p-ADIC ANALYTIC TWISTS AND STRONG SUBCONVEXITY

TWISTS p-ADIQUE ANALYTIQUES ET SOUS-CONVEXITÉ FORTE

VALENTIN BLOMER AND DJORDJE MILIĆEVIĆ

Abstract. Let f be a fixed cuspidal (holomorphic or Maaß) newform. We prove a Weyl-exponent subconvexity bound $L(f \otimes \chi, 1/2+it) \ll_{p,t} q^{1/3+\varepsilon}$ for the twisted L-function of f with a Dirichlet character χ of prime power conductor $q = p^n$ (with an explicit polynomial dependence on p and t). We obtain our result by exhibiting strong cancellation between the Hecke eigenvalues of f and the values of χ, which act as twists by exponentials with a p-adically analytic phase. Among the tools, we develop a general result on p-adic approximation by rationals (a p-adic counterpart to Farey dissection) and a p-adic version of van der Corput's method for exponential sums.

Soit f une forme primitive nouvelle (holomorphe ou Maass). Soient p un nombre premier, $n \geqslant 1$ un entier, et t un nombre réel. Nous démontrons une borne sous-convexe de type Weyl pour la fonction L de f, tordue par un caractère de Dirichlet χ de conducteur $q = p^n$. Plus précisément, on démontre $L(f \otimes \chi, 1/2+it) \ll_{p,t} q^{1/3+\varepsilon}$, avec une dépendance polynomiale et explicite en p et t. La preuve repose sur la compensation entre les valeurs propres de Hecke de f et les valeurs de χ, dont l'oscillation est gouvernée par une phase p-adique analytique. Au cours de la démonstration, on développe quelques outils p-adiques, analogues de méthodes classiques ou archimédiennes, telles que la dissection de Farey et la méthode de van der Corput pour les sommes d'exponentielles.

1. Introduction

1.1. **Orthogonality of arithmetic functions.** It is a central question in number theory to understand the asymptotic distribution of arithmetic functions such as the Möbius function, Dirichlet characters of large conductor, or Hecke eigenvalues of automorphic forms. It is expected that they display a certain degree of randomness, and one also expects a certain degree of (asymptotic) orthogonality between classes of sufficiently independent arithmetic functions. On average, this can often be proved in a strong quantitative sense by large sieve inequalities.

In this paper we are interested in convolutions of Hecke eigenvalues $a(m)$ of automorphic forms for the group $\mathrm{SL}_2(\mathbb{Z})$ and arithmetic functions g that are periodic modulo a large prime power $q = p^n$. Such arithmetic weight functions (possibly with a general defining modulus q) have been studied recently in various contexts for instance in [5, 9, 10]. We develop methods to exhibit cancellation in sums of the type

$$\sum_{\substack{m \leqslant M \\ (m,p)=1}} a(m)g(m), \qquad g : (\mathbb{Z}/p^n\mathbb{Z})^\times \to \mathbb{C}, \tag{1.1}$$

where g is a "twisting" function satisfying certain natural conditions in small p-adic neighborhoods (which we discuss in this introduction), and M is comparatively small in terms of q. As a prototypical example we work out in full detail the case where $g = \chi$ is a primitive Dirichlet character of large conductor p^n. Our main result is as follows.

2000 *Mathematics Subject Classification.* Primary 11F66, 11L40, 11L07.

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

First author supported by the Volkswagen Foundation and a Starting Grant of the European Research Council.

Theorem 1. *Let p be an odd prime. Let f be a holomorphic or Maaß Hecke eigenform for $\mathrm{SL}_2(\mathbb{Z})$ with Hecke eigenvalues $a(m)$, let χ be a primitive character modulo $q = p^n$, let W be a smooth weight function with support in $[1,2]$ satisfying $W^{(j)} \ll Z^j$ for some $Z \geqslant 1$, and let $M \geqslant 1$. Then*

$$L := \sum_m a(m)\chi(m)W\left(\frac{m}{M}\right) \ll_{f,\varepsilon} Z^{5/2}p^{7/6} \cdot M^{1/2}q^{1/3+\varepsilon} \tag{1.2}$$

for any $\varepsilon > 0$.

We outline our approach in the proofs of Theorems 1 and 2 (see below) in Section 1.3. Theorem 1 is properly seen as the p-adic analogue of cancellation in Dirichlet polynomials of the type

$$\sum_{m \leqslant M} a(m)m^{it} \tag{1.3}$$

for large $t \in \mathbb{R}$, which have occupied an important place in number theory and, in particular, in connection with subconvexity of automorphic L-functions. Our twists in (1.2) are p-adically analytic (see (2.2)), and Theorem 1 is a true analogue of bounds on (1.3) in the sense that we study a twist that is highly ramified at one fixed place of $\mathbb{Q}$. It should come as no surprise that Theorem 1, which establishes strong asymptotic orthogonality between Hecke eigenvalues and p-adic twists, will both be of independent interest and have applications to subconvexity, which we describe in Section 1.2.

We now comment on the results of Theorem 1 within a more general framework. Our method can be adapted to treat sums of the form (1.1), where g is sufficiently well-behaved in small p-adic neighborhoods. In particular, we need to be able to control the terms that take place of the first and second derivative (which, for p-adic analytic functions, can be read off from their p-adic power series expansion) of a specific phase resulting from g; see also the discussion at the end of Section 4. Corollary 4 displays a prototype of a requisite two-term expansion, such as that given by (2.3) below in the case of a Dirichlet character. In general, such expansions are easily available for functions g given by complete exponential sums that can be explicitly evaluated by discrete stationary phase (such as in our Lemmas 7 and 9), or for functions g that are exponentials of any p-adically analytic phase with a sufficiently explicit power series expansion (such as, for example, the class $\mathbf{F}$ in [26], which is also fairly stable under natural operations).

The proof of Lemma 9 contains the evaluation of an implicit function where the special shape of (2.3) comes handy. A prototype of a general implicit function theorem can be found in [26, Lemma 9]; analogous technology can be used for a corresponding version of Lemma 9 for general weight functions g. With some careful bookkeeping, the method can also be adapted to yield hybrid bounds for sums of the form (1.1) and (1.2) for characters (and more general arithmetic weights) to all sufficiently powerful moduli q.

We comment on the ranges of various parameters in Theorem 1. In this paper, q is the basic parameter, and we think of p and Z as being relatively small. We do emphasize right away, however, that all results, including Theorems 1 and 2, are completely uniform across all primes p and all prime powers $q = p^n$ (as well as across all values of Z in Theorem 1). Thus, while particularly strong results are obtained in the so-called "depth aspect", taking p fixed and having n tend to infinity, we obtain at the same time new results already for n moderately large, say with such n fixed and p tending to infinity.

The Rankin–Selberg bound (2.9) implies that $L \ll_f M$, so that (1.2) yields a non-trivial result in the range

$$M \geqslant Z^5 p^{7/3} \cdot q^{2/3+\delta} \tag{1.4}$$

for $\delta > 0$. On the other hand, if M is substantially larger than Zq, one can apply the functional equation of $L(f \otimes \chi, s)$ to reduce the length of the sum to about Z^2q^2/M. We present the details of this well-known argument at the beginning of Section 5 below, and conclude from this discussion that the real value of Theorem 2 lies in the range $q^{2/3+\delta} \ll_{Z,p} M \ll_{Z,p} q^{4/3-\delta}$.

While we did not try to optimize the exponent of the parameter Z in Theorem 1, the (explicit) polynomial dependence on Z gives us the flexibility to have slightly oscillating weight functions or weight functions with sharp cut-offs. In particular, in the situation of Theorem 1 we obtain

$$\sum_{m \leqslant M} a(m)\chi(m) \ll_{f,\varepsilon} p^{1/3} \cdot M^{6/7} q^{2/21+\varepsilon} \tag{1.5}$$

which beats the trivial bound if $M \geqslant p^{7/3} q^{2/3+\delta}$, cf. (1.4).

We put considerable care into the exponent of p in Theorem 1, although we do not claim that it is the best obtainable from our method. Finally, the implied constant in (1.2) depends polynomially on the archimedean parameter of f (weight or Laplacian eigenvalue). This can be seen by using the uniform bounds for Bessel functions in [16, Appendix]. Also, the case $p = 2$ can be dealt with in the same fashion at only the cost of some rather cumbersome notation; see [26] for a prototype where small primes are treated uniformly.

It should be noted that Theorems 1 and 2 (stated in the next subsection) are completely independent of bounds towards the Ramanujan conjecture. In fact, the only "automorphic information" needed are an approximate functional equation, the Voronoi summation formula, and a Rankin-Selberg-type mean value bound for Hecke eigenvalues.

We also remark that the natural but easier continuous spectrum analogues of both Theorem 1 and 2, involving the Eisenstein series and their Fourier coefficients $d_t(m) := \sum_{ab=m} (a/b)^{it}$, are known. By Mellin inversion, we have

$$\sum_m d_t(m)\chi(m) W\left(\frac{m}{M}\right) = \frac{1}{2\pi i} \int_{(1/2)} L(s+it,\chi) L(s-it,\chi) \widehat{W}(s) M^s ds.$$

According to [26], one has (the sub-Weyl) subconvexity bound $L(1/2+it,\chi) \ll A_{p,t} \cdot q^{1/6-\delta}$ for a primitive character χ of conductor $q = p^n$ with an explicit $A_{p,t} > 0$ and absolute $\delta > 0$. From this, one obtains the desired cancellation between $d_t(m)$ and characters of conductor $q = p^n$ in the situation of Theorem 1 with the even stronger bound $\ll B_{p,t,Z} \cdot q^{1/3-2\delta} M^{1/2}$ with an explicit $B_{p,t,Z} > 0$.

A very beautiful theory for a somewhat different family of twisting functions g has been and is currently being developed by Fouvry, Kowalski and Michel [9, 10]. Their twists are *algebraic* in nature and come as trace functions of ℓ-adic sheaves on $\mathbb{A}^1_{\mathbb{F}_p}$, including in particular exponentials and Dirichlet characters with rational functions and hyper-Kloosterman sums. Using both spectral-theoretic and algebro-geometric methods, they obtain cancellation in twisted sums of the form

$$L_K := \sum_m a(m) K(m) W\left(\frac{m}{M}\right)$$

where $K : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ (q prime) is an "admissible trace weight" and W is as in Theorem 1. For instance, in [9, Theorem 1.5] they establish the bound $L_K \ll Z \cdot M^{1/2} q^{3/8+\varepsilon}$ for $M \leqslant Zq$. It would lead too far to give a detailed discussion on the similarities and differences of the two approaches, and we restrict ourselves to two fairly obvious observations: as the theory of Fouvry-Kowalski-Michel is powered by algebraic geometry and in particular the Riemann hypothesis over finite fields, their trace weights are naturally periodic modulo a prime. In contrast, our method uses p-adic analysis, hence we consider moduli that are a sufficiently large prime power. (It should be noted, however, that the method of stationary phase, in its geometric incarnation due to Laumon, is also a fundamental tool in [9], and it would be interesting to compare the use of stationary phase in [9] and the present paper.) Secondly and perhaps most importantly, our bound is stronger in terms of q which constitutes precisely the difference between a "Weyl-type" exponent and a "Burgess-type" exponent. We will continue this discussion in the next subsection when we consider applications of Theorem 1 to L-functions.

