TWELFTH MOMENT OF DIRICHLET L-FUNCTIONS TO PRIME POWER MODULI

DJORDJE MILIĆEVIĆ AND DANIEL WHITE

Abstract. We prove the q-aspect analogue of Heath-Brown's result on the twelfth power moment of the Riemann zeta function for Dirichlet L-functions to odd prime power moduli. Our results rely on the p-adic method of stationary phase for sums of products and complement Nunes' bound for smooth square-free moduli.

1. Introduction

Analytic behavior of L-functions inside the critical strip encodes essential arithmetic information, and statistical information about their zeros, moments, and rate of growth along the critical line is of central importance in analytic number theory. The classical Weyl bound shows that the Riemann zeta function satisfies

$$\zeta\left(\tfrac{1}{2}+it\right) \ll_\varepsilon (1+|t|)^{1/6+\varepsilon} \tag{1}$$

where $\varepsilon > 0$ is an arbitrarily small constant that may change from one instance to another throughout this article. The widely believed Lindelöf hypothesis asserts that $\frac{1}{6}$ can be removed from the exponent above. The most recent progress in this direction is due to Bourgain [2], reducing the exponent to $\frac{13}{84}+\varepsilon$. One avenue to understanding the behavior of the Riemann zeta function along the critical line is through power moments, for which asymptotic formulas are only available up to the fourth moment [8, 12]. Higher moments provide tighter control on large values, and in this direction Heath-Brown [7] proved that, for $T \geqslant 1$,

$$\int_T^{2T} \left|\zeta\left(\tfrac{1}{2}+it\right)\right|^{12} \mathrm{d}t \ll_\varepsilon T^{2+\varepsilon}. \tag{2}$$

This is a very elegant bound as it recovers (1) as a rather immediate consequence. However, (2) is quite a bit stronger in that it immediately implies that $\zeta\left(\frac{1}{2}+it\right)$ *cannot sustain* large values; namely that

$$\left|\left\{t \in [T,2T] : \left|\zeta\left(\tfrac{1}{2}+it\right)\right| > V\right\}\right| \ll_\varepsilon T^{2+\varepsilon}V^{-12}. \tag{3}$$

Actually, (2) and (3) are equivalent, as is easily established via integration by parts.

Questions regarding the asymptotic behavior of $\zeta(\frac{1}{2}+it)$ as $t \to \infty$ have q-aspect analogues concerning the central values of Dirichlet L-functions $L(\frac{1}{2},\chi)$, where χ is a primitive character modulo q and $q \to \infty$. For an account of some of the current literature on $L(\frac{1}{2},\chi)$ and L-functions in the t-aspect, we direct the reader to the introduction of [13]. The q-analogue of (1), the bound $L(\frac{1}{2},\chi) \ll_\varepsilon q^{1/6+\varepsilon}$, long out of reach for generic q except for real characters to odd square-free moduli [3], has been recently announced by Petrow–Young [14]. For certain families of Dirichlet L-functions, however, even small improvements are known on $q^{1/6}$; see [11] for a "sub-Weyl" bound $L(\frac{1}{2},\chi) \ll q^{1/6-\delta}$ for prime power moduli and [9] and [17] for smooth square-free moduli.

While Dirichlet L-functions $L(\sigma+it,\chi)$ are also fruitfully used with a fixed modulus q and large $|t|$ to study arithmetic phenomena modulo q, from an adelic point of view it is more natural to

2010 *Mathematics Subject Classification.* Primary 11M06, 11L07; Secondary 11L40, 26E30.

Key words and phrases. L-functions, moments, p-adic analysis, depth aspect, exponential sums, method of stationary phase.

D.M. was supported by the National Science Foundation, Grants DMS-1503629 and DMS-1903301.

consider the dependence on a large conductor q as a measurement of increasing ramification, this time at finite places, and in particular, as a pure parallel to the t-aspect, at a fixed finite place. This explains why many tools of classical "archimedean" analytic number theory have found natural p-adic analogues. The extent of this parallel is yet to be fully understood, and our aim is to explore its manifestation for high moments of L-functions. Our main theorem is a q-aspect analogue of (2) for Dirichlet L-functions to odd prime power moduli.

Theorem 1. *There exists a constant $A > 0$ such that, for every odd prime p and every $q = p^n$,*

$$\sum_{\chi \pmod q} \left|L\left(\tfrac{1}{2}, \chi\right)\right|^{12} \ll_\varepsilon p^A q^{2+\varepsilon}.$$

We remark that Theorem 1 complements the result of Nunes [13] where q is taken to be smooth and square-free. The structure of the proof of Theorem 1 and the main result of Nunes translate the approach taken by Heath-Brown [7] into the context of factorable and prime power moduli. For a detailed comparison between Heath-Brown's and Nunes' work, we direct the reader to the introduction of [13]. Despite the similarities, the methods of evaluation and estimation of exponential sums found throughout are quite different in the present paper. In particular, we make extensive use of a method known as p-adic stationary phase, which we will encapsulate in Lemmata 3 and 4.

As in [7, 13], the moment estimate in Theorem 1 is a consequence of the following statement, which is reminiscent of (3) and its relationship to (2). We will establish the following.

Theorem 2. *For $V > 0$, define*

$$R(V; q) := \left\{\chi \text{ primitive of modulus } q : \left|L\left(\tfrac{1}{2}, \chi\right)\right| > V\right\}.$$

Then there exists a constant $A > 0$ such that, for every odd prime p and every $q = p^n$,

$$|R(V; q)| \ll_\varepsilon p^A q^{2+\varepsilon} V^{-12}.$$

Note that Theorem 1 follows immediately from Theorem 2 via summation by parts. From the available sharp estimates on the fourth moment of Dirichlet L-functions [6, 16], it follows that $|R(V; q)| \ll_\varepsilon q^{1+\varepsilon} V^{-4}$; see section 6. Combining this and the Weyl bound for this particular class of Dirichlet L-functions [15, 11], the range of interest in Theorem 2 is $q^{1/8-\varepsilon} \leqslant V \leqslant q^{1/6+\varepsilon}$.

The p-adic methods of this paper are very flexible. In particular, an analogue of [13, Theorem 1.2], which would sharpen Theorem 2 in the range $q^{3/20+\varepsilon} \leqslant V \leqslant q^{1/6-\varepsilon}$ (but not Theorem 1) can likely be proved with a further application of the p-adic stationary phase method to complete exponential sums with substantially more involved phases than in (6). It would also be of interest to investigate whether the methods of the present paper and [13] can be unified to provide a twelfth moment bound for characters to moduli q with finitely many well-located factors as in [5] (or a hybrid moment including the archimedean average); without imposing overly onerous factorization conditions, though, this may require delicate estimates on complete sums with degenerate critical points as in [5, Lemma 7].

Overview: For the benefit of the reader, we present a conceptual overview of the proof, ignoring non-generic cases, coprimality conditions, q^ε factors, and so on; in particular, we use $f \preccurlyeq g$ to denote $|f| \ll_{p,\varepsilon} q^\varepsilon g$ and $f \sim g$ for $f \preccurlyeq g \preccurlyeq f$. We fix a divisor $q_1 \mid q$, and consider the short second moment

$$S_2(\chi) := \sum_{\psi_1 \pmod{q_1}} \left|L\left(\tfrac{1}{2}, \chi\psi_1\right)\right|^2. \tag{4}$$

We will later choose roughly $q_1 \sim V^2$, so that the expected sharp bound $S_2(\chi) \preccurlyeq q_1$ essentially matches the contribution of a single summand $|L(\frac{1}{2}, \chi)| \sim V$.

Using the approximate functional equation and executing the ψ_1-average leads to weighted dyadic sums over $n \sim N \preccurlyeq q^{1/2}$ of terms of the form $\chi(n + hq_1)\overline{\chi}(n)$, which are $Q_1 = (q/q_1)$-periodic. We apply Poisson summation, incurring the dual variable $j \preccurlyeq Q_1/N$ and the "trace function"

$K_\chi(j,h;Q_1)$, which is shown in (19) and generically depends on $jh \preccurlyeq q/q_1^2$. The upshot of this analysis is Proposition 1, which bounds $S_2(\chi)$ roughly by

$$q_1\bigg(1+Q_1^{-1/2}\sideset{}{^*}\sum_{|m|\preccurlyeq q/q_1^2} K_\chi(m;Q_1)A(m)\bigg), \tag{5}$$

with somewhat messy arithmetic coefficients $A(m) \preccurlyeq 1$.

