G$  the Frobenius automorphism at  $p$ .

*Proof.* The proof follows by noting that  $\varrho(p)$  is the number of fixed points of the Frobenius automorphism  $\sigma_p$  at  $p$ , which is also the character at  $\sigma_p$  of the permutation representation.  $\square$

*Proof of Proposition 18.* First we observe that  $D_r$  can be decomposed as

$$D_r(s, \chi) = \sum_{e|r^\infty} \sum_{(k,r)=1} \chi(ek) \varrho(erk) (ek)^{-s} = \sum_{e|r^\infty} \varrho(er) \chi(e) e^{-s} \sum_{(k,r)=1} \chi(k) \varrho(k) k^{-s},$$

where the notation  $e|r^\infty$  means that  $e$  runs over all possible products of powers of the primes that divide  $r$ .

We define

$$E_r(s, \chi) = \sum_{e|r^\infty} \varrho(er) \chi(e) e^{-s}$$

$$\tilde{D}_r(s, \chi) = \sum_{(k,r)=1} \chi(k) \varrho(k) k^{-s},$$

and, using [Lemma 14](#) and the property  $\varrho(p^n) \leq C$  for all  $n \geq 1$  and  $p$  prime, we observe that  $E_r(s, \chi) \ll r^\epsilon$  uniformly for  $\operatorname{Re}(s) \geq \frac{3}{4}$  and that  $\tilde{D}_r(s, \chi)$  converges absolutely for  $\operatorname{Re}(s) > 1$ .

To be able to explore the properties of  $\varrho$ , we factor the primes that divide the discriminant of  $f$  in  $\tilde{D}_r(s, \chi)$  and, since  $r \mid q$ , we also factor the remaining primes that divide  $q$ . This yields

$$\tilde{D}_r(s, \chi) = E_{1,r}(s, \chi) \prod_{\substack{p \nmid \operatorname{disc}(f) \\ p \nmid q}} \sum_{k \geq 0} \varrho(p^k) \chi(p)^k p^{-ks},$$

where  $E_{1,r}(s, \chi)$  is entire and bounded for  $\operatorname{Re}(s) \geq \frac{3}{4}$  by  $C(\epsilon)q^\epsilon$ .

We proceed in a similar manner and factor out the prime powers with exponent larger than 2, obtaining

$$\tilde{D}_r(s, \chi) = E_{1,r}(s, \chi) E_2(s, \chi) \prod_{\substack{p \nmid \operatorname{disc}(f) \\ p \nmid q}} (1 + \varrho(p) \chi(p) p^{-s}) \quad (45)$$

for  $E_2(s, \chi)$  holomorphic and bounded in vertical strips by  $C(\epsilon)q^\epsilon$  for  $\operatorname{Re}(s) \geq \frac{3}{4}$ .

Now we can use [Lemma 19](#) and a further decomposition to write

$$\tilde{D}_r(s, \chi) = E_{1,r}(s, \chi) E_2(s, \chi) E_{3,r}(s, \chi) \prod_{\pi \in \hat{G}} \prod_p (1 + \chi_\pi(\sigma_p) \chi(p) p^{-s})^{m_\pi}$$

for  $E_{3,r}$  holomorphic and uniformly bounded in vertical strips by  $C(\epsilon, f)q^\epsilon$  for  $\operatorname{Re}(s) \geq \frac{3}{4}$ . We now set  $F_r = E_{1,r} E_2 E_{3,r}$ . To conclude, we use equality (43) and yet another similar decomposition as before and obtain

$$\prod_p (1 + \chi_\pi(\sigma_p) \chi(p) p^{-s}) = E_{r,\pi}(s, \chi) L(s, K_{f,q}/\mathbb{Q}, p_1^* \pi \otimes p_2^* \eta). \quad \square$$

Observe that now we are dealing with Artin  $L$ -functions, which are better understood than the original Dirichlet series. Since  $p_1$  is surjective and  $\pi$  is irreducible, it follows that  $p_1^* \pi$  is an irreducible representation. Furthermore, since  $p_2^* \eta$  is of dimension 1, we can conclude that  $p_1^* \pi \otimes p_2^* \eta$  is also an irreducible representation. Artin's conjecture states that this  $L$ -function is entire except if the representation is trivial — which can occur if  $p_1^* \pi$  is the inverse of  $p_2^* \eta$ .