1.2. **Applications to subconvexity.** A classical result states that the Riemann zeta function satisfies the bound

$$\zeta(1/2+it) \ll_\varepsilon (1+|t|)^{1/6+\varepsilon} \tag{1.6}$$

on the critical line. It was proved first by Hardy and Littlewood (cf. [24]), based on work of Weyl [30], and first written down by Landau [23] in a slightly refined form and generalized to all Dirichlet L-functions. Results of similar strength to (1.6) exist (in the t-aspect) for automorphic L-functions of degree 2. Using deep bounds on triple products, Good [12] proved that, for a fixed holomorphic cusp form f, one has

$$L(f, 1/2+it) \ll_{f,\varepsilon} (1+|t|)^{1/3+\varepsilon}. \tag{1.7}$$

A very different approach to prove (1.7), much more in the spirit of the Weyl-Hardy-Littlewood method, was developed by Jutila [20] and generalized to Maaß forms by Meurman [25]. While (1.6) was improved slightly over the years, (1.7) is still the current record (except for replacing ε-powers by powers of the logarithm).

Subconvexity in the conductor aspect seems to be a harder problem. The analogue of (1.6) is Burgess' [6] bound $L(\chi, 1/2+it) \ll_t \mathrm{cond}(\chi)^{3/16+\varepsilon}$, and again one has a result of similar strength for automorphic L-functions of degree 2 (see [7, 2])

$$L(f \otimes \chi, 1/2+it) \ll_{t,f,\varepsilon} \mathrm{cond}(\chi)^{3/8+\varepsilon} \tag{1.8}$$

for a fixed automorphic form f. Unless χ is quadratic [8], (1.8) has not been improved, and in particular the exponent $1/3$, i.e. the quantitative analogue of (1.7), is unknown. As a corollary of Theorem 1, we can close the gap between (1.7) and (1.8) if the conductor of χ is a prime power $q = p^n$, while we retain explicit polynomial dependence in the parameters p and t.

Theorem 2. *Let p be an odd prime. Let f be a holomorphic or Maaß cuspidal newform for $\mathrm{SL}_2(\mathbb{Z})$, and let χ be a primitive character of conductor $q = p^n$. Let $t \in \mathbb{R}$. Then one has*

$$L(f \otimes \chi, 1/2+it) \ll_{f,\varepsilon} (1+|t|)^{5/2} p^{7/6} \cdot q^{1/3+\varepsilon}.$$

The quality of subconvexity exponent in the q-aspect in Theorem 2, one-third of the way from the trivial bound toward the Lindelöf hypothesis and often referred to as a Weyl-type bound, is a serious barrier that has been breached only for two families of degree-one L-functions [26] and in the present situation is very unlikely to be improved with current technology. The Weyl exponent is known for very few families of L-functions. It is the current record for subconvexity of GL_2 L-functions in the t-aspect and the eigenvalue aspect [21], and it comes up naturally in sup-norm bounds for automorphic forms on hyperbolic surfaces of large volume [11, 4] which may be thought of as partly analogous to subconvexity bounds.

As is the case with Theorem 1 and (1.3), Theorem 2 is a close analogue of (1.7) as involving a twist highly ramified at one fixed (finite) place of $\mathbb{Q}$. The analogy between analytic number theory at finite and infinite places and in particular subconvexity in the depth aspect (cf. early work [1, 15]) has recently received considerable attention (see [26] for a consistent application of p-adic analysis in this context and [27]); see also Vishe [29], who establishes a fast algorithm to compute the value of $L(f \otimes \chi, 1/2)$ using an idea of Venkatesh [28] based on equidistribution of long p-adic horocycles. Theorems 1 and 2 and the p-adic methods we develop in the course of proving them lend strong support to the understanding that, within what we call the level or q-aspect in analytic arithmetic problems, the square-full direction plays a very distinctive rôle.

For fixed p, our results produce subconvexity of Weyl-type quality as $n \to \infty$, but we get subconvexity as soon as $n > 7$, and improve on the Burgess bound as soon as $n > 28$, uniformly across all (odd) primes p.

1.3. **Method of proof and overview of the paper.** Our method of proof of Theorems 1 and 2 is inspired by Jutila's treatment [20] and establishes the p-adic counterpart of this flexible argument. Large parts of the paper are consequently p-adic in nature, and we develop several p-adic results of independent interest, two of which we specifically discuss in Sections 1.4 and 1.5 below. In Section 4, we provide a brief sketch of Jutila's archimedean argument for reader's reference. The central section of the paper, Section 5, presents proofs of Theorems 1 and 2, which we outline below. For clarity, two crucial estimates for these proofs and the methods we develop to address them are then presented in subsequent Sections 6–9.

The starting point of our argument is (2.2) below, which describes our twisting function $\chi(m) = \theta(\alpha \log_p m/p^n)$ as the result of evaluation of the standard additive character $\theta : \mathbb{Q}_p \to \mathbb{C}^\times$ on a "phase" given by a p-adic analytic function. (As discussed there, we need much less information than analyticity.) We split the sum L in Theorem 1 into suitable *arithmetic progressions* to high powers of p (that is, intersections of small p-adic balls with $\mathbb{Z}$), in which the derivative α/m of the non-archimedean phase $\alpha \log_p m$ is very well p-adically approximated by a/b, with a, b of controlled (archimedean) size and coprime to p. This is the p-adic analogue of a Farey decomposition, and in particular a precise version of Dirichlet's approximation theorem; we state and discuss this theorem in Section 1.4 and prove it in Section 3.

We decompose the localized sums using multiplicative characters; the effect of the p-adic approximation effort is a serious reduction of the modulus in this harmonic analysis. An application of Voronoi summation to the resulting sums produces certain complete exponential (character) sums and oscillatory integrals, the former containing the essential asymptotic information. Both are evaluated in Lemmas 2 and 3, which we prove by intricate (archimedean and p-adic) stationary phase method in Sections 6 and 7. In particular, our explicit evaluation of the character sum features exactly two terms, each of which is essentially an exponential with an entirely explicit p-adically analytic phase; see Section 7.2 for a more thorough discussion and underlying intuition.

Corresponding to each of the various arithmetic progressions, we thus obtain a short sum of Hecke eigenvalues highly twisted by exponentials with explicit p-adically analytic and linear archimedean phases. A trivial estimation of these sums individually recovers the convexity bound. However, after applying the Cauchy-Schwarz inequality, we extract extra cancellation on average over the various arithmetic progressions (and get rid of the automorphic information in the process). We achieve this by developing in Section 8 a p-adic second derivative test, an analogue of van der Corput's technique, which we discuss in Section 1.5. We then apply this machinery in Section 9 and obtain generically full square-root strength savings in the resulting exponential sums, thus providing the final ingredient in the proof of Theorem 1.

We point out that all results are written entirely explicitly and with no direct reference to p-adic analysis, in order to make minimal assumptions and various extensions completely transparent. Nevertheless, the p-adic analysis does underlie a lot of important intuition in this article, and the reader may keep the p-adic metaphor in mind throughout; in particular, all of the apparently *ad hoc* calculations and massive cancellations in Sections 7 and 9 appear for structural reasons.

1.4. **p-adic approximation.** The Farey dissection is a classical tool in diophantine approximation. It is the starting point for variants of the circle method without minor arcs and contains as a direct consequence Dirichlet's approximation theorem. In Section 3, we prove the following p-adic Farey dissection theorem that decomposes $\mathbb{Z}_p^\times$ into small p-adic balls, centered at rational numbers a/b with a and b of bounded size. For our application, we want to approximate the derivative α/m of the phase in (2.2); therefore, we state the dissection in the following form.

Theorem 3. *Let $\alpha \in \mathbb{Z}_p^\times$, $\ell \in \mathbb{N}$, and an integer $-\ell \leqslant r \leqslant \ell$ be given. Write $r^+ = \max(r, 0)$ and $r^- = \max(-r, 0)$, and let*[1]

$$S = \big\{(a, b, k) \in \mathbb{Z} \times \mathbb{N} \times \mathbb{N}_0 : b \leqslant p^{k+2r^-},\ |a| \leqslant p^{k+2r^+},\ (a, b) = (a, p) = (b, p) = 1\big\}.$$

For $(a, b, k) \in S$, let

$$\mathbb{Z}_p^\times[a, b, k] = \{m \in \mathbb{Z}_p^\times \mid b\alpha/m - a \in p^{\ell+|r|+k}\mathbb{Z}_p\}.$$

Then there exists a subset $S^0 \subseteq S$ such that

$$\mathbb{Z}_p^\times = \bigsqcup_{(a,b,k)\in S^0} \mathbb{Z}_p^\times[a, b, k] \tag{1.9}$$

[1]Here and in the following, we use the notation $\mathbb{N}_0 := \mathbb{N} \sqcup \{0\} = \{0, 1, 2, \ldots\}$.

and in addition the following two properties hold: if $(a, b, k_1), (a, b, k_2) \in S^0$*, then* $k_1 = k_2$*, and for each* $(a, b, k) \in S^0$ *one has* $k \leqslant \ell - |r|$.

Theorem 3 can also be seen as a statement about integers; its statement and proof are valid practically verbatim by replacing every instance of $\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$ by $\mathbb{Z}$ and $\mathbb{Z}\setminus p\mathbb{Z}$, respectively. Under such interpretation, the theorem states that $\mathbb{Z} \setminus p\mathbb{Z}$ can be partitioned into arithmetic progressions such that, for integers m in each individual partition, α/m is very well p-adically approximated by a/b. The conclusion of Theorem 3 should be contrasted with Dirichlet's familiar approximation theorem, which states that, for every $x \in \mathbb{R}$, there is a rational number a/b with $b \leqslant B$ such that $|x - a/b| \leqslant 1/bB$. Indeed, we will prove Theorem 3 by an elaboration of Dirichlet's Box Principle argument.

Theorem 3 features a parameter r with which one can control the relative size of a and b. This extra flexibility is very important in our application for the proof of Theorem 1. In the most difficult range $M \asymp (qZ)^{(1+o(1))}$, we will be setting $r = 0$ in the application of Theorem 3, cf. (5.19). In other words, we will be approximating p-adic units by a/b with the (archimedean) size of both a and b equally bounded from above. In other ranges, however, it is necessary to choose different values for r. In the extreme case $|r| = \ell$, Theorem 3 reduces (except for the appearance of the absolute value in the condition $|a| \leqslant p^{2\ell}$, an asymptotically insignificant distinction) to the trivial statement that every p-adic integer can be approximated within $p^{-2\ell}$ by an integer no greater than $p^{2\ell}$.