In Lemma 6, we show that the complete exponential sum $K_\chi(m;Q_1)$ exhibits square-root cancellation. This alone yields the upper bound $S_2(\chi) \preccurlyeq q_1 + (q/q_1)^{1/2}$, which is sharp for $q_1 \succcurlyeq q^{1/3}$ and recovers the Weyl subconvexity bound $L(\frac{1}{2},\chi) \preccurlyeq q^{1/6}$ (essentially by Weyl differencing followed by completion, as in [11]).

For purposes of Theorems 1 and 2, we must consider values $q^{1/4} \preccurlyeq q_1 \preccurlyeq q^{1/3}$, in which case the weighted sum of trace functions in (5) is of length $Q_1^{1/2} \preccurlyeq q/q_1^2 \preccurlyeq Q_1^{2/3}$. Weights $A(m)$ make it difficult to directly estimate the sum. Instead, the key idea is sort of a *large sieve*: we argue that (roughly speaking, and as q_1 gets smaller) the vectors $(K_\chi(m;Q_1))_m$ are typically approximately orthogonal for different χ, and thus it is hard for too many of them to avoid cancellation with a single vector $(A(m))_m$. The approximate orthogonality boils down to cancellations in *incomplete sums of products*; since the length is over the square-root of the conductor, we apply the method of completion, incurring an additive twist. Proposition 2, our key arithmetic input, shows square-root cancellation in sums of products of rough form

$$\sideset{}{^*}\sum_{u \pmod Q} K_\chi^\pm(u;Q_1)\overline{K_{\chi'}^\pm(u;Q_1)}e(-uv/Q) \preccurlyeq Q^{1/2}. \tag{6}$$

Here, the modulus $Q \mid Q_1$ drops with the conductor of $\chi\overline{\chi'}$ (essentially the distance between χ and χ' in the dual topology), and we must first separate K_χ into two oscillatory components $K_\chi^\pm$ (as often happens with Bessel functions; see also [1, §9]). Lemma 6 and Proposition 2 form the heart of the paper and are proved by a consistent application of the *p-adic method of stationary phase* to exponential sums with p-adically analytic phases, including characters to prime power moduli; see section 2.

Proceeding with the large sieve idea, we estimate the the sum of $S_2(\chi\psi)$ in (5) over an arbitrary set Ψ of characters ψ modulo some $q_2 \mid q$ (with $q_1 \mid q_2$) by applying the Cauchy–Schwarz inequality to the m-sum and bounding sums of products of $K_{\chi\psi}^\pm(m;Q_1)$ using (6). This shows in Proposition 3 that

$$\sum_{\psi\in\Psi} S_2(\chi\psi) \preccurlyeq \Big((q_1 + q_1^{1/4}q_2^{1/4})|\Psi| + q^{1/2}|\Psi|^{1/2}\Big). \tag{7}$$

The bound (7) imposes a restriction on the size $|\Psi|$ as long as each $S_2(\chi\psi)$ is slightly bigger than $q_1 + q_1^{1/4}q_2^{1/4}$. In section 6, we first fix χ and choose Ψ to be the set of characters modulo q_2 for which one of $|L(\frac{1}{2},\chi\psi\psi_1)|$ in (4) exceeds V, with $q_1 = q^{-\varepsilon}V^2$ and $q_2 = q_1^3$, obtaining $|\Psi| \preccurlyeq qV^{-4}$. From here it is a matter of bookkeeping to Theorem 2 and hence Theorem 1.

Notation: Throughout the paper, $\varepsilon > 0$ indicates a fixed positive number, which may be different from line to line but may at any point be taken to be as small as desired. As usual, $f \ll g$ and $f = O(g)$ indicate that $|f| \leqslant Cg$ for some effective constant $C > 0$, which may be different from line to line but does not depend on any parameters except as follows. In this introduction, all implied constants in $\ll$ and O are absolute, except that they may depend on $\varepsilon > 0$ if so indicated as in $\ll_\varepsilon$. In the rest of the paper, we allow the implied constants (but suppress this from notation) to depend on both the odd prime p and $\varepsilon > 0$. All dependencies on p are easily seen to be polynomial, leading to the statements of Theorems 1 and 2; we do not make an effort to optimize the value of $A > 0$.

We denote the cardinality of a finite set S by $|S|$; we use the same notation for the Lebesgue measure, with the meaning clear from the context. As is customary in analytic number theory, we also write $e(z) = e^{2\pi iz}$.

Acknowledgements: The authors would like to thank an anonymous referee for their careful reading and constructive suggestions, which helped us improve the paper in several places.

2. Preliminaries

2.1. **Approximate functional equation.** A ubiquitous tool in the analysis of L-functions inside the critical strip is the approximate functional equation (see [10, §5.2]). This equation has various manifestations depending on context and purpose. A typical form of this equation in the context of bounding central values states that one may recover the size of $L(\frac{1}{2}, \chi)$ by inserting $s = \frac{1}{2}$ into the associated Dirichlet series which is essentially truncated at $q^{1/2}$ via a suitable smooth weight function. For our purposes, the following lemma is convenient, which follows by applying a dyadic partition of unity to [10, Theorem 5.3].

Lemma 1. *Let χ be a primitive Dirichlet character modulo q. Then,*

$$\left|L\left(\tfrac{1}{2}, \chi\right)\right|^2 \ll \log q \sum_{\substack{N \leqslant q^{1/2+\varepsilon} \\ N \text{ dyadic}}} \left| \frac{1}{\sqrt{N}} \sum_n \chi(n) V_N(n) \right|^2 + q^{-100},$$

where V_N is a smooth function depending only on N and q, whose support is contained in $[N/2, 2N]$ and whose derivatives satisfy $V_N^{(j)} \ll_j N^{-j}$ for every $j \in \mathbb{N}$.

2.2. **p-adically analytic phases.** Among the key features of our treatment of exponential sums will be: *(i)* the consistent interpretation of oscillating terms (such as characters) as exponentials with phases that are p-adically analytic functions and *(ii)* the analysis thereof. For a rigorous treatment of these concepts, we refer to [11, §2]. Recall that a p-adically analytic function f on a domain $D \subseteq \mathbb{Z}_p$ is locally expressible, around each point $a \in D$, in a p-adic ball of the form $\{x \in \mathbb{Z}_p : |x - a|_p \leqslant p^{-\varrho}\} \subseteq D$ ($\varrho \in \mathbb{Z}_{\geqslant 0}$) as the sum of its p-adically convergent Taylor power series. We let $r_p(f; a)$ denote the largest such $p^{-\varrho}$ (which is not quite the same as the p-adic radius of convergence) and $r_p(f) = \inf_{a \in D} r_p(f; a) \geqslant 0$; in all phases we will encounter, $r_p(f) \geqslant p^{-1}$ will hold. It is not hard to see that $r_p(f'; a) \geqslant r_p(f; a)$.

We will make extensive use of the p-adic logarithm, which for simplicity we define on $1 + p\mathbb{Z}_p$. Recall that, throughout the paper, p is an odd prime.

Definition 1. *The p-adic logarithm, $\log_p : 1 + p\mathbb{Z}_p \to p\mathbb{Z}_p$ is the analytic function given as*

$$\log_p(1 + x) := \sum_{k \geqslant 1} (-1)^{k-1} \frac{x^k}{k}.$$

Access to the above is critical due to the following lemma, with roots in Postnikov [15] and which we quote from [11, Lemma 13].

Lemma 2. *Let χ be a primitive character modulo p^n. Then there exists a p-adic unit A such that, for every p-adic integer k,*

$$\chi(1 + kp) = e\left(\frac{A \log_p(1 + kp)}{p^n}\right). \tag{8}$$

Lemma 2 allows us to explicate the phase of any exponential of the form $\chi(1 + kp)e(f(k)/p^n)$ when χ is a character modulo p^n.

It will be necessary to handle solutions to quadratic equations over $\mathbb{Z}_p$, which requires the use of p-adic square roots. For p an odd prime and $x \in \mathbb{Z}_p^{\times 2}$, the congruence $u^2 \equiv x \pmod{p^\kappa}$ has exactly

two solutions modulo every p^κ, which reside within two p-adic towers and limit to the solutions of $u^2 = x$ as $\kappa \to \infty$. We denote these solutions $\pm x_{1/2}$. For $(\,\cdot\,)_{1/2} : \mathbb{Z}_p^{\times 2} \to \mathbb{Z}_p^\times$ to be well-defined, a choice of square root for each $y \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}$ must be made. This set of choices propagates to $\mathbb{Z}_p^{\times 2}$ and represents one of the $2^{(p-1)/2}$ branches of the p-adic square root. A thorough treatment of p-adic square roots can be found in [1, §2]; we content ourselves with summarizing two properties of import to us.