To avoid assuming Artin's conjecture, we will use the Brauer induction theorem instead (see, e.g., [\[Serre 1977, Theorem 19\]](#)). It states that, for every subgroup  $H$  of  $G$  and one-dimensional character  $\beta_H : H \rightarrow \mathbb{C}^\times$ , there exist integers  $n_{\pi, \beta_H}$  such that

$$\chi_\pi = \sum_H \sum_{\beta_H} n_{\pi, \beta_H} \cdot \operatorname{Ind}_H^G \beta_H.$$

Observe that this implies that  $L(s, K_{f,q}/\mathbb{Q}, p_1^* \pi)$  can be represented as

$$\begin{aligned} L(s, K_{f,q}/\mathbb{Q}, p_1^* \pi) &= L(s, K_f/\mathbb{Q}, \pi) = \prod_H \prod_{\beta_H} L(s, K_f/\mathbb{Q}, \text{Ind}_H^G \beta_H)^{n_{\pi, \beta_H}} \\ &= \prod_H \prod_{\beta_H} L(s, K_f/K_H, \beta_H)^{n_{\pi, \beta_H}}, \end{aligned}$$

where  $K_H \subset K_f$  is the subfield fixed by  $H$  — which implies that  $H$  is the Galois group of  $K_f$  over  $K_H$ .

We can now introduce the twist by the Dirichlet character. We write  $H' = p_1^{-1}(H)$  and observe that we can write

$$p_1^* \pi = \bigoplus_H n_{\pi, \beta_H} \text{Ind}_{H'}^{G_{r'}}(p_1^* \beta_H),$$

and thus

$$p_1^* \pi \otimes p_2^* \eta = \bigoplus_H \bigoplus_{\beta_H} n_{\pi, \beta_H} \text{Ind}_{H'}^{G_{r'}}(p_1^* \beta_H \otimes \text{Res}_{H'}^{G_{r'}} p_2^* \eta).$$

So, defining  $\theta_{\beta_H} = p_1^* \beta_H \otimes \text{Res}_{H'}^{G_{r'}} p_2^* \eta$ , we can finally write

$$L(s, K_{f,q}/\mathbb{Q}, p_1^* \chi \otimes p_2^* \eta) = \prod_H \prod_{\beta_H} L(s, K_{f,q}/K_H, \theta_{\beta_H})^{n_{\pi, \beta_H}},$$

and thus  $D_r$  has the representation

$$D_r(s, \chi) = F_r(s, \chi) \prod_{\pi \in \hat{G}} E_{r, \pi}(s, \chi) \prod_H \prod_{\beta_H} L(s, K_{f,q}/K_H, \theta_{\beta_H})^{n_{\pi, \beta_H}}. \quad (46)$$

Now the  $L(s, K_{f,q}/K_H, \theta_{\beta_H})^{n_{\pi, \beta_H}}$  are Artin  $L$ -functions of dimension 1, which we know are entire except for a pole at  $s = 1$  if  $\theta_{\beta_H}$  is the trivial one-dimensional character.

**9.3. Bounds on the Artin  $L$ -functions near  $s = 1$ .** We denote by  $q_{\pi, i}$  the conductor of  $L(s, K_{f,q}/K_H, \theta_{\beta_H})$  and observe that we can bound it as follows (see, e.g., [Bushnell and Henniart 1997]):

$$q_{\pi, \beta_H} \leq \text{cond}(p_1^* \beta_H) \cdot \text{cond}(\text{Res}_{H'}^{G_q} p_2^* \eta) \leq Mq,$$

where  $M = \sup_{\pi, \beta_H} \text{cond}(p_1^* \beta_H)$ . It is well known that  $L(s, K_{f,q}/K_H, \theta_{\beta_H})$  can have at most one real zero  $\beta$  in the region

$$\sigma \geq 1 - \frac{c}{\log(q_{\pi, \beta_H}(|t| + 3))} \quad (47)$$

for  $s = \sigma + it \in \mathbb{C}$  and  $c$  a universal constant; see, e.g., [Iwaniec and Kowalski 2004, Theorem 5.35]. Note that this zero can only exist if  $\theta_i$  is a quadratic character.