Finally we comment on the application of Theorem 3 in the context of estimating (1.1) where g is a more general twisting exponential with a p-adically analytic phase, or an arithmetic weight function satisfying a two-term expansion as in Corollary 4 (or some variation of it). Then it follows as in Lemma 10 that, for a suitable fixed κ, the "first derivative" $g_1(x)$ of the phase satisfies $g_1(x + p^\kappa t) - g_1(x) \in p^{\kappa+\lambda} t\mathbb{Z}_p^\times$, and in particular $g_1(x + t) - g_1(x) \in p^\mu\mathbb{Z}_p$ for $t \in p^\kappa\mathbb{Z}_p$, if and only if $t \in p^{\mu-\lambda}\mathbb{Z}_p$. Therefore, in such a situation, the dissection of $\mathbb{Z}_p^\times$ provided in Theorem 3 according to p-adic approximations of $g_1(m)/|g_1(m)|_p$ by a rational number also induces a dissection of the original values $m \in \mathbb{Z}_p$ into p-adic balls; moreover, the radii will typically be commensurate in these two dissections since generically $\operatorname{ord}_p g_1 \approx \lambda$.

1.5. p-adic van der Corput theory.

Van der Corput's theory (see [14]) relies on fundamental estimates of exponential sums in terms of the known information about the rate of change of a sufficiently smooth phase. As a typical case, one is interested in non-trivial bounds for sums of the type

$$\sum_{M_1 \leqslant m \leqslant M_2} e^{ig(m)} \tag{1.10}$$

where g is sufficiently smooth and one has some control on the derivatives of g. In particular, the second derivative test estimates an exponential sum in terms of the size of the second derivative of the phase $g(x)$, since this quantity can be used to control the number of stationary phase points.

We are interested in functions f of arithmetic nature that enjoy some p-adic regularity. In this case, we can establish bounds of the same strength as in the classical theory. In the following we give a prototype of a second derivative test for p-adic exponential sums. A much more general and flexible version of the theorem, tailored for a variety of applications, will be given in Section 8. Our theorem provides an estimate for an exponential sum of the form

$$\sum_{M_1 \leqslant m \leqslant M_2} f(m)$$

(and generalizations thereof) where f is a function for which the values $f(x + p^\kappa t)$ along arithmetic progressions with difference p^κ (which can be thought of as p-adic balls around x) are sufficiently well modelled by quadratic exponentials $f(x) \cdot \theta\big(g_1(x) \cdot p^\kappa t + \frac{1}{2} g_2(x) \cdot p^{2\kappa} t^2\big)$. Here, θ is the standard additive character on $\mathbb{Q}_p$; see Section 2.1.

Corollary 4. *Let $\lambda,\varphi\in\mathbb{N}_0$. Let $f:\mathbb{Z}_p\to\mathbb{C}^\times$, $g_1:\mathbb{Z}_p\to p^{-\varphi}\mathbb{Z}_p$, $g_2:\mathbb{Z}_p\to p^{-\lambda}\mathbb{Z}_p^\times$, $h:\mathbb{Z}_p\times\mathbb{Z}_p\times\mathbb{N}_0\to\mathbb{Z}_p$ be functions satisfying*

$$f(x+p^\kappa t)=f(x)\theta\left(g_1(x)p^\kappa t+\tfrac{1}{2}g_2(x)p^{2\kappa}t^2+\frac{h(x,t,\kappa)}{p^{\max(0,\lambda-2\kappa-1)}}\right)$$

for every $x,t\in\mathbb{Z}$, $\kappa\in\mathbb{N}_0$. Let $M_1<M_2$ be real numbers. Then

$$\sum_{M_1\leqslant m\leqslant M_2} f(m)\ll\|f\|_\infty\big((M_2-M_1)+p^\varphi+p^\lambda\big)p^{-\lambda/2}$$

for any $\varepsilon>0$.

The more general version, Theorem 5 below, allows, among other things, a smooth weight function $W(m)$, an extra archimedean linear phase $e(\omega m)$ with $\omega\in\mathbb{R}$, substantially more general assumptions on f, and a sum not over a full interval $[M_1,M_2]$, but over a collection of residue classes modulo some power of p.

Finally, we remark that, while the statements of both Theorem 3 and Theorem 5/Corollary 4 can be formulated so as to involve integers only (without mentioning the p-adic completions), they are *bona fide* p-adic statements (even if an elementary reformulation may be preferable for certain purposes). After all, the same could be said about their archimedean analogues: for example, the archimedean van der Corput theory is also concerned with the values of the exponentials in (1.10) over $m\in\mathbb{Z}$ only. It goes without saying, however, that formulating its methods in the language of integers only would be but an exercise in forceful futility, and, in that case as well as in ours, the appropriate completions provide a natural framework in which to formulate analytic assumptions and methods.

Acknowledgements. We would like to thank Peter Sarnak and Philippe Michel for useful discussions. The first author acknowledges the support by the Volkswagen Foundation and a Starting Grant of the European Research Council. Initial work on this paper was completed while the second author visited the Max Planck Institute for Mathematics in Bonn; it is a pleasure to acknowledge the support and excellent research infrastructure at MPIM. Finally, we would very much like to thank the referee for an extremely helpful report that substantially improved the presentation of the paper.

2. Preliminaries and notation

In this section we set up some notation and compile for future reference a number of useful results, some of which are well-known.

2.1. **Notation.** We denote by $\mathbb{Z}_p$ the ring of p-adic integers in the field $\mathbb{Q}_p$ of p-adic numbers, and by $\mathbb{Z}_p^\times=\mathbb{Z}_p\setminus p\mathbb{Z}_p$ the group of its units. Then $\mathbb{Q}_p^\times=\mathbb{Q}_p\setminus\{0\}=\bigsqcup_{k\in\mathbb{Z}}p^k\mathbb{Z}_p^\times$; for $x\in p^k\mathbb{Z}_p^\times$, we write $\operatorname{ord}_p x=k$, $|x|_p=p^{-k}$, and

$$x_0=x\cdot|x|_p^{-1}=x\cdot p^{-k};$$

that is, x_0 denotes the unit part of x. In Sections 9 and 5.5, we also formally write $\operatorname{ord}_p 0=\infty$ and $p^\infty\mathbb{Z}_p^\times=\{0\}$.

If $k\geqslant 0$ and a domain $A\subseteq\mathbb{Z}_p$ are such that $A+p^k\mathbb{Z}_p\subseteq A$, or equivalently if $\mathcal{A}(x)$ is a property enjoyed by some $x\in\mathbb{Z}_p$ such that $\mathcal{A}(x+p^kt)\Leftrightarrow\mathcal{A}(x)$ for every $t\in\mathbb{Z}_p$, and if f is a $p^k\mathbb{Z}_p$-periodic function, then by

$$\sum_{x\bmod p^k,\,x\in A}f(x)\quad\text{and}\quad\sum_{x\bmod p^k\,:\,\mathcal{A}(x)}f(x)$$

we mean, respectively, the (finite) sum of $f(x)$ over an arbitrary set of representatives of classes in $A/p^k\mathbb{Z}_p$ (such as $A\cap\{1,2,\dots,p^k\}$), and the sum of $f(x)$ over an arbitrary set of representatives of those classes $x\in\mathbb{Z}_p/p^k\mathbb{Z}_p$ for which $\mathcal{A}(x)$ holds (such as $\{x\in\{1,2,\dots,p^k\}:\mathcal{A}(x)\}$). The sum is understood to be only over those classes that satisfy all specified conditions if more than one is listed. We keep analogous conventions for appropriately periodic subsets of (or properties defined on) $\mathbb{Z}$.

For $x \in \mathbb{Z}$ coprime to the modulus (or sometimes for $x \in \mathbb{Z}_p^\times$), the notation $\bar{x}$ will always denote the multiplicative inverse to a modulus which will be obvious from the context. In particular, if no obvious modulus is specified, then $\bar{x} = x^{-1}$ will denote the inverse of x in $\mathbb{Z}_p^\times$, which agrees with the multiplicative inverse of x to any prime power p^n. While both $\bar{x}$ and x^{-1} have the same meaning for $x \in \mathbb{Z}_p^\times$, for aesthetic reasons we usually give preference to the former in notations that explicitly depend only on the congruence class of x to an obvious modulus (such as in ϵ-factors, Kloosterman sums, and so on) and to the latter in expressions of a more direct p-adic nature such as phases in the context of p-adic local analysis (even when the expression happens to be locally constant).

The prime $p = 3$ requires a very minor technical adaptation at one place in our argument; to track it, we denote $\iota' = 1$ if $p = 3$ and $\iota' = 0$ otherwise. This notation compares to $\iota'(3)$ in [26].

For $r \in \mathbb{Z}$, we denote

$$r^+ = \max(r, 0), \quad r^- = (-r)^+ = \max(-r, 0).$$

We use the standard Landau notation. We write $f = \mathrm{O}(g)$ or, equivalently, $f \ll g$, if there exists a constant $C > 0$ such that $|f| \leqslant Cg$ whenever all variables involved belong to the specified ranges. The notation $f = \mathrm{O}_{A,B,\dots}(g)$ or $f \ll_{A,B,\dots} g$ denotes that the constant C may depend on the specific values of $A, B, \dots$.

We write $e(x) = e^{2\pi i x}$ for $x \in \mathbb{R}$, and we write $\theta : \mathbb{Q}_p \to \mathbb{C}^\times$ for the standard additive character on $\mathbb{Q}_p$ trivial on $\mathbb{Z}_p$. Specifically, if $x = \sum_{j \geqslant j_0} a_j p^j \in \mathbb{Q}_p$, then $\theta(x) = \exp(2\pi i \sum_{j<0} a_j p^j)$. In particular, on $\mathbb{Z}[1/p] \subseteq \mathbb{Q}_p \cap \mathbb{R}$ we have $\theta(\cdot) = e(\cdot)$, and this relation is crucial for moving arithmetic oscillation between p-adic and archimedean places.

2.2. **Certain classes.** We introduce the following terminology, including an auxiliary class of functions.