Each branch $x_{1/2}$ of the square root is an analytic function expressible by a convergent power series in balls of radius $r_p \geqslant p^{-1}$. Specifically, on $1 + p\mathbb{Z}_p$, the binomial expansion

$$(1 + xp)^{1/2} = \sum_{k \geqslant 0} \binom{1/2}{k} (xp)^k \tag{9}$$

gives the branch with values in $1 + p\mathbb{Z}_p$ (as seen by formally squaring the right-hand side), which is in fact an automorphism of $1 + p\mathbb{Z}_p$. For an arbitrary $u \in \mathbb{Z}_p^{\times 2}$, a simple argument modulo p shows that

$$(u + xp)_{1/2} = u_{1/2}(1 + x\overline{u}p)^{1/2} \tag{10}$$

where $\overline{u}$ denotes the p-adic inverse of u. While $(\,\cdot\,)_{1/2}$ cannot in general be expected to be multiplicative, (10) gives it both a pseudo-morphism rule and a power expansion. Moving forward, we fix a branch to be used throughout, drop the $(\,\cdot\,)_{1/2}$ notation and simply write $(\,\cdot\,)^{1/2}$ or use a radical symbol for our chosen branch, using caution to only use (9), (10), and $\sqrt{m}^2 = m$ when exercising the usual archimedean exponent rules. For future reference, we note that, for all $u, u' \in \mathbb{Z}_p^{\times 2}$,

$$\operatorname{ord}_p(\sqrt{u} - \sqrt{u'}) = \operatorname{ord}_p(u - u'). \tag{11}$$

2.3. **p-adic method of stationary phase.** The following pair of lemmata establishes what is known as the p-adic method of stationary phase (see, for example, [11, §4], [1, §7]), allowing one to evaluate complete sums involving such exponentials. They are the proper p-adic analogues of the classical method of stationary phase for exponential integrals of the form $\int_{\mathbb{R}} g(x)e(f(x))\,\mathrm{d}x$ with a suitable smooth phase f and weight g, which generically proceeds in two principal steps: *(i)* showing that ranges where $|f'|$ is not suitably small are negligible, and *(ii)* close to each non-degenerate stationary point x_0 of the phase f, approximating f quadratically, with resulting Gaussian-type integrals evaluating to about $g(x_0)e(f(x_0))/\sqrt{|f''(x_0)|}$ (see [4]).

Lemma 3. *Let p be an odd prime, $1 \leqslant \ell \leqslant n$ be integers, and $f : \mathbb{Z}_p^\times \to \mathbb{Z}_p$ be an analytic function invariant modulo p^n under translation by $p^n\mathbb{Z}_p$. If $r_p(f) \geqslant p^{-\ell}$ and $p^{k\ell} f^{(k)}(x)/k! \equiv 0 \pmod{p^n}$ for all $x \in \mathbb{Z}_p^\times$ when $k \geqslant 2$, then*

$$\sideset{}{^*}\sum_{x \pmod{p^n}} e\left(\frac{f(x)}{p^n}\right) = \sideset{}{^*}\sum_{\substack{x_0 \pmod{p^n} \\ f'(x_0) \equiv 0 \pmod{p^{n-\ell}}}} e\left(\frac{f(x_0)}{p^n}\right).$$

Proof. Expanding $f(x)$ around x_0 gives $f(x_0 + tp^\ell) = \sum_{k \geq 0} f^{(k)}(x_0)(tp^\ell)^k/k!$. With this, observe

$$\sideset{}{^*}\sum_{x \pmod{p^n}} e\left(\frac{f(x)}{p^n}\right) = \frac{1}{p^{n-\ell}} \sideset{}{^*}\sum_{x_0 \pmod{p^n}} \sum_{t \pmod{p^{n-\ell}}} e\left(\frac{f(x_0) + f'(x_0)tp^\ell}{p^n}\right)$$

where the inner sum contributes $p^{n-\ell}e(f(x_0)/p^n)$ when $f'(x_0) \equiv 0 \pmod{p^{n-\ell}}$ and vanishes otherwise. □

Lemma 3 reduces a complete exponential sum to p-adic neighborhoods in which $|f'(x)|_p$ is small. The following lemma is a further refined statement that explicitly evaluates these localized sums and is suited for exponential sums that we will encounter in the proof of Lemma 6.

Lemma 4. *Let p be an odd prime, $n \geqslant 2$, and $f : \mathbb{Z}_p^\times \to \mathbb{Z}_p$ be an analytic function satisfying the hypotheses in Lemma 3 for $\ell = \lceil n/2 \rceil$. Let $X \subseteq (\mathbb{Z}/p^n\mathbb{Z})^\times$ denote the solution set of $f'(x_0) \equiv 0 \pmod{p^{\lfloor n/2 \rfloor}}$, and assume that, for all $x_0 \in X$, $r_p(f; x_0) \geqslant p^{-\lfloor n/2 \rfloor}$, $f''(x_0) \in \mathbb{Z}_p$, and $p^{\lfloor n/2 \rfloor k} f^{(k)}(x_0)/k! \equiv 0 \pmod{p^n}$ for $k \geqslant 3$. Then, X is invariant under translation by $p^{\lfloor n/2 \rfloor}\mathbb{Z}$, and, for an arbitrary set of representatives $\tilde{X}$ for $X/p^{\lfloor n/2 \rfloor}\mathbb{Z}$,*

$$\sideset{}{^*}\sum_{x \pmod{p^n}} e\left(\frac{f(x)}{p^n}\right) = p^{n/2} \sum_{x_0 \in \tilde{X}} e\left(\frac{f(x_0)}{p^n}\right) \Delta_f(x_0; p^n),$$

where all summands are independent of the choice of $\tilde{X}$, and, writing $f'(x_0)_\circ := f'(x_0)/p^{\lfloor n/2 \rfloor}$ and $\left(\frac{\cdot}{p}\right)$ for the Legendre symbol,

$$\Delta_f(x_0; p^n) = \begin{cases} 1, & 2 \mid n; \\ \epsilon(p)\left(\frac{2f''(x_0)}{p}\right) e\left(\frac{-\overline{2f''(x_0)} f'(x_0)_\circ^2}{p}\right), & 2 \nmid n, p \nmid f''(x_0); \\ \sqrt{p}\mathbf{1}_{p \mid f'(x_0)_\circ}, & 2 \nmid n, p \mid f''(x_0), \end{cases} \quad \epsilon(p) = \begin{cases} 1, & p \equiv 1 \pmod 4; \\ i, & p \equiv 3 \pmod 4. \end{cases}$$

Proof. The translational invariance of X modulo $p^{\lfloor n/2 \rfloor}\mathbb{Z}$ is clear from our hypotheses and the expansion of $f'(x_0 + tp^{\lfloor n/2 \rfloor})$ at each $x_0 \in X$. Application of Lemma 3 with $\ell = \lceil n/2 \rceil$ together with an expansion of f around each $x_0 \in \tilde{X}$ gives

$$\begin{aligned} \sideset{}{^*}\sum_{x \pmod{p^n}} e\left(\frac{f(x)}{p^n}\right) &= \sum_{x_0 \in \tilde{X}} \sum_{t \pmod{p^{\lceil n/2 \rceil}}} e\left(\frac{f(x_0 + tp^{\lfloor n/2 \rfloor})}{p^n}\right) \\ &= p^{\lfloor n/2 \rfloor} \sum_{x_0 \in \tilde{X}} e\left(\frac{f(x_0)}{p^n}\right) \sum_{t \pmod{p^{n - 2\lfloor n/2 \rfloor}}} e\left(\frac{f'(x_0)_\circ t + \bar{2} f''(x_0) t^2}{p^{n - 2\lfloor n/2 \rfloor}}\right). \end{aligned}$$