To simplify the notation, in what follows we let  $g = \theta_{\beta_H}$  and we omit the field  $K_{f,q}/K_H$ . Denote by  $\beta$  the possible exception in region (47) and let  $q$  be the conductor of  $g$ . Also, we set  $r_1 = 1$  if  $g$  has an exceptional zero  $\beta$ , and  $r_1 = 0$  otherwise. Analogously,  $r_2 = 1$  if  $g$  is the trivial character and consequently has a pole at  $s = 1$ , and  $r_2 = 0$  if not.

**Proposition 20.** *Let  $s = \sigma + it \in \mathbb{C}$  satisfy the conditions*

$$\sigma \geq 1 - \frac{c}{10 \log(Mq(|t| + 3))}, \quad (48)$$

$$|s - \beta| \geq \frac{1}{20 \log(3Mq)}, \quad (49)$$

$$|s - 1| \geq \frac{1}{20 \log(3Mq)}. \quad (50)$$

We have that

$$L(s, g) \ll \log(Mq(|t| + 3)), \quad \frac{1}{L(s, g)} \ll \log(Mq(|t| + 3)),$$

where the implied constant does not depend on the parameters.

If  $g$  is not trivial, condition (50) can be dropped. Condition (49) can be dropped if  $g$  has no exceptional zero.

*Proof.* We set  $\gamma(s, g) = \pi^{-s/2} \gamma(\frac{1}{2}(s + \kappa_g))$ , where  $\kappa_g = 0$  or  $1$ , and let  $\Lambda(s, g) = q^{s/2} \gamma(s, g) L(s, g)$  be the extended  $L$ -function. It is a known fact that  $\Lambda(s, g)$  is a meromorphic function of order at most 1. Thus, we can proceed as in [Montgomery and Vaughan 2007, Theorem 11.4] to obtain the proposition.  $\square$

#### 9.4. Finishing the proof.

*Proof of Proposition 16.* To bound the sum  $\sum_{n \leq N/r} \varrho(rn) \chi(n)$  we first smooth it:

$$\sum_{\substack{n=1 \\ (n,q)=r}}^{N/r} \varrho(n) \chi(n) = \sum_{\substack{n=1 \\ (n,q)=r}}^{\infty} \varrho(n) \chi(n) \phi(n) + O(\tilde{N}),$$

where  $\phi$  is defined as

$$\phi(x) = \min\left(x, 1, 1 + \frac{N/r - x}{\tilde{N}}\right)$$

for  $0 \leq x \leq N/r + \tilde{N}$ , and  $\phi(x) = 0$  for  $x > N/r + \tilde{N}$ , with  $\tilde{N} > 0$  to be chosen later. Observe that Mellin inversion implies that

$$\begin{aligned} \sum_{\substack{n=1 \\ (n,q)=r}}^{\infty} \varrho(n) \chi(n) \phi(n) &= \frac{1}{2\pi i} \int_{(3)} D_r(s, \chi) \hat{\phi}(s) ds \\ &= \frac{1}{2\pi i} \int_{(3)} F_r(s, \chi) \prod_{\pi \in \hat{G}} E_{r,\pi}(s, \chi) (L(s, K_{f,r'}/\mathbb{Q}, p_1^* \pi \otimes p_2^* \eta))^{m_\pi} \hat{\phi}(s) ds \\ &= \frac{1}{2\pi i} \int_{(3)} F_r(s, \chi) \prod_{\pi \in \hat{G}} E_{r,\pi}(s, \chi) \prod_H \prod_{\beta_H} L(s, K_{f,q}/K'_H, \theta_{\beta_H})^{n_{\pi, \beta_H}} \hat{\phi}(s) ds, \end{aligned} \quad (51)$$

where (3) denotes the contour obtained by traversing the straight line  $\{s = 3 + it, t \in \mathbb{R}\}$  from  $t = -\infty$  to  $t = +\infty$ .