Definition 1. *Let $\kappa \in \mathbb{Z}$. We denote by $\mathbf{M}_{p^\kappa}$ an arbitrary element of $p^\kappa\mathbb{Z}_p$, which may be different from line to line. For $\kappa \in \mathbb{N}_0$, we denote by $\boldsymbol{\mu}_{p^\kappa} = \theta(\cdot/p^\kappa) = \theta\big(\mathbf{M}_{p^{-\kappa}}\big)$ an arbitrary complex $(p^\kappa)^{th}$ root of unity, which may be different from line to line.*

Further, let $A_1, \dots, A_s \subseteq \mathbb{Z}_p$ and $\Omega_0 \in \mathbb{N}$ be such that $(1 + p^{\Omega_0}\mathbb{Z}_p)A_i \subseteq A_i$ for every $1 \leqslant i \leqslant s$. We denote by $\mathbf{M}_{p^\kappa}^{\Omega_0}[y_1, \dots, y_s]$ an arbitrary function $M : \prod_{i=1}^s A_i \to p^\kappa\mathbb{Z}_p$, which may be different from line to line, such that, for every $y_1, \dots, y_s$, every $\Omega \geqslant \Omega_0$, and every $y_i' \in (1 + p^\Omega\mathbb{Z}_p)y_i$,

$$M(y_1', \dots, y_s') - M(y_1, \dots, y_s) \in p^{\kappa+\Omega}\mathbb{Z}_p.$$

We also write $\mathbf{M}_{p^\kappa}[y_1, \dots, y_s]$ if the value of Ω_0 is clear from the context (such as $\Omega_0 = 1$).

The classes $\mathbf{M}_{p^\kappa}$, $\boldsymbol{\mu}_{p^\kappa}$, and $\mathbf{M}_{p^\kappa}^{\Omega_0}[y_1, \dots, y_s]$ will be useful for efficient tracking of terms which we think of as remainders in certain two-term p-adic expansions. The domains $A_1, \dots, A_s$ will always be clear from the context. Some examples of immediate interest to us will be introduced in Subsections 2.3 and 2.4 below. We will only need $s = 2$ in Definition 1.

We will frequently use that

$$\mathbf{M}_1[y_1, \dots, y_s] \cdot \mathbf{M}_{p^\kappa}[y_1, \dots, y_s] \subseteq \mathbf{M}_{p^\kappa}[y_1, \dots, y_s] \tag{2.1}$$

for classes $\mathbf{M}_1$ and $\mathbf{M}_{p^\kappa}$ on the same underlying domains $A_1, \dots, A_s$ (or, equivalently, when restricted to the intersection of their respective domains). Indeed, for every $f \in \mathbf{M}_1[y_1, \dots, y_s]$, $g \in \mathbf{M}_{p^\kappa}[y_1, \dots, y_s]$, $\Omega \geqslant \Omega_0$, and $y_1', \dots, y_s'$ with $y_i' \in (1 + p^\Omega\mathbb{Z}_p)y_i$ as above, we have that

$$\begin{aligned}&(fg)(y_1', \dots, y_s') - (fg)(y_1, \dots, y_s)\\ &\quad = \big(f(y_1', \dots, y_s') - f(y_1, \dots, y_s)\big)g(y_1', \dots, y_s') + f(y_1, \dots, y_s)\big(g(y_1', \dots, y_s') - g(y_1, \dots, y_s)\big) \in p^{\kappa+\Omega}\mathbb{Z}_p.\end{aligned}$$

In other words, functions in $\mathbf{M}_1[y_1, \dots, y_s]$ on fixed domains $A_1, \dots, A_s$ form a ring, and $\mathbf{M}_{p^\kappa}[y_1, \dots, y_s]$ is an $\mathbf{M}_1[y_1, \dots, y_s]$-module.

2.3. **Characters.** We recall the structure of multiplicative characters modulo $q = p^n$. In this section, as everywhere else in the paper, p denotes an odd prime; all statements hold with minor but necessary modifications in the case $p = 2$. The p-adic logarithm $\log_p$ is defined on $1 + p\mathbb{Z}_p$ by the convergent series

$$\log_p(1+x) = \sum_{j=1}^{\infty} \frac{(-1)^j}{j} x^j \quad (x \in p\mathbb{Z}_p)$$

and gives an isomorphism of the multiplicative group $(1 + p\mathbb{Z}_p)$ with the additive group $p\mathbb{Z}_p$. From [26, Lemma 13] we recall that, for every primitive character χ of conductor p^n, there exists $\alpha \in \mathbb{Z}_p^\times$ such that, for every $m \equiv 1 \pmod p$,

$$\chi(m) = \theta\left(\frac{\alpha \log_p m}{p^n}\right). \tag{2.2}$$

We recall this argument briefly for completeness. For every $\alpha \in \mathbb{Z}_p$, the map $\chi_{[\alpha]}(m) = \theta(\alpha \log_p m/p^n)$ is a character of the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})_1^\times := (1 + p\mathbb{Z})/(1 + p^n\mathbb{Z})$; let $\Gamma_{n,1}$ denote the dual of $(\mathbb{Z}/p^n\mathbb{Z})_1^\times$. The map $\alpha \mapsto \chi_{[\alpha]}$ defines a homomorphism from $\mathbb{Z}_p \to \Gamma_{n,1}$, and it is easy to see that its kernel is exactly $p^{n-1}\mathbb{Z}_p$. A counting argument shows that we thus obtain an isomorphism (and hence a surjection) $\mathbb{Z}_p/p^{n-1}\mathbb{Z}_p \to \Gamma_{n,1}$. The restriction of a primitive character χ of conductor p^n to $(\mathbb{Z}/p^n\mathbb{Z})_1^\times$ lies in $\Gamma_{n,1} \setminus \Gamma_{n-1,1}$ and is hence of the form $\chi_{[\alpha]}$ for some $\alpha \in \mathbb{Z}_p^\times$.

In fact, we do not need the full strength of (2.2). However, we will use the following corollary, valid for every $\kappa \geqslant 1$ and every $u \in \mathbb{Z}_p^\times$, $t \in \mathbb{Z}_p$:

$$\chi\big(u + p^\kappa t\big) = \chi(u)\theta\left(\frac{\alpha}{p^n}\Big(\frac{1}{u}p^\kappa t - \frac{1}{2u^2}p^{2\kappa}t^2\Big) + \mathbf{M}_{p^{3\kappa-n-\iota'}}[u,t]\right), \tag{2.3}$$

where $\Omega_0 = 1$ in the sense of Definition 1. Here and later, χ is identified with its obvious $p^n\mathbb{Z}_p$-periodic extension to $\mathbb{Z}_p^\times$, which also satisfies (2.2) for all $m \in 1 + p\mathbb{Z}_p$. The equation (2.3) is all the p-adic local information we will require about the function χ. To prove (2.3), we note that (2.2) implies that

$$\chi\big(u + p^\kappa t\big) = \chi(u)\chi\big(1 + p^\kappa u^{-1}t\big) = \chi(u)\theta\left(\frac{\alpha}{p^n}\Big(\frac{1}{u}p^\kappa t - \frac{1}{2u^2}p^{2\kappa}t^2\Big) + f(u,t)\right),$$

where

$$f(u,t) = \alpha p^{3\kappa-n} \sum_{j=3}^{\infty} \frac{(-1)^{j-1}}{j u^j} p^{(j-3)\kappa} t^j. \tag{2.4}$$

For $p \geqslant 5$ and $j \geqslant 4$, the inequality $p^{j-3} \geqslant j$ follows by trivial induction; the same is true for $p = 3$ and $j \geqslant 5$. Hence, in all of these ranges,

$$\operatorname{ord}_p j \leqslant \frac{\log j}{\log p} \leqslant j - 3 \leqslant (j-3)\kappa.$$

From this it follows that $f(u,t) \in \mathbf{M}_{p^{3\kappa-n-\iota'}}$ for $u \in \mathbb{Z}_p^\times$, $t \in \mathbb{Z}_p$.

That $f(u,t) \in \mathbf{M}_{p^{3\kappa-n-\iota'}}[u,t]$ follows immediately by subtracting (2.4) and the same expression for $f(u',t')$, with arbitrary $u' \in (1+p^\Omega\mathbb{Z}_p)u$, $t' \in (1+p^\Omega\mathbb{Z}_p)t$, and $\Omega \geqslant 1$, and observing that $t^j/u^j - t'^j/u'^j = \big((u't)^j - (ut')^j\big)/(uu')^j \in p^\Omega\mathbb{Z}_p$ for every $j \in \mathbb{N}$.

It will suffice for many (but not all) of our purposes to know that there exists an $\alpha \in \mathbb{Z} \setminus p\mathbb{Z}$ such that, for every $\kappa \in \mathbb{N}$ with $3\kappa \geqslant n$ and every $t \in \mathbb{Z}$,

$$\chi\big(1 + p^\kappa t\big) = \theta\left(\frac{\alpha}{p^n}\big(p^\kappa t - \tfrac{1}{2}p^{2\kappa}t^2\big)\right). \tag{2.5}$$

The equality (2.5) is (for $p > 3$) a trivial consequence of (2.2), but it is also entirely elementary. Indeed, for $3\kappa \geqslant n$, one checks immediately that the right-hand side is a multiplicative function of $1 + p^\kappa t$.

Then, $\alpha \mapsto \theta\big(\alpha(p^\kappa t - \frac{1}{2}p^{2\kappa}t^2)/p^n\big)$ defines an injective homomorphism from $(\mathbb{Z}/p^{n-\kappa}\mathbb{Z})^\times$ to the group of characters of order $p^{n-\kappa}$ of the group $(1+p^\kappa\mathbb{Z})/(1+p^n\mathbb{Z})$, which is hence a surjection. In all our uses of (2.5), we will work under the assumption that $3\kappa \geqslant n+\iota'$; in such case, (2.5) follows from (2.2) or (2.3) with the same value of α. (We remark that, for a fixed $\kappa \geqslant 1$, an $\alpha \in \mathbb{Z}_p^\times$ can be found so that (2.3) and (2.5) hold with $\iota' = 0$ even when $p = 3$; however, such a value of α will depend on κ, and the notational complexities involved do not appear any more pleasant than our simple and from the point of view of the series expansion of $\log_p$ natural implement of setting $\iota' = 1$.)

Finally, for a Dirichlet character ψ modulo N, we denote by

$$\tau(\psi) = \sum_{h \bmod N} \psi(h) e\left(\frac{h}{N}\right)$$

the Gauß sum with $|\tau(\psi)| = \sqrt{N}$ if χ is primitive.

2.4. ***p*-adic square roots.** For every $x \in \mathbb{Z}_p^{\times 2}$, there are exactly two solutions to the solution $u^2 = x$; we now describe them more precisely. Recall that by Hensel's lemma (for p odd) $\mathbb{Z}_p^{\times 2}$ is the finite union of sets $r + p\mathbb{Z}_p$ over all square congruence classes $r \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}$. For every $x \in \mathbb{Z}_p^{\times 2}$ and every $\kappa \geqslant 1$, the congruence $u^2 \equiv x \pmod{p^\kappa}$ has exactly two solutions $\pm u \pmod{p^\kappa}$. These solutions come in two p-adic towers as $\kappa \to \infty$, whose limits are the two p-adic solutions to $u^2 = x$ which we alluded to and which we wish to denote as $\pm u_{1/2}(x)$.