For n even, the inner sum is trivial and the desired result follows. If n is odd, the contribution from $p \mid f''(x_0)$ is clear, while, for $p \nmid f''(x_0)$, completing the square yields for the inner sum

$$e\left(\frac{-\overline{2f''(x_0)} f'(x_0)_\circ^2}{p}\right) \sum_{t \pmod p} e\left(\frac{\bar{2} f''(x_0) t^2}{p}\right) = \epsilon(p)\sqrt{p}\left(\frac{\bar{2} f''(x_0)}{p}\right) e\left(\frac{-\overline{2f''(x_0)} f'(x_0)_\circ^2}{p}\right),$$

by the classical evaluation of the quadratic Gauss sum. This finishes the proof. □

Remark 1. *The general (if somewhat cumbersome) conditions in Lemma 4 are easily satisfied, say, for every analytic function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ with $r_p(f) \geqslant 1/p$ and $f^{(j)}(\mathbb{Z}_p) \subseteq \mathbb{Z}_p$ for all $j \geqslant 0$. The same is true for Lemma 3 with $\ell \geqslant n/2$.*

In Lemma 4, in the odd nonsingular case $2 \nmid n$, $p \nmid f''(x_0)$, we see that $f'(x_0 + tp^{\lfloor n/2 \rfloor}) \equiv 0 \pmod{p^{\lceil n/2 \rceil}}$ for exactly one $t \pmod p$; picking such a representative $\tilde{x}_0 := x_0 + tp^{\lfloor n/2 \rfloor} \in \tilde{X}$, we have more simply $\Delta_f(\tilde{x}_0; p^n) = \epsilon(p)\left(\frac{2f''(\tilde{x}_0)}{p}\right)$.

Remark 2. *Versions of Lemmata 3 and 4 exist for sums over other subsets of residue classes $x \pmod{p^n}$, where the phase f may have as domain a finite union of translates of $p^\lambda\mathbb{Z}_p$, with $\lambda \leqslant \ell$ in Lemma 3 and $\lambda \leqslant n/2$ in Lemma 4. The proofs of these parallel statements are the same; indeed, they only require that the sum be over a set of residues invariant under translation by a suitable $p^\ell\mathbb{Z}_p$ with $\ell \geqslant \lambda$ and $r_p(f) \geqslant p^{-\ell}$. Specifically, the proof of Proposition 2 will require Lemma 3 to be applied over quadratic residues and non-residues modulo p^n. Lemmata 3 and 4 also hold for sums of the form $\sum g(x)e(f(x)/p^n)$ where g is invariant under translation by $p^\ell\mathbb{Z}_p$.*

In practice, we will apply Lemmata 3 and 4 in situations where explicitly writing the exponent of $q = p^n$ gets notationally cumbersome. To represent what are essentially square roots in these cases, we define

$$\mathrm{rt}_*(p^n) := p^{\lfloor n/2 \rfloor} \quad \text{and} \quad \mathrm{rt}^*(p^n) := p^{\lceil n/2 \rceil}.$$

2.4. **Completion.** While Lemmata 3 and 4 provide powerful tools for evaluating the types of complete exponential sums that will be found throughout, we will eventually encounter those which are incomplete. In anticipation of this, we introduce the next lemma which prepackages a technique known as completion.

Lemma 5. *Suppose f is an arithmetic function with period Q. Then*

$$\sum_{m\leqslant M} f(m) \ll \frac{1}{Q}\sum_{v \pmod Q} \left|\widehat{f}(v)\right| \cdot \min\left\{M, \|v/Q\|^{-1}\right\}, \quad \widehat{f}(v) := \sum_{u \pmod Q} f(u)e\left(\frac{-uv}{Q}\right),$$

where $\|x\|$ is the distance from x to the nearest integer.

Proof. Splitting the sum into residue classes modulo Q yields

$$\sum_{m\leqslant M} f(m) = \sum_{u \pmod Q} f(u) \sum_{m\leqslant M} \frac{1}{Q}\sum_{v \pmod Q} e\left(\frac{(m-u)v}{Q}\right) = \frac{1}{Q}\sum_{v \pmod Q} \widehat{f}(v)\sum_{m\leqslant M} e\left(\frac{mv}{Q}\right).$$

The bound

$$\sum_{m\leqslant M} e\left(\frac{mv}{Q}\right) \ll \min\{M, \|v/Q\|^{-1}\}$$

on the sum of a geometric sequence completes the proof. □

3. Short second moment

As before and throughout, p will be an odd prime and q some prime power p^n for n a positive integer. Further consider

$$p \leqslant q_1 \leqslant q_2 < q, \tag{12}$$

where the q_i are also powers of p. A central object to our proofs, as in [7, 13], is the short second moment. In the q-aspect, this will be a power moment which samples from a q_1-neighborhood around some fixed primitive character $\chi \pmod q$. This analogy is particularly natural from a p-adic point of view, as the (Pontrjagin) dual group of $\mathbb{Z}_p^*$ carries the natural dual topology, with respect to which these correspond to actual small neighborhoods of χ. We denote

$$S_2(\chi) := \sum_{\psi_1 \pmod{q_1}} \left|L\left(\tfrac{1}{2}, \chi\psi_1\right)\right|^2.$$

We will eventually analyze the size of short moments on average, but first must gather information on $S_2(\chi)$ itself.

3.1. **Executing the short second moment.** We immediately apply Lemma 1 to $S_2(\chi)$. This yields

$$\begin{aligned} S_2(\chi) &\ll q^{\varepsilon} \sum_{\psi_1 \pmod{q_1}} \sum_{\substack{N\leqslant q^{1/2+\varepsilon}\\ N \text{ dyadic}}} \left|\frac{1}{\sqrt{N}}\sum_n \chi\psi_1(n)V_N(n)\right|^2 + q^{-99} \\ &\ll \frac{q^{\varepsilon}}{N}\sum_{\psi_1 \pmod{q_1}} \left|\sum_n \chi\psi_1(n)V_N(n)\right|^2 + q^{-99} \end{aligned} \tag{13}$$

for some $N \leqslant q^{1/2+\varepsilon}$ by exchanging order of summation and choosing the summand which maximizes the inner sum. Denote the sum in (13) without the error term and q^{ε} factor as $B(N)$. Expansion and orthogonality of characters gives

$$B(N) \ll \frac{q_1}{N}\sum_{n\equiv n' \pmod{q_1}} \chi(n')\overline{\chi}(n)V_N(n')\overline{V_N(n)}.$$

We note the similarity of the resulting sum (the sum of squares of short p-adic averages, a reflection of the ψ_1-average via Parseval's identity) to those encountered with Weyl differencing in the context of factorable moduli (see, for example, [11, §5]), and we proceed similarly.

Recall that $V_N \ll 1$ with support contained in $[N/2, 2N]$. The diagonal terms corresponding to $n = n'$ contribute $O(q_1)$ to $B(N)$. The addition of this to the remaining pairs (n', n) gives

$$B(N) \ll q_1 + \frac{q_1}{N} \operatorname{Re} \sum_{h\geq 1} \sum_{n\geq 1} \chi(n+hq_1)\overline{\chi}(n) V_N(n+hq_1)\overline{V_N(n)}, \tag{14}$$

since each (n', n) appears above or can be accounted for by conjugation. Denote the inner sum in (14) as $S_{hq_1}(N; \chi)$. Since $\chi(n + hq_1)\overline{\chi}(n)$ is periodic modulo $Q_1 = q/q_1$, we may write

$$S_{hq_1}(N;\chi) = \sideset{}{^*}\sum_{r \pmod{Q_1}} \chi(r+hq_1)\overline{\chi}(r) \sum_j V_N(r+jQ_1+hq_1)\overline{V_N(r+jQ_1)}. \tag{15}$$

We will apply Poisson summation to the inner sum in S_{hq_1}. Examination of

$$\begin{aligned} &\int_{\mathbb{R}} V_N(r+xQ_1+hq_1)\overline{V_N(r+xQ_1)} e(-jx)\,\mathrm{d}x \\ &\qquad = Q_1^{-1} e(rj/Q_1) \int_{\mathbb{R}} V_N(y+hq_1)\overline{V_N(y)} e(-jy/Q_1)\,\mathrm{d}y \end{aligned} \tag{16}$$

shows that the Fourier transform in (16) is

$$Q_1^{-1} e\left(\frac{rj}{Q_1}\right) \widehat{W_{hq_1}}(j/Q_1) \quad \text{where} \quad W_{hq_1}(y) := V_N(y+hq_1)\overline{V_N(y)}. \tag{17}$$