Our goal is to shift the contour of integration and use the information on the  $L$ -functions

$$L(s, K_{f,q}/K'_H, \theta_{\beta_H})$$

to obtain good bounds for  $S_r(s, \tilde{F}_r)$ . Observe that we can find  $\frac{1}{2}c \leq Q \leq \frac{1}{10}c$  such that all the conditions of [Proposition 20](#) are satisfied for

$$s \in \mathcal{Z} = \left\{ s = \sigma + it, \sigma = 1 - \frac{Q}{\log(Mq(|t|+3))} \right\}.$$

Moving the contour of integration in (51) to  $\mathcal{Z}$ , we get

$$\begin{aligned} \sum_{\substack{n=1 \\ (n,q)=r}}^{\infty} \varrho(n) \chi(n) \phi(n) \\ = \frac{1}{2\pi i} \int_{\mathcal{Z}} D_r(s, \chi) \hat{\phi}(s) ds + \alpha \operatorname{Res}(D_r(s, \chi), 1) \cdot \frac{N}{r} + \tilde{\alpha} \operatorname{Res}(D_r(s, \chi), \beta) \cdot N^{\beta}, \end{aligned} \quad (52)$$

where  $\alpha = 1$  if there is  $\pi \in \hat{G}$  for which  $p_1^* \pi \otimes p_2^* \eta$  is the principal character in  $K_{f,r'}/\mathbb{Q}$  with  $m_{\pi} = 1$ , and  $\alpha = 0$  otherwise. Likewise,  $\tilde{\alpha} = 1$  if  $L(s, K_{f,q}/K'_H, \theta_{\beta_H})$  has an exceptional zero  $\beta$  and  $n_{\pi, \beta_H} = -1$ , and  $\tilde{\alpha} = 0$  otherwise. Note from [Proposition 18](#) that there is at most one trivial character  $p_1^* \pi \otimes p_2^* \eta$  and one quadratic character  $\theta_{\beta_H}$ . Moreover, if  $p_1^* \pi \otimes p_2^* \eta$  is the trivial character, then we observe that  $\chi$  must have a conductor with modulus  $h$  that divides  $\operatorname{disc}(f)$ .

We bound each term of the right-hand side of (52) separately. To bound the first term, we note that the Mellin transform of  $\phi$  satisfies

$$\hat{\phi}(s) = \int_0^{N+\tilde{N}} \phi(z) z^{s-1} dz \ll \frac{N^{\sigma}}{|s|} \min\left(1, \frac{N}{|s|\tilde{N}}\right),$$

where  $\sigma = \operatorname{Re}(s)$ ; see [\[Iwaniec and Kowalski 2004, Theorem 5.12\]](#). Thus,

$$\int_{\mathcal{Z}} D_r(s, \chi) \hat{\phi}(s) ds \ll \int_{\mathcal{Z}} |D_r(s, \chi)| \frac{N^{\sigma}}{|s|} \min\left(1, \frac{N}{|s|\tilde{N}}\right) |ds|.$$

We let  $T = N/(r\tilde{N})$  and  $\sigma(T) = 1 - Q/\log(Mq(T+3))$ , and we note that the observation above and [Propositions 18](#) and [20](#) imply that

$$\int_{\mathcal{Z}} D_r(s, \chi) \hat{\phi}(s) ds \ll N^{\sigma(T)} q^{Y\epsilon}$$

for a constant  $Y > 0$  that only depends on  $f$ .

We now deal with the last term  $\tilde{\alpha} \operatorname{Res}(D_r(s, \chi), \beta) \cdot N^{\beta}$ . Siegel proved (see, e.g., [\[Iwaniec and Kowalski 2004, Theorem 5.28\]](#)) that if the exceptional zero  $\beta$  exists then, for every  $\epsilon > 0$ , there exists a constant  $C(\epsilon) > 0$  such that

$$\beta \leq 1 - \frac{c(\epsilon)}{\operatorname{cond}(\theta_i)^{\epsilon}} \leq 1 - \frac{c(\epsilon)}{Mq^{\epsilon}}. \quad (53)$$

To bound the residue at  $\beta$  we notice that, if  $\theta_{\pi, \beta_H}$  is not trivial, we can use [Proposition 20](#) and obtain

$$|L(s, K_{f,q}/K'_H, \theta_{\beta_H})|^{n_{\pi,i}} \ll |\log 3Mq|^{n_{\pi, \beta_H}}.$$