More precisely, for every $r \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}$, there are exactly two classes $s \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that $s^2 = r$. Suppose we are given a choice function $s : (\mathbb{Z}/p\mathbb{Z})^{\times 2} \to (\mathbb{Z}/p\mathbb{Z})^\times$ such that, for every $r \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}$, the class $s(r) \in (\mathbb{Z}/p\mathbb{Z})^\times$ satisfies $s(r)^2 = r$. Then, for every $x \in \mathbb{Z}_p^{\times 2}$, we let $u_{1/2}(x) \in \mathbb{Z}_p^\times$ be the unique p-adic integer u such that $u^2 = x$ and $u \in s(x + p\mathbb{Z})$. In this way, each of the $2^{(p-1)/2}$ choices for $s : (\mathbb{Z}/p\mathbb{Z})^{\times 2} \to (\mathbb{Z}/p\mathbb{Z})^\times$ gives way to a unique function $u_{1/2} : \mathbb{Z}_p^{\times 2} \to \mathbb{Z}_p^\times$; we may think of these $2^{(p-1)/2}$ functions as p-adic square roots (or branches of the p-adic square root), and we will fix once and for all one of them. We also write $\pm x_{1/2}$ for $\pm u_{1/2}(x)$; for $k \in \mathbb{Z}$, by $x_{1/2}^k$ we always mean $(x_{1/2})^k$. Note that, for $\kappa \geqslant 1$, $u^2 \equiv x \pmod{p^\kappa}$ has solutions if and only if $x \in \mathbb{Z}_p^{\times 2}$, in which case the congruence holds if and only if $u \equiv \pm x_{1/2} \pmod{p^\kappa}$. Also, note that, for every $x, y \in \mathbb{Z}_p^{\times 2}$ and every $\kappa \geqslant 1$, $u_{1/2}(x) \equiv u_{1/2}(y) \pmod{p^\kappa}$ if and only if $x \equiv y \pmod{p^\kappa}$. Finally, $x/x_{1/2} = x_{1/2}$ and $(1/x_{1/2})^2 = 1/x$ for every $x \in \mathbb{Z}_p^{\times 2}$, simply because $x_{1/2}^2 = x$.

Next, we note that, for every $\kappa \geqslant 1$ and every $u \in \mathbb{Z}_p^{\times 2}$, $t \in \mathbb{Z}_p$,

$$\left(u_{1/2} + \frac{1}{2u_{1/2}}p^\kappa t - \frac{1}{8u_{1/2}^3}\cdot p^{2\kappa}t^2\right)^2 \in \big(u + p^\kappa t\big) + p^{3\kappa}\mathbb{Z}_p,$$

so that

$$\big(u + p^\kappa t\big)_{1/2} \equiv u_{1/2} + \frac{1}{2u_{1/2}}p^\kappa t - \frac{1}{8u_{1/2}^3}p^{2\kappa}t^2 \pmod{p^{3\kappa}}. \tag{2.6}$$

With the terminology of Definition 1, we claim that actually

$$\big(u + p^\kappa t\big)_{1/2} = u_{1/2} + \frac{1}{2u_{1/2}}p^\kappa t - \frac{1}{8u_{1/2}^3}p^{2\kappa}t^2 + \mathbf{M}_{p^{3\kappa}}[u, t], \tag{2.7}$$

again with $\Omega_0 = 1$ in Definition 1. Both equalities (2.6) and (2.7) can also be proved using a power series expansion as was done in Section 2.3 (since it is not hard to see that actually $(u + p^\kappa t)_{1/2} = u_{1/2}(1 + p^\kappa t/u)^{1/2}$, with the latter power given by the familiar power series expansion of $(1+x)^{1/2}$ for $x \in p\mathbb{Z}_p$), but we give a simple elementary proof of (2.7) instead. This equality contains all the p-adic local information we will require about the function $(\cdot)_{1/2}$.

Indeed, write (2.7) as $g = h + f$, where $f \in p^{3\kappa}\mathbb{Z}_p$, and, for $u' \in (1 + p^{\Omega}\mathbb{Z}_p)u$, $t' \in (1 + p^{\Omega}\mathbb{Z}_p)t'$, write the corresponding equality as $g' = h' + f'$, where $f' \in p^{3\kappa}\mathbb{Z}_p$; then we need to prove that $f' - f \in p^{3\kappa+\Omega}\mathbb{Z}_p$. Here, the function $(\cdot)_{1/2}$ is a fixed branch of the p-adic square-root, and, in particular, since $u + p^{\kappa}t \equiv u' + p^{\kappa}t'$ (mod p^{Ω}), we have that $g - g' \in p^{\Omega}\mathbb{Z}_p$. Then, $g^2 - h^2 = \frac{1}{8}p^{3\kappa}t^3/u^2 - \frac{1}{64}p^{4\kappa}t^2/u^3$ and so

$$\big(g^2 - h^2\big) - \big(g'^2 - h'^2\big) \in p^{3\kappa+\Omega}\mathbb{Z}_p.$$

Writing $h = g - f$ and $h' = g' - f'$, the above may be re-written as

$$2\big(gf - g'f'\big) - \big(f^2 - f'^2\big) = 2f\big(g - g'\big) + \big(f - f'\big)\big(2g' - f - f'\big) \in p^{3\kappa+\Omega}\mathbb{Z}_p.$$

In light of $f\big(g - g'\big) \in p^{3\kappa+\Omega}\mathbb{Z}_p$ and $2g' - f - f' \in \mathbb{Z}_p^{\times}$, it is immediate that $f - f' \in p^{3\kappa+\Omega}\mathbb{Z}_p$, as was to be proved.

2.5. **Automorphic forms.** We recall the Voronoi summation formula [22]:

Lemma 1. *Let D be a positive integer and ψ a character modulo D. Let g be a holomorphic newform of weight $\kappa + 1 \geqslant 1$ or a weight zero Maaß newform of spectral parameter $\kappa/2 \in [0, \infty) \cup (-i/2, i/2)$, level D and character ψ with Hecke eigenvalues $a_g(m)$. Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ with $(b, aD) = 1$. Let $h := g|_W$ where W is the classical Fricke involution of level D sending newforms of level D and character ψ to newforms of level D and character $\bar{\psi}$. Denote by $a_h(m)$ the Hecke eigenvalues of h. Let $F : (0, \infty) \to \mathbb{C}$ be a smooth, compactly supported function. Then*

$$\sum_{m \geqslant 1} a_g(m) e\left(\frac{a}{b}m\right) F(m) = \sum_{\pm} \frac{\psi(\mp b)}{b\sqrt{D}} \sum_{m \geqslant 1} a_h(m) e\left(\mp\frac{\overline{aD}}{b}m\right) \int_0^{\infty} F(x)\mathcal{J}_{\kappa}^{\pm}\left(\frac{4\pi\sqrt{mx}}{b\sqrt{D}}\right) dx$$

where

$$\mathcal{J}_{\kappa}^{+}(x) = \begin{cases} 2\pi i^{\kappa+1} J_{\kappa}(x), & g \text{ holomorphic of weight } \kappa + 1, \\ i\pi \frac{J_{i\kappa}(x) - J_{-i\kappa}(x)}{\sinh(\pi\kappa/2)}, & g \text{ Maaß with spectral parameter } \kappa/2, \end{cases}$$

and

$$\mathcal{J}_{\kappa}^{-}(x) = \begin{cases} 0, & g \text{ holomorphic of weight } \kappa + 1, \\ i\pi \frac{I_{i\kappa}(x) - I_{-i\kappa}(x)}{\sinh(\pi\kappa/2)} = 4\cosh(\pi\kappa/2)K_{i\kappa}(x), & g \text{ Maaß with spectral parameter } \kappa/2. \end{cases}$$

The Selberg eigenvalue conjecture (known for $\mathrm{SL}_2(\mathbb{Z})$) implies $\kappa \in \mathbb{R}$, but we will only use the "trivial bound" $|\Im\kappa| < 1/2$.

We are interested in the special case when $g = f \otimes \chi$ for a newform f of level 1 and χ a primitive character modulo N. Then g is a newform of level N^2 and character χ^2 (see [18, Prop. 14.20]), and a matrix computation shows (see [17, Theorem 7.5]) that $h = (\tau(\chi)^2/N)\bar{g}$. Hence we conclude that, under the above assumptions,

$$\begin{aligned} &\sum_{m} a_f(m)\chi(m) e\left(\frac{a}{b}m\right) F(m) \\ &\quad = \frac{\tau(\chi)^2}{N} \cdot \frac{\chi^2(b)}{bN} \sum_{\pm} \sum_{m} a_f(m)\bar{\chi}(m) e\Big(\mp\frac{\overline{aN^2}}{b}m\Big) \int_0^{\infty} F(x)\mathcal{J}_{\kappa}^{\pm}\left(\frac{4\pi\sqrt{mx}}{bN}\right) dx \end{aligned} \tag{2.8}$$

(note that f has real coefficients because it has trivial central character). We will frequently use the Rankin-Selberg bound

$$\sum_{m \leqslant x} |a_f(m)|^2 \ll_f x. \tag{2.9}$$

2.6. **Bessel functions.** We start with the bound

$$\mathcal{J}_\kappa^{\pm}(x) \ll_\kappa \begin{cases} x^{-|\Im\kappa|}(1+|\log x|), & 0 < x \leqslant 1, \\ x^{-1/2}, & x \geqslant 1, \end{cases}$$

for $\kappa \in \mathbb{C}$, which follows from the power series expansion [13, 8.402.1, 8.445] for $x \leqslant 1$ and from the asymptotic formula [13, 8.451] for $x > 1$. Integration by parts in combination with [13, 8.472.3, 8.486.14] shows the formula

$$\int_0^\infty F(x) B_s(\alpha\sqrt{x})dx = \left(\pm\frac{2}{\alpha}\right)^j \int_0^\infty \frac{\partial^j}{\partial x^j}(F(x)x^{-s/2})x^{(s+j)/2}B_{s+j}(\alpha\sqrt{x})dx$$

for $B_s \in \{J_s, Y_s, K_s\}$, $\alpha > 0$, $s \in \mathbb{C}$, $j \in \mathbb{N}$ and $F : (0,\infty) \to \mathbb{C}$ smooth and of compact support. Here, the $+$ sign applies for K_s, and the $-$ sign applies for J_s and Y_s. In particular, if F has support in the interval $[M, 2M]$, and $F^{(j)} \ll_j M^{-j}Z_0^j$ for some $Z_0 \geqslant 1$ and all $j \in \mathbb{N}_0$, then

$$\int_0^\infty F(x)\mathcal{J}_\kappa^{\pm}(\alpha\sqrt{x})dx \ll_{j,\kappa} M\left(1+\frac{1}{\sqrt{M}\alpha}\right)^{j+|\Im\kappa|+\varepsilon}\left(\frac{Z_0}{\sqrt{M}\alpha}\right)^j. \tag{2.10}$$

Finally we record the representation

$$\mathcal{J}_\kappa^{\pm}(x) = e^{ix}\Omega_\kappa^{\pm}(x) + e^{-ix}\overline{\Omega}_\kappa^{\pm}(x) \tag{2.11}$$

for a smooth and non-oscillating function $\Omega_\kappa^{\pm}$, i.e.

$$x^j(\Omega_\kappa^{\pm})^{(j)}(x) \ll_{j,\kappa} \begin{cases} x^{-|\Im\kappa|}(1+|\log x|), & 0 < x \leqslant 1, \\ x^{-1/2}, & x \geqslant 1, \end{cases} \tag{2.12}$$

for all $j \in \mathbb{N}_0$. This follows as in [19, Section 4] (where Ω_κ^+ is given explicitly) in the $+$-case, and it follows trivially with $\Omega_\kappa^-(x) = e^{-ix}\mathcal{J}_\kappa^-(x)/2$ from the rapid decay of the K-function in the other case.