Using (13) through (17) together with Poisson summation yields

$$S_2(\chi) \ll q^{\varepsilon}\left(q_1 + \frac{q_1}{N} \operatorname{Re} \sum_{h\geq 1} Q_1^{-1/2} \sum_j \widehat{W_{hq_1}}(j/Q_1) K_\chi(j,h;Q_1)\right), \tag{18}$$

where, for $\tilde{q}$ a proper divisor of q, we define

$$K_\chi(a,b;\tilde{q}) := \tilde{q}^{-1/2} \sideset{}{^*}\sum_{r \pmod{\tilde{q}}} \chi\big(r + b(q/\tilde{q})\big)\overline{\chi}(r) e(ar/\tilde{q}). \tag{19}$$

In particular, for $(m, \tilde{q}) = 1$, we also write $K_\chi(m; \tilde{q}) := K_\chi(1, m; \tilde{q}) = K_\chi(m, 1; \tilde{q})$, so that

$$K_\chi(m;\tilde{q}) = \tilde{q}^{-1/2} \sideset{}{^*}\sum_{r \pmod{\tilde{q}}} \chi\big(1 + (q/\tilde{q})r\big) e(m\bar{r}/\tilde{q}). \tag{20}$$

This sum (which takes on the role of trace functions from the context of square-free moduli [13]) is of central importance to our arguments. We summarize some of its important properties in Lemma 6 in section 4, below. In this section, we will only require the elementary reduction and vanishing claim (25).

By the support of V_N, we may actually take $h \ll N/q_1$ in (18). We will soon identify the range j that is essential to (18). Once this range becomes finite, we will configure our bound in a way that highlights the main object of our study.

3.2. **Establishing the bound on $S_2(\chi)$.** We first show that the contribution to (18) from $j = 0$ may be neglected. By Lemma 6 below,

$$K_\chi(0,h;Q_1) = \begin{cases} Q_1^{1/2}(1-p^{-1}), & Q_1 \mid h; \\ -Q_1^{1/2}/p, & Q_1/p \parallel h; \\ 0, & \text{otherwise.} \end{cases}$$

The contribution from $j=0$ to (18) is then

$$q^{\varepsilon}q_1Q_1^{-1/2}\operatorname{Re}\sum_{1\leqslant h\ll Nq_1^{-1}}N^{-1}\widehat{W_{hq_1}}(0)K_\chi(0,h;Q_1)\ll q^{\varepsilon}q_1\sum_{\substack{1\leqslant h\ll Nq_1^{-1}\\ Q_1\mid hp}}1\ll q^{\varepsilon}\frac{N}{Q_1}. \tag{21}$$

Repeated use of integration by parts shows

$$\widehat{W_{hq_1}}(y)\ll_m N\left(\frac{1}{Ny}\right)^m$$

for every positive integer m. From this bound, $h\ll N/q_1$, and the trivial bound on $K_\chi(j,h;Q_1)$, the contribution to (18) from $|j|>q^{\varepsilon}Q_1/N$ is $O(q^{-100})$. Using (18) and (21), we find

$$S_2(\chi)\ll q^{\varepsilon}\bigg(q_1+\frac{q_1}{Q_1^{1/2}}\operatorname{Re}\sum_{0<h\ll N/q_1}\sum_{0<|j|\ll q^{\varepsilon}Q_1/N}N^{-1}\widehat{W_{hq_1}}(j/Q_1)K_\chi(j,h;Q_1)\bigg). \tag{22}$$

According to Lemma 6, noting that $(Q_1^2/p)\nmid jh\ll q^{\varepsilon}Q_1/q_1$, we may rewrite the double sum above as

$$\begin{aligned}&\sum_{p^\eta\ll q^{1/2+\varepsilon}q_1^{-1}}\sideset{}{^*}\sum_{h'\ll N(q_1p^\eta)^{-1}}\sideset{}{^*}\sum_{0<|j'|<q^{\varepsilon}Q_1(Np^\eta)^{-1}}N^{-1}\widehat{W_{h'p^\eta q_1}}(j'p^\eta/Q_1)K_\chi(j'p^\eta,h'p^\eta;Q_1)\\ &\quad=\sum_{p^\eta\ll q^{1/2+\varepsilon}q_1^{-1}}p^{\eta/2}\sideset{}{^*}\sum_{|m|\ll q^{1+\varepsilon}(q_1^2p^{2\eta})^{-1}}K_\chi(m;Q_1/p^\eta)\sum_{\substack{h'|j'|=m\\ h'\ll N(q_1p^\eta)^{-1}\\ |j'|<q^{\varepsilon}Q_1(Np^\eta)^{-1}}}N^{-1}\widehat{W_{h'p^\eta q_1}}(j'p^\eta/Q_1).\end{aligned} \tag{23}$$

Denoting the inner sum of (23) as $A(m;p^\eta)$, the above becomes

$$\sum_{p^\eta\ll q^{1/2+\varepsilon}q_1^{-1}}p^{\eta/2}\sideset{}{^*}\sum_{|m|\ll q^{1+\varepsilon}(q_1^2p^{2\eta})^{-1}}K_\chi(m;Q_1/p^\eta)A(m;p^\eta), \tag{24}$$

where $A(m;p^\eta)\ll m^{\varepsilon}$ by the divisor bound. The key thing is that these noisy coefficients do not depend on χ, which will allow us to remove them via an application of the Cauchy–Schwarz inequality in section 5. Combining (22) through (24) we obtain Proposition 1.

Proposition 1. *Let q_1 and q be subject to the conditions in (12). Then there exist coefficients $A(m;p^\eta)\ll m^{\varepsilon}$ such that, for every primitive character $\chi \pmod q$,*

$$S_2(\chi)\ll q^{\varepsilon}q_1\bigg(1+Q_1^{-1/2}\operatorname{Re}\sum_{p^\eta\ll q^{1/2+\varepsilon}q_1^{-1}}p^{\eta/2}\sideset{}{^*}\sum_{|m|\ll q^{1+\varepsilon}(q_1^2p^{2\eta})^{-1}}K_\chi(m;Q_1/p^\eta)A(m;p^\eta)\bigg),$$

where $K_\chi(m;Q_1/p^\eta)$ are as in (19).

4. Exponential sum estimates

In this section, we evaluate and estimate complete exponential sums to prime power moduli. Our principal tools are the p-adic stationary phase method Lemmata 3 and 4. In Lemma 6, we consider the complete exponential sum $K_\chi(j,h;\tilde{q})$ introduced in (19) and show that it can be expressed in terms of explicit exponentials $K_\chi^{\pm}(m;\tilde{q})$ with p-adically analytic phases. Then, in Proposition 2, we show square-root cancellation in complete sums of products of $K_\chi^{\pm}(m;\tilde{q})$ including additive twists.

4.1. **Evaluation of $K_\chi(m;\tilde{q})$.** In the following lemma, we explicitly evaluate the complete exponential sum $K_\chi(j,h;\tilde{q})$.

Lemma 6. *Let $\tilde{q}$ be a proper divisor of q and, for every $j \in \mathbb{Z}$, let $p^{\eta_j} = (j,\tilde{q})$. Then, the sum $K_\chi(j,h;\tilde{q})$ defined in (19) satisfies*

$$K_\chi(j,h;\tilde{q}) = \begin{cases} p^{\eta/2}K_\chi(jh/p^{2\eta};\tilde{q}/p^\eta), & \eta = \eta_j = \eta_h,\ \tilde{q} \neq p^\eta; \\ \tilde{q}^{1/2}(1-p^{-1}), & \eta_j = \eta_h = \eta_{\tilde{q}}; \\ -\tilde{q}^{1/2}/p, & \eta_j + \eta_h = 2\eta_{\tilde{q}} - 1; \\ 0, & \textit{otherwise.} \end{cases} \tag{25}$$

Further, let A be an integer such that (8) holds for χ, and assume that $\tilde{q} \geqslant p^2$. Then, for $(m,\tilde{q}) = 1$,

$$K_\chi(m;\tilde{q}) = K_\chi^+(m;\tilde{q}) + K_\chi^-(m;\tilde{q}), \tag{26}$$

where

$$K_\chi^\pm(m;\tilde{q}) = \begin{cases} \Delta_\theta(s_\pm(m/A;\tilde{q});\tilde{q})e\left(Ag_\pm(m/A;\tilde{q})/\tilde{q}\right), & \left(\frac{Am}{p}\right) = 1; \\ 0, & \textit{otherwise,} \end{cases}$$

where, for $\left(\frac{m}{p}\right) = 1$,

$$\begin{aligned} g_\pm(m;\tilde{q}) &= (\tilde{q}/q)\log_p\left(1 + (q/\tilde{q})s_\pm(m;\tilde{q})\right) + m/s_\pm(m;\tilde{q}), \\ s_\pm(m;\tilde{q}) &= \tfrac{1}{2}\left(mq/\tilde{q} \pm \sqrt{(mq/\tilde{q})^2 + 4m}\right), \end{aligned} \tag{27}$$

θ is the phase associated to $K_\chi(m;\tilde{q})$ in (20), and Δ_θ is as described in Lemma 4.