If  $\theta_{\beta_H}$  is trivial then

$$|L(s, K_{f,q}/K'_H, \theta_{\beta_H})|^{n_{\pi, \beta_H}} \ll_{\epsilon} q^{\epsilon |n_{\pi, \beta_H}|},$$

and, for the residue given by the  $L$ -function with quadratic character, we have

$$\text{Res}\left(\frac{1}{L(s, K_{f,q}/K'_H, \theta_{\beta_H})}, \beta\right) = \frac{1}{L(s, K_{f,q}/K'_H, \theta_{\beta_H})}.$$

We can deduce that  $L'(s, K_{f,q}/K'_H, \theta_{\beta_H}) \gg 1$  from the last part of Theorem 11.4 in [Montgomery and Vaughan 2007]. Putting everything together, we obtain

$$\text{Res}(D_r(s, \chi), \beta) \cdot N^{\beta} \leq q^{\epsilon} N^{1-C(\epsilon)/q^{\epsilon}}.$$

Pick  $T = \exp(\frac{1}{3}\sqrt{\log N})$ . Since  $q \leq (\log N)^B$ , the considerations above imply that

$$S_r(N, \tilde{F}_r) = \alpha \text{Res}(D_r(s, \chi), 1) \cdot \frac{N}{r} + O(Ne^{-\frac{1}{c(\epsilon)}\sqrt{\log N}}) \quad (54)$$

for a constant  $c(\epsilon)$  and  $\epsilon > 0$  sufficiently small. Since

$$\sum_{n \leq N} \varrho(n) \leq \lambda N$$

and the error term in (54) is  $o(N)$ , we conclude that

$$\text{Res}(D_r(s, \chi), 1) \leq \lambda r. \quad \square$$

## 10. Sharpness of Theorem 1

Following the approach of [Montgomery and Vaughan 1977], we will construct a completely multiplicative function  $f = f_{N,F}$ , with  $|f(n)| \leq 1$ , such that

$$\left| \sum_{n \leq N} f(n) e(F(n)) \right| \geq \frac{1}{10} \frac{N}{\log N}. \quad (55)$$

We first observe that the function  $G : \mathbb{C} \rightarrow \mathbb{C}$  given by

$$G(z) = \sum_{n \leq N} z^{\Omega(n)} e(F(n)) + \sum_{N/2 < p \leq N} (1 - ze(F(p)))$$

is entire and its value at zero satisfies

$$G(0) = \sum_{N/2 < p \leq N} 1 \geq \frac{1}{10} \frac{N}{\log N}$$

for  $N$  sufficiently large. Thus, by the maximum modulus principle, there exists a  $z_0 \in \mathbb{C}$ ,  $|z_0| = 1$ , such that  $|G(z_0)| \geq |G(0)|$ .

Define the completely multiplicative function  $f$  by  $f(p) = z_0$  for  $p \leq \frac{1}{2}N$ , and  $f(p) = e(-F(p))$  for  $p > \frac{1}{2}N$ . To conclude that (55) is satisfied, we just observe that

$$\sum_{n \leq N} f(n) e(F(n)) = \sum_{n \leq N} z_0^{\Omega(n)} e(F(n)) + \sum_{N/2 < p \leq N} (1 - z_0 e(F(p))) = G(z_0) \gg \frac{N}{\log N}.$$

## Acknowledgements

We would like to thank Emmanuel Kowalski for his helpful comments and suggestions. We would also like to thank Alberto Perelli for a useful conversation and his helpful comments.

Matteo Bordignon was supported in part by OP RDE project no. CZ.02.2.69/0.0/0.0/18\_053/0016976 International mobility of research, technical and administrative staff at the Charles University, in part by an Australian Mathematical Society Lift-off Fellowship and in part while a Ph.D. student of the University of New South Wales Canberra.

Bryce Kerr would like to acknowledge the support of the Max Planck Institute for Mathematics and the Australian Research Council (DE220100859).