In our applications of (2.10) and (2.12), we will have $|\Im\kappa| < 1/2$ by the trivial bounds towards the Selberg eigenvalue conjecture.

3. Proof of Theorem 3

To keep notation simple, we prove the theorem in the case $r \geqslant 0$. The proof in the case $r < 0$ is along exactly the same lines, *mutatis mutandis*, by switching the roles of a and b.

First, we claim that, for any two $(a_1, b_1, k_1), (a_2, b_2, k_2) \in S$, with $k_1 \leqslant k_2$, exactly one of the following two situations occurs:

(1) $a_1/b_1 - a_2/b_2 \notin p^{\ell+r+k_1}\mathbb{Z}_p$, and $\mathbb{Z}_p^\times[a_1, b_1, k_1] \cap \mathbb{Z}_p^\times[a_2, b_2, k_2] = \emptyset$, or

(2) $a_1/b_1 - a_2/b_2 \in p^{\ell+r+k_1}\mathbb{Z}_p$, and $\mathbb{Z}_p^\times[a_2, b_2, k_2] \subseteq \mathbb{Z}_p^\times[a_1, b_1, k_1]$, with set equality if and only if $k_1 = k_2$.

For suppose that $a_1/b_1 - a_2/b_2 \notin p^{\ell+r+k_1}\mathbb{Z}_p$, and that $m \in \mathbb{Z}_p^\times[a_1, b_1, k_1] \cap \mathbb{Z}_p^\times[a_2, b_2, k_2]$. Then $\alpha/m - a_1/b_1 \in p^{\ell+r+k_1}\mathbb{Z}_p$, and $\alpha/m - a_2/b_2 \in p^{\ell+r+k_2}\mathbb{Z}_p \subseteq p^{\ell+r+k_1}\mathbb{Z}_p$, since $k_1 \leqslant k_2$. It follows that $a_1/b_1 - a_2/b_2 \in p^{\ell+r+k_1}\mathbb{Z}_p$; contradiction. Hence, if $a_1/b_1 - a_2/b_2 \notin p^{\ell+r+k_1}\mathbb{Z}_p$, then $\mathbb{Z}_p^\times[a_1, b_1, k_1] \cap \mathbb{Z}_p^\times[a_2, b_2, k_2] = \emptyset$, i.e. (1) holds.

On the other hand, suppose that $a_1/b_1 - a_2/b_2 \in p^{\ell+r+k_1}\mathbb{Z}_p$, and let $m_2 \in \mathbb{Z}_p^\times[a_2, b_2, k_2]$ be arbitrary. Then $m_2 \in \mathbb{Z}_p^\times$ and $\alpha/m_2 - a_2/b_2 \in p^{\ell+r+k_2}\mathbb{Z}_p \subseteq p^{\ell+r+k_1}\mathbb{Z}_p$, since $k_1 \leqslant k_2$, and therefore $\alpha/m_2 - a_1/b_1 = (\alpha/m_2 - a_2/b_2) + (a_2/b_2 - a_1/b_1) \in p^{\ell+r+k_1}\mathbb{Z}_p$ too, so that $m_2 \in \mathbb{Z}_p^\times[a_1, b_1, k_1]$. This proves that, if $a_1/b_1 - a_2/b_2 \in p^{\ell+r+k_1}\mathbb{Z}_p$, then $\mathbb{Z}_p^\times[a_2, b_2, k_2] \subseteq \mathbb{Z}_p^\times[a_1, b_1, k_1]$, i.e. the first statement of (2) holds. If $k_1 = k_2$, then the reverse inclusion also holds, and so $\mathbb{Z}_p^\times[a_1, b_1, k_1] = \mathbb{Z}_p^\times[a_2, b_2, k_2]$. If $k_1 < k_2$, then, letting $m_2 \in \mathbb{Z}_p^\times[a_2, b_2, k_2]$ be arbitrary (for example, $m_2 = \alpha b_2/a_2$), we have that $m_2 + p^{\ell+r+k_1} \in \mathbb{Z}_p^\times[a_1, b_1, k_1] \setminus \mathbb{Z}_p^\times[a_2, b_2, k_2]$, so that $\mathbb{Z}_p^\times[a_2, b_2, k_2] \subsetneq \mathbb{Z}_p^\times[a_1, b_1, k_1]$. This completes the proof of (2).

It is clear that (1) and (2) are mutually exclusive.

Let $S_k = \{(a,b) \mid (a,b,k) \in S\}$. We now inductively construct a set $S_k^0 \subseteq S_k$ as follows. Consider the relation $\sim_0$ on S_0 defined for $(a_1,b_1),(a_2,b_2) \in S_0$ as

$$(a_1,b_1) \sim_0 (a_2,b_2) \iff a_1/b_1 - a_2/b_2 \in p^{\ell+r}\mathbb{Z}_p.$$

This is clearly an equivalence relation. We let S_0^0 be a set of unique representatives of the equivalence classes of $\sim_0$. Suppose the sets S_κ^0 have been constructed for all $0 \leqslant \kappa < k$. Let

$$S_k^\sharp = \{(a,b) \in S_k : a/b - a_1/b_1 \notin p^{\ell+r+\kappa}\mathbb{Z}_p \text{ for every } 0 \leqslant \kappa < k,\ (a_1,b_1) \in S_\kappa^0\}.$$

Consider the relation $\sim_k$ on $S_k^\sharp$ defined for $(a_1,b_1),(a_2,b_2) \in S_k^\sharp$ as

$$(a_1,b_1) \sim_k (a_2,b_2) \iff a_1/b_1 - a_2/b_2 \in p^{\ell+r+k}\mathbb{Z}_p.$$

Again, this is clearly an equivalence relation. We let S_k^0 be a set of unique representatives of the equivalence classes of $\sim_k$. Proceeding inductively, we can construct sets $S_0^0, S_1^0, \ldots, S_{\ell-r}^0$. Let

$$S^0 = \{(a,b,k) : 0 \leqslant k \leqslant \ell - r,\ (a,b) \in S_k^0\}.$$

We are now ready to prove the statements made in the lemma. We first prove that the union in (1.9) is disjoint. Suppose that the sets $\mathbb{Z}_p^\times[a_1,b_1,k_1]$ and $\mathbb{Z}_p^\times[a_2,b_2,k_2]$ are not disjoint, for some $(a_1,b_1) \in S_{k_1}^0$, $(a_2,b_2) \in S_{k_2}^0$, $(a_1,b_1,k_1) \neq (a_2,b_2,k_2)$, and (without loss of generality) $k_1 \leqslant k_2$. According to (1) and (2) above, we must have $a_1/b_1 - a_2/b_2 \in p^{\ell+r+k_1}\mathbb{Z}_p$. If $k_1 = k_2$, then $(a_1,b_1) \sim_{k_1} (a_2,b_2)$; however, this is impossible in light of $(a_1,b_1) \neq (a_2,b_2)$ and the construction of $S_{k_1}^0$ as a system of unique representatives of equivalence classes of $\sim_{k_1}$. On the other hand, if $k_1 < k_2$, then, since $(a_1,b_1) \in S_{k_1}^0$, we have that $(a_2,b_2) \notin S_{k_2}^\sharp$, so we certainly cannot have $(a_2,b_2) \in S_{k_2}^0$ – a contradiction.

We proceed to prove that the disjoint union of subsets of $\mathbb{Z}_p^\times$ on the right-hand side of (1.9) indeed equals the entire set $\mathbb{Z}_p^\times$. Let $m \in \mathbb{Z}_p^\times$ be given, and consider the following elements of $\mathbb{Z}_p$:

$$A(a,b) = b\alpha - ma, \quad 0 < a \leqslant p^{\ell+r},\ 0 \leqslant b \leqslant p^{\ell-r}.$$

This gives us $p^{\ell+r}(p^{\ell-r}+1) > p^{2\ell}$ numbers in $\mathbb{Z}_p$. Since $|\mathbb{Z}_p/p^{2\ell}\mathbb{Z}_p| = p^{2\ell}$, there must be two distinct $(a_1,b_1) \neq (a_2,b_2)$ with $0 < a_i \leqslant p^{\ell+r}$, $0 \leqslant b_i \leqslant p^{\ell-r}$ and (without loss of generality) $b_1 \leqslant b_2$ such that $A(a_2,b_2) - A(a_1,b_1) \in p^{2\ell}\mathbb{Z}_p$, that is,

$$(b_2 - b_1)\alpha - m(a_2 - a_1) \in p^{2\ell}\mathbb{Z}_p.$$

We note right away that we cannot have $b_1 = b_2$, since then $p^{2\ell} \mid (a_2 - a_1)$. Along with $|a_2 - a_1| < p^{\ell+r} \leqslant p^{2\ell}$, this would imply that $a_1 = a_2$, so that $(a_1,b_1) = (a_2,b_2)$, a contradiction.

So let $b_2 - b_1 = p^s\tilde{b}$ for some $s \geqslant 0$ and $\tilde{b} \in \mathbb{N}$ with $(p,\tilde{b}) = 1$. Since $0 < b_2 - b_1 \leqslant b_2 \leqslant p^{\ell-r}$, we have that $s \leqslant \ell - r$, and in particular $s < 2\ell$. It follows that we must have $p^s \mid (a_2 - a_1)$; let $a_2 - a_1 = p^s\tilde{a}$ for some $\tilde{a} \in \mathbb{Z}$. We note that $0 < \tilde{b} \leqslant p^{\ell-r-s}$ and $|\tilde{a}| < p^{\ell+r-s}$. We find that

$$p^s\tilde{b}\alpha - mp^s\tilde{a} \in p^{2\ell}\mathbb{Z}_p$$

and hence

$$\tilde{b}\alpha - m\tilde{a} \in p^{2\ell-s}\mathbb{Z}_p,$$

$$\alpha - m\tilde{a}/\tilde{b} \in p^{2\ell-s}\mathbb{Z}_p.$$

Moreover, since $\alpha \in \mathbb{Z}_p^\times$, it follows that $\tilde{a} \in \mathbb{Z}_p^\times$ too, that is, $(\tilde{a},p) = 1$. Recall that $\tilde{a}$ and $\tilde{b}$ are usual integers. Let $d \geqslant 1$ be their (positive) greatest common divisor, let $a = \tilde{a}/d$, and let $b = \tilde{b}/d$; note that $(d,p) = 1$ and that $1/b = d/\tilde{b}$, and so

$$\alpha - ma/b \in p^{2\ell-s}\mathbb{Z}_p,$$

with $b \in \mathbb{N}$, $b \leqslant p^{\ell-r-s}$, $|a| < p^{\ell+r-s}$, and $(a,b) = (a,p) = (b,p) = 1$.