Proof. We first establish (25). Write $h \equiv h'p^{\eta_h} \pmod{\tilde{q}}$ and $j \equiv j'p^{\eta_j} \pmod{\tilde{q}}$ where $p \nmid h'j'$, and set $\eta = \min\{\eta_j,\eta_h\}$. If $p^\eta \neq \tilde{q}$, then by the substitution $r \mapsto \overline{j'r}$ for the variable of summation in (19) and a reduction to a sum over residues modulo $\tilde{q}/p^\eta$ we have

$$K_\chi(j,h;\tilde{q}) = \tilde{q}^{-1/2}p^\eta \sideset{}{^*}\sum_{r \pmod{\tilde{q}/p^\eta}} \chi\left(1 + \frac{q}{\tilde{q}/p^\eta}p^{\eta_h-\eta}rj'h'\right)e\left(\frac{p^{\eta_j-\eta}\overline{r}}{\tilde{q}/p^\eta}\right). \tag{28}$$

In particular, this proves the first case of (25). The second case, when $p^\eta = \tilde{q}$, follows from a trivial evaluation of the definition (19).

We now assume $\eta_j \neq \eta_h$. For $\eta_j + \eta_h = 2\eta_{\tilde{q}} - 1$, the situation quickly boils down, directly or with an application of (8), to

$$K_\chi(j,h;\tilde{q}) = \tilde{q}^{-1/2}(\tilde{q}/p) \sideset{}{^*}\sum_{r \pmod{p}} e(r/p) = -\tilde{q}^{1/2}/p.$$

In any other event, let ϕ be the phase associated to (28) where

$$\phi^{(k)}(x) = (-1)^{k-1}(k-1)!\left(A\left(\frac{p^{\eta_h-\eta}j'h'}{1 + xj'hq/\tilde{q}}\right)^k\left(\frac{q}{\tilde{q}/p^\eta}\right)^{k-1} - kp^{\eta_j-\eta}x^{-(k+1)}\right) \tag{29}$$

for $k \geqslant 1$ and $x \in \mathbb{Z}_p^\times$ by (8). From (29), it is easy to see that $\phi^{(k)}(x)/(k-1)! \in \mathbb{Z}_p$ for $x \in \mathbb{Z}_p^\times$. Moreover

$$(\mathrm{rt}^*(\tilde{q}/p^\eta))^k/k \equiv 0 \pmod{\tilde{q}/p^\eta}$$

for all $k \geqslant 2$, so that $(\mathrm{rt}^*(\tilde{q}/p^\eta))^k\phi^{(k)}(x)/k! \equiv 0 \pmod{\tilde{q}/p^\eta}$ for all $x \in \mathbb{Z}_p^\times$ and all $k \geqslant 2$. Thus ϕ satisfies the hypotheses of Lemma 3 with $p^\ell = \mathrm{rt}^*(\tilde{q}/p^\eta)$. Since in this case $\mathrm{rt}_*(\tilde{q}/p^\eta) \geqslant p$ and exactly one of η_h and η_j equals η, we find that $K_\chi(j,h;\tilde{q})$ must vanish since no solutions to $\phi'(x) \equiv 0 \pmod{p}$ exist in $(\mathbb{Z}/p\mathbb{Z})^\times$. This completes the proof of (25).

Next, for A, $(m,\tilde{q})=1$, and $\tilde{q}\geqslant p^2$ as stated, the phase θ associated to $K_\chi(m;\tilde{q})$ in (20) agrees with the phase ϕ in (28) and (29) with $h=1$, $j=j'=m$, and $\eta_j=\eta_h=\eta=0$ (substituting $r\mapsto\overline{m}r$); in particular,

$$\theta'(x)=\frac{A}{1+xq/\tilde{q}}-\frac{m}{x^2}\quad\text{and}\quad\theta''(x)=-\frac{Aq/\tilde{q}}{(1+xq/\tilde{q})^2}+\frac{2m}{x^3}.$$

We will use Lemma 4. If $\left(\frac{Am}{p}\right)=-1$, there are no solutions to $\theta'(x_0)\equiv 0 \pmod{\mathrm{rt}_*(\tilde{q})}$ by an obstruction modulo p, so that $K_\chi(m;\tilde{q})=0$ in this case. Otherwise, solving the equation $\theta'(x_0)=0$ yields $x_0=s_\pm(m/A;\tilde{q})$. Upon noting that $\theta''(x_0)\equiv 2mx_0^{-3}\not\equiv 0 \pmod p$, an application of Hensel's lemma gives exactly two unique solutions to the congruence above, proving (26). □

4.2. **Sums of products.** As we input Proposition 1 into estimating short second moments in aggregate over sets of characters, we will incur incomplete sums of products of trace functions $K_\chi(m;\tilde{q})$ evaluated in Lemma 6, with two different characters χ. Specifically, the inner sum in (32) will be estimated using the method of completion, Lemma 5. In preparation for this, in this section we prove the following proposition.

Proposition 2. *Let $\tilde{q}\geqslant p^2$ be a proper divisor of q and $K_\chi(m;\tilde{q})$ be as in (20). Further, let χ and χ' be two primitive Dirichlet characters modulo q with associated units A and A' as in (8). Denote $\delta_q(\chi,\chi')=(q/p,A-A')$ and $Q=\tilde{q}/(\tilde{q},\delta_q(\chi,\chi'))$. Then:*

(a) for $Q\geqslant p$, the expression $K_\chi^\pm(m;\tilde{q})\overline{K_{\chi'}^\pm(m;\tilde{q})}$ is Q-periodic and satisfies, for every $v\in\mathbb{Z}$,

$$\sideset{}{^*}\sum_{m \pmod Q} K_\chi^\pm(m;\tilde{q})\overline{K_{\chi'}^\pm(m;\tilde{q})}e\left(\frac{-mv}{Q}\right)\ll Q^{1/2};\tag{30}$$

(b) for $Q\geqslant p^2$, the left-hand side of (30) vanishes unless $|v|_p=1$;

(c) for $Q=1$, $K_\chi^\pm(m;\tilde{q})\overline{K_{\chi'}^\pm(m;\tilde{q})}=\mathbf{1}_{(Am/p)=1}$.

Proof. Evaluation (26) expresses $K_\chi^\pm(m;\tilde{q})$ in terms of exponentials with p-adically analytic phases. Thus, as in sections 2.2–2.3 and the proof of Lemma 6, we continue to treat the phases in complete exponential sums such as (30) as p-adically analytic functions on their respective domains. Since p-adic differentiation and power series will be involved, for the duration of this proof, we will use notation $K_\chi^\pm(u;\tilde{q})$ so as to avoid any visual suggestion that the arguments of these phases may only be rational integers.