## References

- [Bachman 2003] G. Bachman, “On exponential sums with multiplicative coefficients, II”, *Acta Arith.* **106**:1 (2003), 41–57. [MR](#) [Zbl](#)
- [Bourgain et al. 2013] J. Bourgain, P. Sarnak, and T. Ziegler, “Disjointness of Moebius from horocycle flows”, pp. 67–83 in *From Fourier analysis and number theory to Radon transforms and geometry*, edited by H. M. Farkas et al., Dev. Math. **28**, Springer, 2013. [MR](#) [Zbl](#)
- [Bourgain et al. 2016] J. Bourgain, C. Demeter, and L. Guth, “Proof of the main conjecture in Vinogradov’s mean value theorem for degrees higher than three”, *Ann. of Math.* (2) **184**:2 (2016), 633–682. [MR](#) [Zbl](#)
- [de la Bretèche 1998] R. de la Bretèche, “Sommes d’exponentielles et entiers sans grand facteur premier”, *Proc. London Math. Soc.* (3) **77**:1 (1998), 39–78. [MR](#) [Zbl](#)
- [de la Bretèche and Granville 2022] R. de la Bretèche and A. Granville, “Exponential sums with multiplicative coefficients and applications”, *Trans. Amer. Math. Soc.* **375**:10 (2022), 6875–6901. [MR](#) [Zbl](#)
- [Bushnell and Henniart 1997] C. J. Bushnell and G. Henniart, “An upper bound on conductors for pairs”, *J. Number Theory* **65**:2 (1997), 183–196. [MR](#) [Zbl](#)
- [Chang 2010] M.-C. Chang, “An estimate of incomplete mixed character sums”, pp. 243–250 in *An irregular mind*, edited by I. Bárány and J. Solymosi, Bolyai Soc. Math. Stud. **21**, János Bolyai Math. Soc., Budapest, 2010. [MR](#) [Zbl](#)
- [Chang 2014] M.-C. Chang, “Short character sums for composite moduli”, *J. Anal. Math.* **123** (2014), 1–33. [MR](#) [Zbl](#)
- [Cochrane and Zheng 1999] T. Cochrane and Z. Zheng, “Pure and mixed exponential sums”, *Acta Arith.* **91**:3 (1999), 249–278. [MR](#) [Zbl](#)
- [Crişan and Pollack 2020] V. Crişan and P. Pollack, “The smallest root of a polynomial congruence”, *Math. Res. Lett.* **27**:1 (2020), 43–66. [MR](#) [Zbl](#)
- [Daboussi 1975] H. Daboussi, “Fonctions multiplicatives presque périodiques B”, pp. 321–324 in *Journées Arithmétiques de Bordeaux* (Conf., Univ. Bordeaux, 1974), Astérisque **24–25**, Société Mathématique de France, Paris, 1975. [MR](#) [Zbl](#)
- [Enflo 1995] P. Enflo, “Some problems in the interface between number theory, harmonic analysis and geometry of Euclidean space”, *Quaestiones Math.* **18**:1–3 (1995), 309–323. [MR](#) [Zbl](#)
- [Gong and Jia 2015] K. Gong and C. Jia, “Shifted character sums with multiplicative coefficients”, *J. Number Theory* **153** (2015), 364–371. [MR](#) [Zbl](#)
- [Granville and Soundararajan 2001] A. Granville and K. Soundararajan, “Large character sums”, *J. Amer. Math. Soc.* **14**:2 (2001), 365–397. [MR](#) [Zbl](#)
- [Granville and Soundararajan 2007] A. Granville and K. Soundararajan, “Large character sums: pretentious characters and the Pólya–Vinogradov theorem”, *J. Amer. Math. Soc.* **20**:2 (2007), 357–384. [MR](#) [Zbl](#)
- [Heath-Brown and Pierce 2015] D. R. Heath-Brown and L. B. Pierce, “Burgess bounds for short mixed character sums”, *J. Lond. Math. Soc.* (2) **91**:3 (2015), 693–708. [MR](#) [Zbl](#)