Letting $k = \ell - r - s$, we have that $(a, b) \in S_k$ and

$$m \in \mathbb{Z}_p^\times[a, b, k].$$

Let

$$S' = \{\kappa \in \mathbb{N}_0 : \mathbb{Z}_p^\times[a', b', \kappa] \cap \mathbb{Z}_p^\times[a, b, k] \neq \emptyset \quad \text{for some } (a', b') \in S_\kappa\}.$$

Clearly $k \in S'$; let $\kappa_0 = \min S'$, so that $\kappa_0 \leqslant k$, and let $(a', b') \in S_{\kappa_0}$ be such that $\mathbb{Z}_p^\times[a', b', \kappa_0] \cap \mathbb{Z}_p^\times[a, b, k] \neq \emptyset$. According to (1) and (2) above, we have that $\mathbb{Z}_p^\times[a, b, k] \subseteq \mathbb{Z}_p^\times[a', b', \kappa_0]$, and, in particular,

$$m \in \mathbb{Z}_p^\times[a', b', \kappa_0].$$

We claim that, if $\kappa_0 \geqslant 1$, then $(a', b') \in S^\sharp_{\kappa_0}$. For if this were not the case, we would have that $a''/b'' - a'/b' \in p^{\ell+r+\kappa}\mathbb{Z}_p$ for some $0 \leqslant \kappa < \kappa_0$, $(a'', b'') \in S^0_\kappa$. But then, according to (2), $\mathbb{Z}_p^\times[a', b', \kappa_0] \subseteq \mathbb{Z}_p^\times[a'', b'', \kappa]$, so that $\kappa \in S'$, contradicting the minimality of κ_0. This implies $\kappa_0 = 0$ or $(a', b') \in S^\sharp_{\kappa_0}$. In any case, since $S^0_{\kappa_0}$ is a full set of unique representatives of $\sim_{\kappa_0}$, we must have $(a', b') \sim_{\kappa_0} (a'_0, b'_0)$ for some $(a'_0, b'_0) \in S^0_{\kappa_0}$. But then, according to (2), $\mathbb{Z}_p^\times[a', b', \kappa_0] = \mathbb{Z}_p^\times[a'_0, b'_0, \kappa_0]$, so that

$$m \in \mathbb{Z}_p^\times[a'_0, b'_0, \kappa_0]$$

with $(a'_0, b'_0, \kappa_0) \in S^0$. This shows that an arbitrary $m \in \mathbb{Z}_p^\times$ is included in the union on the right-hand side of (1.9). This completes the proof of (1.9).

The final claim of Theorem 3 is immediate, for if, say, $k_1 < k_2$, then $a/b - a/b \in p^{\ell+r+k_1}\mathbb{Z}_p$ with $(a, b) \in S^0_{k_1}$, so that $(a, b) \notin S^\sharp_{k_2}$ and so a fortiori $(a, b) \notin S^0_{k_2}$. □

4. A sketch of Jutila's method

In this section we give a very brief sketch of Jutila's method [20] for bounding (1.3), ignoring all technicalities. We use a lot of imprecise notation and suppress in particular smooth weight functions and ε's. The full proof with all details can be found in [20], but we hope that the following sketch can guide the reader through the argument.

Let $a(m)$ denote the Fourier coefficients of f and consider (a smoothed version of)

$$L := \sum_{m \asymp M} a(m) m^{2\pi i t} = \sum_{m \asymp M} a(m) e(t \log m)$$

where $t^{2/3} \ll M \ll t$ (for smaller M we estimate trivially, for bigger M we use the functional equation).

Step 1: Farey Dissection. Let $\rho = a/b \asymp t/M$ be a typical rational number with $b \asymp B$, $a \asymp tB/M$. We consider intervals I_ρ centered at t/ρ of length $\approx M/(AB)$. These AB intervals cover $[M, 2M]$. This gives

$$L \approx \sum_\rho \sum_{m \in I_\rho} a(m) e(t \log m).$$

A Taylor expansion about t/ρ suggests to re-write this as

$$\sum_\rho \sum_{m \in I_\rho} a(m) e(m\rho) e(t \log m - m\rho).$$

Step 2: Voronoi summation. We apply Voronoi summation to the inner sum:

$$\sum_{m \in I_\rho} a(m) e(m\rho) e(t \log m - m\rho) \approx \frac{1}{b} \sum_m a(m) e(m\bar{\rho}) \int_{I_\rho} e(t \log x - x\rho) \mathcal{J}_\kappa\left(\frac{4\pi\sqrt{mx}}{b}\right) dx$$

Let us assume that

$$MB^{-2} \gg t^{1/2}, \tag{4.1}$$

so that one can run a stationary phase argument. We recall our assumption that all sums and integrals are understood to be smooth. After some moderately pleasant computation one obtains

$$\int_{I_\rho} e(t\log x - x\rho)\mathcal{J}_\kappa\left(4\pi\frac{\sqrt{mx}}{b}\right)dx \approx \delta_{m\asymp MB^{-2}} B(M/t)^{1/2}\cdot\rho^{-2\pi it} e\left(t\phi\left(\frac{m}{4abt}\right)\right)$$

with $\phi(x) = \operatorname{arcsinh}(x^{1/2}) + (x+x^2)^{1/2} - x$. Substituting back, we obtain

$$L \approx \frac{M^{1/2}}{t^{1/2}}\sum_\rho \rho^{-2\pi it}\sum_{m\asymp MB^{-2}} a(m)e(m\bar\rho)e\left(t\phi\left(\frac{m}{4abt}\right)\right).$$

Since the sum over ρ contains tB^2/M terms, a trivial estimate returns $(Mt)^{1/2}$ which at most recovers the trivial bound, but we can hope to exploit cancellation in the ρ-sum. This is the purpose of the next two steps.

Step 3: Cauchy-Schwarz inequality. By Cauchy-Schwarz and a standard Rankin-Selberg mean value bound for $a(m)$, we get

$$L \ll \frac{M}{t^{1/2}B}\Big\{\sum_{\rho_1,\rho_2}\left(\frac{\rho_1}{\rho_2}\right)^{-2\pi it}\sum_{m\asymp MB^{-2}} e\left(m\left(\frac{\bar a_1}{b_1}-\frac{\bar a_2}{b_2}\right)+t\phi\left(\frac{m}{a_1b_1t}\right)-t\phi\left(\frac{m}{a_2b_2t}\right)\right)\Big\}^{1/2}.$$

Step 4: Bounding exponential sums. For $\rho_1\neq\rho_2$ we treat the m-sum by van der Corput's technique, see e.g. [IK, Corollary 8.13]), while for $\rho_1=\rho_2$ we estimate trivially. In this way we obtain

$$L \ll \frac{M}{B} + t^{1/2}B^{1/2}M^{1/4} \ll M^{1/2}t^{1/3}$$

upon choosing $B = M^{1/2}/t^{1/3}$ which is in agreement with (4.1). This is non-trivial for $M \geqslant t^{2/3+\delta}$.

An inspection of the method shows that it works for more general sums

$$\sum_{m\asymp M} a(m)e(f_t(m))$$

where $f_t'(m)\asymp t/M$, $f_t''(m)\asymp t/M^2$ and $f_t^{(j)}(m)\ll t/M^j$ for $j\geqslant 3$.

5. Proofs of Theorems 1 and 2

5.1. **General ranges, assumptions, and notation.** Already in the introduction we mentioned that the critical range for applications of Theorem 1 is $M\approx Zq$, and that, for larger M, one can reduce the length of the sum to about Z^2q^2/M. We now make this more precise. By Mellin inversion and the functional equation of $L(f\otimes\chi,s)$ we have

$$\sum_m a(m)\chi(m)W\left(\frac{m}{M}\right) = \eta\sum_m a(m)\bar\chi(m)\tilde W\left(\frac{m}{q^2Z^2/M}\right),$$

where $\eta=\eta(\chi)$ is a constant of absolute value 1, and

$$\tilde W(x) = \frac{1}{2\pi i}\int_{(c)}\frac{L_\infty(f,s)}{L_\infty(f,1-s)}\widehat{W}(1-s)(Z^2x)^{-s}ds,$$

where $\widehat W(s)$ is the Mellin transform of W. It is easy to see that $\widehat W(s)\ll_{\Re s,A}(1+|s|/Z)^{-A}$ for any $A\geqslant 0$, and hence by Stirling's formula

$$\tilde W^{(j)}(x)\ll_{c,f,j} x^{-c}\left(\frac{Z}{x}\right)^j$$

for any $c>0$ and $j\in\mathbb{N}_0$. In particular, choosing a smooth partition of unity, we find that

$$\sum_m a(m)\chi(m)W\left(\frac{m}{M}\right) = \eta\sum_{R=2^\nu}\sum_m a(m)\bar\chi(m)\Phi_R\left(\frac{m}{R}\right)$$

for smooth, compactly supported functions Φ_R satisfying

$$\Phi_R^{(j)} \ll_{j,c} \left(\frac{R}{q^2Z^2/M}\right)^{-c} Z^j$$

for any $c > 0$ and $j \in \mathbb{N}_0$. In particular, by choosing c sufficiently large, we can assume that $R \leqslant (q^2Z^2/M)^{1+\varepsilon}$, and, for those R, we choose $c = \varepsilon$ in the preceding estimate and apply Theorem 1 with Φ_R in place of W. The upshot is that in the situation of Theorem 1 we can assume without loss of generality that

$$M \leqslant (qZ)^{1+\varepsilon}. \tag{5.1}$$

We recall the set-up and our general assumptions that will be in force for the rest of the paper. Let $\alpha \in \mathbb{Z}_p^\times$ be such that (2.2) holds for the character χ modulo $q = p^n$ in Theorem 1. (As pointed out in Section 2.3, we will only use the corollary (2.3) in our arguments.) We fix a positive integer ℓ and a parameter r with $|r| \leqslant \ell$. At the end of the proof of Theorem 1, in Section 5.5 in (5.18) and (5.19), we will optimize ℓ and r. At this point, we only assume

$$\ell < n/4. \tag{5.2}$$

In view of (5.2), (5.1), and (1.4), we may and will assume without loss of generality that

$$n \geqslant 5 \quad \text{and} \quad Z^5p^{7/3}q^{2/3} \leqslant M \leqslant (qZ)^{1+\varepsilon}, \quad \text{in particular} \quad M \leqslant \min(q^2, Zq^{4/3}). \tag{5.3}$$

Other than $n \geqslant 5$, much of our argument until the final choice of parameters in Section 5.5 is in fact insensitive to the precise form of the conditions (5.3) and requires only that $Z \ll M^A$ and $M \ll q^A$ for some large constant $A > 0$; we list them here since their concrete form imparts no loss while simplifying the writeup.