By Lemma 6, the sum on the left-hand side of (30) vanishes unless $AA'\in\mathbb{Z}_p^{\times 2}$; we assume this henceforth and restrict the sum (as we may) to primitive classes $u \pmod Q$ such that $(\frac{u/A}{p})=1$. Further, let θ_χ and $\theta_{\chi'}$ be phases associated to $K_\chi(u;\tilde{q})$ and $K_{\chi'}(u;\tilde{q})$ as in (20), respectively. Then, by Lemma 6, we have for $(\frac{u/A}{p})=1$

$$\begin{aligned}&K_\chi^\pm(u;\tilde{q})\overline{K_{\chi'}^\pm(u;\tilde{q})}\\&\quad=\Delta_{\theta_\chi}(s_\pm(u/A;\tilde{q});\tilde{q})\overline{\Delta_{\theta_{\chi'}}(s_\pm(u/A';\tilde{q});\tilde{q})}e\left(\frac{Ag_\pm(u/A;\tilde{q})-A'g_\pm(u/A';\tilde{q})}{(\tilde{q},\delta_q(\chi,\chi'))Q}\right)\end{aligned}$$

where, for fixed χ and χ', the product of the Δ factors depends only on the class of $u \pmod p$, as is readily verified using $\theta_\chi'(x_{0,A})=0$ and $\theta_\chi''(x_{0,A})\equiv 2ux_{0,A}^{-3} \pmod p$ with $x_{0,A}=s_\pm(u/A;\tilde{q})$ from the proof of Lemma 6. This proof also shows that $g_\pm(u;\tilde{q})$, a function analytic on its domain $\mathbb{Z}_p^{\times 2}$, is invariant modulo $\tilde{q}$ under translation by $\tilde{q}\mathbb{Z}_p$. Moreover, a moment's reflection on the definition (27) combined with (10) and (9) shows that for $u\in\mathbb{Z}_p^{\times 2}$ both $s_\pm(u;\tilde{q})$ and $g_\pm(u;\tilde{q})$ may be expanded into a convergent power series in $\sqrt{u}$ with coefficients in $\mathbb{Z}_p$. From this and (11) it follows that, for $u\in A\mathbb{Z}_p^{\times 2}$,

$$Ag_\pm(u/A;\tilde{q})-A'g_\pm(u/A';\tilde{q})=(\tilde{q},\delta_q(\chi,\chi'))\cdot\sigma(u)$$

is divisible by $(\tilde{q}, \delta_q(\chi,\chi'))$ and invariant modulo $\tilde{q}$ under translation by $Q\mathbb{Z}_p$ (for $Q \geqslant p$). This establishes the periodicity claim and (c) follows from the definition of Δ_θ, noting that $A \equiv A' \pmod p$ in this case.

As for the estimate (30), the case $Q = p$ is trivial since we are taking $p \ll 1$, so we assume that $Q \geqslant p^2$. We will be interested in applying Lemma 3 and Remark 2 with $p^n = Q$, phase σ, and $p^\ell = \mathrm{rt}^*(Q)$. Since $s_\pm(u/A;\tilde{q})$ solves $\theta'(x_0) = 0$ in the proof of Lemma 6, we observe

$$\frac{\mathrm{d}}{\mathrm{d}u} A g_\pm(u/A;\tilde{q}) = \left\{ \frac{\partial}{\partial u} + \frac{\partial}{\partial s_\pm} \cdot \frac{\mathrm{d}s_\pm(u/A;\tilde{q})}{\mathrm{d}u} \right\} A g_\pm(u/A;\tilde{q}) = \frac{1}{s_\pm(u/A;\tilde{q})},$$

so that, by rationalizing denominators,

$$\sigma'(u) = \frac{\pm 1/2}{\delta_q(\chi,\chi')} \left(\sqrt{(q/\tilde{q})^2 + 4A/u} - \sqrt{(q/\tilde{q})^2 + 4A'/u} \right) - v.$$

Expanding the difference of roots above according to (10) and (9) yields the quantity

$$\sum_{k\geqslant 0} \binom{1/2}{k} (q/\tilde{q})^{2k} \big((4A/u)^{1/2} (u/4A)^k - (4A'/u)^{1/2} (u/4A')^k \big),$$

which, along with (11), shows that the sum in (30) with phase σ satisfies the appropriate conditions in Lemma 3 (keeping in mind Remark 2). From here and (11), we see that the sum in (30) vanishes unless $|v|_p = 1$, as solutions to the stationary phase congruence $\sigma'(u) \equiv 0 \pmod{\mathrm{rt}_*(Q)}$ could not exist otherwise. Since $\alpha^{1/2}\beta^{1/2}/(\alpha\beta)^{1/2} \in \{\pm 1\}$ for every $\alpha, \beta \in \mathbb{Z}_p^{\times 2}$, any solutions to the stationary phase congruence must satisfy one of the four congruences

$$\delta_q(\chi,\chi')^{-1} \sum_{k\geqslant 0} \binom{1/2}{k} (q/\tilde{q})^{2k} \big(\epsilon_1 (u/4A)^k - \epsilon_2 (A'/A)^{1/2} (u/4A')^k \big) \equiv v\,(u/A)^{1/2} \pmod{\mathrm{rt}_*(Q)}$$

with $\epsilon_i \in \{\pm 1\}$, where in fact $\epsilon_1 = \epsilon_2$ unless, possibly, $\delta_q(\chi,\chi') = 1$. Each of these four congruences is polynomial in $(u/A)^{1/2}$ modulo $\mathrm{rt}_*(Q)$, satisfies the hypotheses of Hensel's lemma, and reduces to a non-degenerate linear congruence in $(u/A)^{1/2}$ modulo p. Thus there are $O(1)$ solutions modulo $\mathrm{rt}_*(Q)$ to the stationary phase congruence. The proposition then follows. □

5. Short second moment estimates

Proposition 1 provides an individual bound for the short second moment $S_2(\chi)$ in terms of averages of the arithmetic function $K_\chi(m;\tilde{q})$. In this section, we leverage this result and the estimates on exponential sums from section 4 to prove in Proposition 3 our penultimate result, an aggregate bound on the short second moment over a *collection* of characters modulo q_2.

Proposition 3. *Let q_1, q_2, and q be subject to the conditions in (12). Let χ be any primitive character modulo q, and let Ψ be any set of Dirichlet characters modulo q_2. Then*

$$\sum_{\psi_2 \in \Psi} S_2(\chi\psi_2) \ll q^\varepsilon \left((q_1 + q_1^{1/4} q_2^{1/4}) |\Psi| + q^{1/2} |\Psi|^{1/2} \right).$$

Proof. We will use Proposition 1; in its notation, we may assume that $Q_1/p^\eta \gg q^{1/2-\varepsilon} \geqslant p^2$, as Proposition 3 is trivially true for $q \ll p^4$. Decomposing $K_\chi(m;Q_1/p^\eta)$ as $K_\chi^+ + K_\chi^-$ as in Lemma 6, Proposition 1 gives us

$$\sum_{\psi_2 \in \Psi} S_2(\chi\psi_2) \ll q^\varepsilon \left(q_1 |\Psi| + q_1^{3/2} q^{-1/2} \big(T^+(\Psi) + T^-(\Psi) \big) \right), \tag{31}$$

where

$$T^\pm(\Psi) := \mathrm{Re} \sum_{\psi_2 \in \Psi} \sum_{p^\eta \ll q^{1/2+\varepsilon} q_1^{-1}} p^{\eta/2} \sideset{}{^*}\sum_{|m| \ll q^{1+\varepsilon}(q_1^2 p^{2\eta})^{-1}} K_{\chi\psi_2}^\pm(m;Q_1/p^\eta) A(m;p^\eta)$$

and $A(m;p^\eta) \ll m^\varepsilon$. Application of the Cauchy–Schwarz inequality produces the bound

$$T^\pm(\Psi) \leqslant \frac{q^{1/2+\varepsilon}}{q_1}\left(\sum_{\psi_2,\psi_2'\in\Psi}\sum_{p^\eta\ll q^{1/2+\varepsilon}q_1^{-1}} p^{-\eta}\sideset{}{^*}\sum_{|m|\ll q^{1+\varepsilon}(q_1^2p^{2\eta})^{-1}} K^\pm_{\chi\psi_2}(m;Q_1/p^\eta)\overline{K^\pm_{\chi\psi_2'}(m;Q_1/p^\eta)}\right)^{1/2}. \tag{32}$$

By Proposition 2, the inner summand above is periodic modulo

$$Q_{\eta,\psi_2,\psi_2'} = \frac{Q_1/p^\eta}{(Q_1/p^\eta,(q/q_2)\delta_{q_2}(\psi_2,\psi_2'))}$$

whenever $Q_{\eta,\psi_2,\psi_2'} \geqslant p^2$. Moreover, in this case, any complete segments of the inner sum in (32) vanish, and an application of Lemma 5 and Proposition 2 to any remaining incomplete segment gives that

$$\sideset{}{^*}\sum_{|m|\ll q^{1+\varepsilon}(q_1^2p^{2\eta})^{-1}} K^\pm_{\chi\psi_2}(m;Q_1/p^\eta)\overline{K^\pm_{\chi\psi_2'}(m;Q_1/p^\eta)} \ll q^\varepsilon Q^{1/2}_{\eta,\psi_2,\psi_2'}.$$