- [Hildebrand 1988a] A. Hildebrand, “Large values of character sums”, *J. Number Theory* **29**:3 (1988), 271–296. [MR](#) [Zbl](#)
- [Hildebrand 1988b] A. Hildebrand, “On the constant in the Pólya–Vinogradov inequality”, *Canad. Math. Bull.* **31**:3 (1988), 347–352. [MR](#) [Zbl](#)
- [Hildebrand and Tenenbaum 1993] A. Hildebrand and G. Tenenbaum, “Integers without large prime factors”, *J. Théor. Nombres Bordeaux* **5**:2 (1993), 411–484. [MR](#) [Zbl](#)
- [Hooley 1964] C. Hooley, “On the distribution of the roots of polynomial congruences”, *Mathematika* **11** (1964), 39–49. [MR](#) [Zbl](#)
- [Hua 1965] L. K. Hua, *Additive theory of prime numbers*, Translations of Mathematical Monographs **Vol. 13**, Amer. Math. Soc., Providence, RI, 1965. [MR](#) [Zbl](#)
- [Indlekofer and Kátai 1989] K.-H. Indlekofer and I. Kátai, “Exponential sums with multiplicative coefficients”, *Acta Math. Hungar.* **54**:3–4 (1989), 263–268. [MR](#) [Zbl](#)
- [Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications **53**, Amer. Math. Soc., Providence, RI, 2004. [MR](#) [Zbl](#)
- [Jiang et al. 2021] Y. Jiang, G. Lü, and Z. Wang, “Exponential sums with multiplicative coefficients without the Ramanujan conjecture”, *Math. Ann.* **379**:1–2 (2021), 589–632. [MR](#) [Zbl](#)
- [Karatsuba 2010] A. A. Karatsuba, “New estimates for short Kloosterman sums”, *Mat. Zametki* **88**:3 (2010), 384–398. [MR](#) [Zbl](#)
- [Kátai 1986] I. Kátai, “A remark on a theorem of H. Daboussi”, *Acta Math. Hungar.* **47**:1–2 (1986), 223–225. [MR](#) [Zbl](#)
- [Kerr 2020] B. Kerr, “On the constant in the Pólya–Vinogradov inequality”, *J. Number Theory* **212** (2020), 265–284. [MR](#) [Zbl](#)
- [Korolëv 2018] M. A. Korolëv, “Kloosterman sums with multiplicative coefficients”, *Izv. Ross. Akad. Nauk Ser. Mat.* **82**:4 (2018), 3–17. In Russian; translated in *Izv. Math.* **82**:4 (2018), 647–661. [MR](#) [Zbl](#)
- [Korolev and Shparlinski 2020] M. Korolev and I. Shparlinski, “Sums of algebraic trace functions twisted by arithmetic functions”, *Pacific J. Math.* **304**:2 (2020), 505–522. [MR](#) [Zbl](#)
- [Matomäki et al. 2023] K. Matomäki, M. Radziwiłł, T. Tao, J. Teräväinen, and T. Ziegler, “Higher uniformity of bounded multiplicative functions in short intervals on average”, *Ann. of Math. (2)* **197**:2 (2023), 739–857. [MR](#) [Zbl](#)
- [Matthiesen 2018] L. Matthiesen, “Generalized Fourier coefficients of multiplicative functions”, *Algebra Number Theory* **12**:6 (2018), 1311–1400. [MR](#) [Zbl](#)
- [Matthiesen 2020] L. Matthiesen, “Linear correlations of multiplicative functions”, *Proc. Lond. Math. Soc. (3)* **121**:2 (2020), 372–425. [MR](#) [Zbl](#)
- [Montgomery and Vaughan 1977] H. L. Montgomery and R. C. Vaughan, “Exponential sums with multiplicative coefficients”, *Invent. Math.* **43**:1 (1977), 69–82. [MR](#) [Zbl](#)
- [Montgomery and Vaughan 2007] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory, I: Classical theory*, Cambridge Studies in Advanced Mathematics **97**, Cambridge Univ. Press, 2007. [MR](#) [Zbl](#)
- [Serre 1977] J.-P. Serre, *Linear representations of finite groups*, Grad. Texts in Math. **42**, Springer, 1977. [MR](#) [Zbl](#)
- [Wirsing 1961] E. Wirsing, “Das asymptotische Verhalten von Summen über multiplikative Funktionen”, *Math. Ann.* **143** (1961), 75–102. [MR](#) [Zbl](#)
- [Wooley 2016] T. D. Wooley, “The cubic case of the main conjecture in Vinogradov’s mean value theorem”, *Adv. Math.* **294** (2016), 532–561. [MR](#) [Zbl](#)

Communicated by Roger Heath-Brown

Received 2023-06-18

Revised 2024-07-21

Accepted 2024-09-03

[matteobordignon91@gmail.com](mailto:matteobordignon91@gmail.com)

Department of Mathematics, KTH Royal Institute of Technology, Stockholm, Sweden

Faculty of Mathematics and Physics, Charles University, Praha, Czech Republic

[cynthia.bortolotto@math.ethz.ch](mailto:cynthia.bortolotto@math.ethz.ch)

Department of Mathematics, ETH Zürich, Zürich, Switzerland

[bryce.kerr@unsw.edu.au](mailto:bryce.kerr@unsw.edu.au)

University of New South Wales, School of Science, Canberra, Australia

# Algebra & Number Theory

[msp.org/ant](http://msp.org/ant)

## EDITORS

### MANAGING EDITOR

Antoine Chambert-Loir  
Université Paris-Diderot  
France

### EDITORIAL BOARD CHAIR

David Eisenbud  
University of California  
Berkeley, USA

## BOARD OF EDITORS

Jason P. Bell	University of Waterloo, Canada	Philippe Michel	École Polytechnique Fédérale de Lausanne
Bhargav Bhatt	University of Michigan, USA	Martin Olsson	University of California, Berkeley, USA
Frank Calegari	University of Chicago, USA	Irena Peeva	Cornell University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Saclay, France	Jonathan Pila	University of Oxford, UK
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Samit Dasgupta	Duke University, USA	Bjorn Poonen	Massachusetts Institute of Technology, USA
Hélène Esnault	Freie Universität Berlin, Germany	Victor Reiner	University of Minnesota, USA
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Peter Sarnak	Princeton University, USA
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	SUNY Buffalo, USA
Wee Teck Gan	National University of Singapore	Shunsuke Takagi	University of Tokyo, Japan
Andrew Granville	Université de Montréal, Canada	Pham Huu Tiep	Rutgers University, USA
Ben J. Green	University of Oxford, UK	Ravi Vakil	Stanford University, USA
Christopher Hacon	University of Utah, USA	Akshay Venkatesh	Institute for Advanced Study, USA
Roger Heath-Brown	Oxford University, UK	Melanie Matchett Wood	Harvard University, USA
János Kollár	Princeton University, USA	Shou-Wu Zhang	Princeton University, USA
Michael J. Larsen	Indiana University Bloomington, USA		

## PRODUCTION

[production@msp.org](mailto:production@msp.org)

Silvio Levy, Scientific Editor

---

See inside back cover or [msp.org/ant](http://msp.org/ant) for submission instructions.

---

The subscription price for 2025 is US \$565/year for the electronic version, and \$820/year (+\$70, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.


---

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

---

ANT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2025 Mathematical Sciences Publishers

# Algebra & Number Theory

Volume 19    No. 8    2025

---

<a href="#">The core of monomial ideals</a>	1463
LOUIZA FOULI, JONATHAN MONTAÑO, CLAUDIA POLINI and BERND ULRICH	
<a href="#">Pullback formulas for arithmetic cycles on orthogonal Shimura varieties</a>	1495
BENJAMIN HOWARD	
<a href="#">Weyl sums with multiplicative coefficients and joint equidistribution</a>	1549
MATTEO BORDIGNON, CYNTHIA BORTOLOTTI and BRYCE KERR	
<a href="#">Rational points of rigid-analytic sets: a Pila–Wilkie-type theorem</a>	1581
GAL BINYAMINI and FUMIHARU KATO	
<a href="#">Extending the unconditional support in an Iwaniec–Luo–Sarnak family</a>	1621
LUCILE DEVIN, DANIEL FIORILLI and ANDERS SÖDERGREN	
<a href="#">On the maximum gonality of a curve over a finite field</a>	1637
XANDER FABER, JON GRANTHAM and EVERETT W. HOWE	
<a href="#">Solvable and nonsolvable finite groups of the same order type</a>	1663
PAWEŁ PIWEK	