When $Q_{\eta,\psi_2,\psi_2'} \leqslant p$, we bound the inner sum of (32) trivially. The second to inner-most sum of (32) is therefore asymptotically bounded above by

$$\begin{aligned}\sum_{\substack{p^\eta\ll q^{1/2+\varepsilon}q_1^{-1}\\ Q_{\eta,\psi_2,\psi_2'}\geqslant p^2}} \frac{q^\varepsilon Q^{1/2}_{\eta,\psi_2,\psi_2'}}{p^\eta} + \sum_{\substack{p^\eta\ll q^{1/2+\varepsilon}q_1^{-1}\\ Q_{\eta,\psi_2,\psi_2'}\leqslant p}} \frac{q^{1+\varepsilon}}{q_1^2p^{3\eta}}\\ \ll q^\varepsilon\left(\frac{q_2}{q_1\delta_{q_2}(\psi_2,\psi_2')}\right)^{1/2} + q^{1+\varepsilon}\min\left(\frac{q_1\delta_{q_2}(\psi_2,\psi_2')^3}{q_2^3},\frac{1}{q_1^2}\right),\end{aligned}$$

where in fact the second term only enters if $\delta_{q_2}(\psi_2,\psi_2') \gg q_2q^{-(1/2+\varepsilon)}$. Inserting the above into (32), we obtain

$$T^\pm(\Psi) \ll \frac{q^{1/2+\varepsilon}}{q_1}\left(\frac{q_2^{1/4}}{q_1^{1/4}}|\Psi| + \frac{q^{1/2}}{q_1^{1/2}}|\Psi|^{1/2}\right).$$

Inserting this bound into (31), we complete the proof of Proposition 3. □

6. Proof of Theorem 2

Let ε be an arbitrary, small positive real number. We will begin by defining the sets

$$\begin{aligned}R_2(V;\chi) &:= \{\chi_2 \pmod{q_2} : \chi\chi_2 \in R(V;q)\}\\ \text{and}\quad \Psi(V;\chi) &:= \{\psi_2 \pmod{q_2} : \psi_1\psi_2 \in R_2(V;\chi) \text{ for some } \psi_1 \pmod{q_1}\}.\end{aligned}$$

Clearly we may assume that q is a sufficiently high power of p. Asymptotics of the fourth moment of Dirichlet L-functions due to Heath-Brown [6] and later improved by Soundararajan [16] imply that

$$\sum_{\chi \pmod q} \left|L\left(\tfrac12,\chi\right)\right|^4 \ll q^{1+\varepsilon},$$

from which it follows that $|R(V;q)| \ll q^{1+\varepsilon}V^{-4}$. This suffices to handle the case when $V \leqslant q^{1/8+2\varepsilon}$. On the other hand, by the Weyl bound for Dirichlet L-functions to prime power moduli due to Postnikov [15] (see also [11]), $|R_2(V;\chi)| = 0$ for $V \geqslant q^{1/6+\varepsilon}$.

Consider now the values of $q^{1/8+2\varepsilon} \leqslant V \leqslant q^{1/6+\varepsilon}$. We combine the observations

$$|R_2(V;\chi)| \leqslant \frac{1}{V^2\varphi(q_1)}\sum_{\psi_2\in\Psi(V;\chi)} S_2(\chi\psi_2) \quad\text{and}\quad |\Psi(V;\chi)| \leqslant \varphi(q_1)R_2(V;\chi),$$

with Proposition 3 and the choices $V^2q^{-3\varepsilon} \leqslant q_1 \leqslant V^2q^{-2\varepsilon}$ and $q_2 = q_1^3$. With these choices, we obtain

$$\begin{aligned}|R_2(V;\chi)| &\ll \frac{q^\varepsilon}{V^2\varphi(q_1)}\Big(q_1\varphi(q_1)|R_2(V;\chi)| + q^{1/2}\varphi(q_1)^{1/2}|R_2(V;\chi)|^{1/2}\Big)\\ &\ll q^{-\varepsilon}|R_2(V;\chi)| + \frac{q^{1/2-\varepsilon}}{q_1^{3/2}}|R_2(V;\chi)|^{1/2},\end{aligned}$$

from which in turn it follows that

$$|R_2(V;\chi)| \ll \frac{q^{1+\varepsilon}}{q_1V^4}.$$

As a consequence,

$$|R(V;q)| = \frac{1}{\varphi(q_2)}\sideset{}{^*}\sum_{\chi \pmod q}|R_2(V;\chi)| \ll q^{2+\varepsilon}V^{-12},$$

which completes the proof of Theorem 2, and hence of Theorem 1.

References

[1] Valentin Blomer and Djordje Milićević. "p-adic analytic twists and strong subconvexity". In: *Ann. Sci. Éc. Norm. Supér. (4)* 48.3 (2015), pp. 561–605. DOI: 10.24033/asens.2252.

[2] J. Bourgain. "Decoupling, exponential sums and the Riemann zeta function". In: *J. Amer. Math. Soc.* 30.1 (2017), pp. 205–224. DOI: 10.1090/jams/860.

[3] J. B. Conrey and H. Iwaniec. "The cubic moment of central values of automorphic L-functions". In: *Ann. of Math. (2)* 151.3 (2000), pp. 1175–1216. DOI: 10.2307/121132.

[4] S. W. Graham and G. Kolesnik. *van der Corput's method of exponential sums*. Vol. 126. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1991, pp. vi+120. DOI: 10.1017/CBO9780511661976.

[5] D. R. Heath-Brown. "Hybrid bounds for Dirichlet L-functions". In: *Invent. Math.* 47.2 (1978), pp. 149–170. DOI: 10.1007/BF01578069.

[6] D. R. Heath-Brown. "The fourth power mean of Dirichlet's L-functions". In: *Analysis* 1.1 (1981), pp. 25–32. DOI: 10.1524/anly.1981.1.1.25.

[7] D. R. Heath-Brown. "The twelfth power moment of the Riemann-function". In: *Quart. J. Math. Oxford Ser. (2)* 29.116 (1978), pp. 443–462. DOI: 10.1093/qmath/29.4.443.

[8] A. E. Ingham. "Mean-value theorems in the theory of the Riemann zeta-function". In: *Proc. London Math. Soc. (2)* 27.4 (1927), pp. 273–300. DOI: 10.1112/plms/s2-27.1.273.

[9] Alastair James Irving. "Estimates for character sums and Dirichlet L-functions to smooth moduli". In: *Int. Math. Res. Not. IMRN* 15 (2016), pp. 4602–4633. DOI: 10.1093/imrn/rnv285.

[10] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*. Vol. 53. American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, RI, 2004, pp. xii+615. DOI: 10.1090/coll/053.

[11] Djordje Milićević. "Sub-Weyl subconvexity for Dirichlet L-functions to prime power moduli". In: *Compos. Math.* 152.4 (2016), pp. 825–875. DOI: 10.1112/S0010437X15007381.

[12] Yoichi Motohashi. *Spectral theory of the Riemann zeta-function*. Vol. 127. Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge, 1997, pp. x+228. DOI: 10.1017/CBO9780511983399.

[13] Ramon M Nunes. "The twelfth moment of Dirichlet L-functions with smooth moduli". In: *Int. Math. Res. Not. IMRN* (2019). DOI: 10.1093/imrn/rnz089.

[14] I. Petrow and M. P. Young. "The Weyl bound for Dirichlet L-functions of cube-free conductor". In: *ArXiv e-prints* (Nov. 2018). arXiv: 1811.02452 [math.NT].

[15] A. G. Postnikov. "On the sum of characters with respect to a modulus equal to a power of a prime number". In: *Izv. Akad. Nauk SSSR. Ser. Mat.* 19 (1955), pp. 11–16.

[16] K. Soundararajan. "The fourth moment of Dirichlet L-functions". In: *Analytic number theory.* Vol. 7. Clay Math. Proc. Amer. Math. Soc., Providence, RI, 2007, pp. 239–246.

[17] J. Wu and P. Xi. "Arithmetic exponent pairs for algebraic trace functions and applications". In: *ArXiv e-prints* (Mar. 2016). arXiv: 1603.07060 [math.NT].

Bryn Mawr College, Department of Mathematics, 101 North Merion Avenue, Bryn Mawr, PA 19010, USA

Current address: Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany

Email address: dmilicevic@brynmawr.edu

Bryn Mawr College, Department of Mathematics, 101 North Merion Avenue, Bryn Mawr, PA 19010, USA

Email address: dfwhite@brynmawr.edu