5.2. **Splitting into arithmetic progressions and harmonic analysis.** Jutila's method succeeds by decomposing the m-sum into short intervals, in which the derivative t/m of the archimedean phase $t \log m$ is well-approximated by a rational number a/b. We begin our argument by using Theorem 3 with the values of α, ℓ, and r specified in Section 5.1, and obtain a set S^0 of triples (a, b, k) inducing the partition (1.9) of $\mathbb{Z}_p^\times$ into sets $\mathbb{Z}_p^\times[a, b, k]$, in which the derivative of the non-archimedean phase is very well p-adically approximated by $a/b = a\bar{b}$, and whose intersections with $\mathbb{Z}$ are arithmetic progressions of difference $p^{\ell+|r|+k}$. Corresponding to this partition, we can decompose

$$L = \sum_{s=(a,b,k)\in S^0} \sum_{m\in\mathbb{Z}\cap\mathbb{Z}_p^\times[a,b,k]} a(m)\chi(m)W\left(\frac{m}{M}\right) = \sum_{s=(a,b,k)\in S^0} L_s,$$

where

$$L_s = \sum_m a(m)f_s(m)e\left(\frac{a\bar{b}}{p^n}m\right)W\left(\frac{m}{M}\right)$$

and, for every $m \in \mathbb{Z}$,

$$f_s(m) = \begin{cases} \chi(m)\theta\left(-\frac{a\bar{b}}{p^n}m\right), & m \in \mathbb{Z}_p^\times[a, b, k], \\ 0, & \text{else}. \end{cases} \tag{5.4}$$

In other words, keeping in mind that $0 \leqslant k \leqslant \ell - |r|$ for all $(a, b, k) \in S^0$, we split the original sum into arithmetic progressions of moduli between $p^{\ell+|r|}$ and $p^{2\ell}$. It is convenient to split the sum over s further into $O(\log^3 q)$ pieces according to the size of a and b. We have

$$L \ll q^\varepsilon \max_{\substack{0\leqslant k\leqslant \ell-|r| \\ A\leqslant \frac{1}{2}p^{k+2r^+} \\ B\leqslant \frac{1}{2}p^{k+2r^-}}} |L_{A,B,k}|, \qquad L_{A,B,k} := \sum_{\substack{s=(a,b,k)\in S^0 \\ A\leqslant |a|\leqslant 2A \\ B\leqslant b\leqslant 2B}} L_s. \tag{5.5}$$

In light of (5.5), a good bound for every individual $L_{A,B,k}$ will be satisfactory for Theorem 1. We keep A,B,k fixed for the rest of this section.

It is important to observe that, for every $s=(a,b,k)\in S^0$, the function f_s defined by (5.4) is periodic modulo $p^{n-\ell-|r|-k}$. Indeed, in light of (5.2) and $k\leqslant \ell-|r|$, we have $n-\ell-|r|-k>n-2(n/4)=n/2$, so that (2.5) gives, for every $m\in\mathbb{Z}_p^\times[a,b,k]$ and $\mu\in\mathbb{Z}$,

$$\begin{aligned} f_s\big(m+p^{n-\ell-|r|-k}\mu\big) &= \chi\big(m+p^{n-\ell-|r|-k}\mu\big)\theta\left(-\frac{a/b}{p^n}\big(m+p^{n-\ell-|r|-k}\mu\big)\right) \\ &= \chi(m)\theta\left(-\frac{a/b}{p^n}m\right)\chi\big(1+p^{n-\ell-|r|-k}\bar{m}\mu\big)\theta\left(-\frac{a/b}{p^n}p^{n-\ell-|r|-k}\mu\right) \\ &= f_s(m)\theta\left(\frac{(\alpha/m-a/b)\mu}{p^{\ell+|r|+k}}\right). \end{aligned}$$

According to the definition of $\mathbb{Z}_p^\times[a,b,k]$, we have that $\alpha/m-a/b\in p^{\ell+|r|+k}\mathbb{Z}_p$; this clearly implies that $f_s\big(m+p^{n-\ell-|r|-k}\mu\big)=f_s(m)$. In particular, $f_s\big(m+p^{n-\ell-|r|-k}\mu\big)\neq 0$ if and only if $f_s(m)\neq 0$, and so $m+p^{n-\ell-|r|-k}\mu\in\mathbb{Z}_p^\times[a,b,k]$ if and only if $m\in\mathbb{Z}_p^\times[a,b,k]$. (The latter is also immediate from $\ell+|r|+k\leqslant n-\ell-|r|-k$.)

For a Dirichlet character ψ modulo $p^{n-\ell-|r|-k}$, denote

$$\widehat{f}_s(\psi) := \sum_{m \bmod p^{n-\ell-|r|-k}} f_s(m)\bar{\psi}(m). \tag{5.6}$$

Then, we have that

$$f_s(m)=\frac{\delta_p}{p^{n-\ell-|r|-k}}\sum_{\psi \bmod p^{n-\ell-|r|-k}}\widehat{f}_s(\psi)\psi(m),$$

where $\delta_p=(1-p^{-1})^{-1}$. Hence we may write

$$L_s=\frac{\delta_p}{p^{n-\ell-|r|-k}}\sum_{0\leqslant c\leqslant n-\ell-|r|-k}L_{s,c},$$

where

$$L_{s,c}=\sum_{\substack{\psi \bmod p^{n-\ell-|r|-k}\\ \operatorname{cond}\psi=p^c}}\widehat{f}_s(\psi)\sum_m a(m)\psi(m)e\bigg(-\frac{a\overline{p^n}}{b}m\bigg)e\left(\frac{a}{bp^n}m\right)W\left(\frac{m}{M}\right); \tag{5.7}$$

here we employed the well-known reciprocity formula for the exponential: $e(a\bar{u}/v)e(a\bar{v}/u)=e(a/uv)$ for every $a\in\mathbb{Z}$, $(u,v)=1$.

5.3. **Voronoi summation and stationary phase evaluation.** We are now prepared for the second step of Jutila's method, the application of the Voronoi formula (2.8) to the inner sum in (5.7), with $N=p^c$ and $F(m)=e\big(\frac{a}{bp^n}m\big)W\left(\frac{m}{M}\right)$.

For technical reasons it is convenient to estimate the contribution of $c\leqslant 1$ separately. In this case, ψ is periodic modulo p, and hence

$$\psi(m)e\left(-\frac{a\overline{p^n}}{b}m\right)=\sum_{\xi \bmod p}\beta(\xi)e\left(\left(\frac{\xi}{p}-\frac{a\overline{p^n}}{b}\right)m\right)$$

for certain complex numbers $\beta(\xi)$ satisfying $\sum|\beta(\xi)|^2\leqslant p$. We write $\xi/p-a\overline{p^n}/b=y/w$ with $w\leqslant pb$ in lowest terms and apply the Voronoi formula (Lemma 1 with $D=1$, $b=w$) to the m-sum in (5.7) obtaining

$$\sum_{\xi \bmod p}\beta(\xi)\frac{1}{w}\sum_{m\geqslant 1}a(m)e\left(\mp\frac{\bar{y}}{w}m\right)\int_0^\infty e\left(\frac{a}{bp^n}x\right)W\left(\frac{x}{M}\right)\mathcal{J}_\kappa^\pm\left(\frac{4\pi\sqrt{mx}}{w}\right)dx$$

for the m-sum in (5.7). By (2.10) with $Z_0 = Z + AM/(Bp^n)$ and the size condition on A, B, k in (5.5), the above expression is

$$\ll \sum_{\xi \bmod p} |\beta(\xi)| \frac{1}{w} \sum_{m \geqslant 1} |a(m)| M \left(1 + \frac{w}{\sqrt{Mm}}\right)^{j+\frac{1}{2}} \left(\frac{(Z + AM/(Bp^n))w}{\sqrt{Mm}}\right)^j$$
$$\ll Mp \left(1 + \frac{p^{1+\ell-r}}{\sqrt{M}}\right)^{j+\frac{1}{2}} \left(\frac{Zp^{1+\ell-r}}{\sqrt{M}} + \frac{p^{1+\ell+r}\sqrt{M}}{p^n}\right)^j$$

for any $j \geqslant 3$. Here we used $-|r| + 2r^{\pm} = \pm r$. Summing this over characters ψ with conductor dividing p as in (5.7) and using the trivial bound $|\widehat{f}_s(\psi)| \leqslant p^{n-2(\ell+|r|+k)}$, the total contribution of these characters to L_s is at most

$$E := Mp^{2-(\ell+|r|+k)} \left(1 + \frac{p^{1+\ell-r}}{\sqrt{M}}\right)^{j+\frac{1}{2}} \left(\frac{Zp^{1+\ell-r}}{\sqrt{M}} + \frac{p^{1+\ell+r}\sqrt{M}}{p^n}\right)^j \tag{5.8}$$

for any $j \geqslant 3$. Our choice of parameters will imply that E is very small; we return to this point in (5.20). From now on, we assume that $c \geqslant 2$ and observe that in this case ψ coincides with its underlying primitive character as an arithmetic function on the integers.

For $c \geqslant 2$, we apply (2.8) to the inner sum in (5.7) getting

$$L_{s,c} = \sum_{\substack{\psi \bmod p^{n-\ell-|r|-k} \\ \text{cond}\, \psi = p^c}} \widehat{f}_s(\psi) \cdot \frac{\psi^2(b)}{p^c b} \cdot \frac{\tau(\psi)^2}{p^c} \sum_{m \geqslant 1} a(m) \bar{\psi}(m) e\Big(\frac{\bar{a}p^n\overline{p^{2c}}}{b} m\Big) \mathcal{I}_{s,c}(m),$$

with

$$\mathcal{I}_{s,c}(m) = \int_0^\infty W\left(\frac{x}{M}\right) e\left(\frac{a}{bp^n}x\right) \mathcal{J}_\kappa^{\pm}\left(\frac{4\pi\sqrt{mx}}{bp^c}\right) dx, \tag{5.9}$$

and hence

$$L_s = \frac{\delta_p}{p^{n-\ell-|r|-k}} \sum_{2 \leqslant c \leqslant n-\ell-|r|-k} \frac{1}{p^c b} \sum_{m \geqslant 1} a(m) e\Big(\frac{\bar{a}p^n\overline{p^{2c}}}{b} m\Big) \cdot \mathcal{I}_{s,c}(m) \cdot \mathcal{L}_{s,c}(m) + O(E), \tag{5.10}$$

where

$$\mathcal{L}_{s,c}(m) = \sum_{\substack{\psi \bmod p^c \\ \psi \text{ primitive}}} \frac{\tau(\psi)^2}{p^c} \psi(b^2 \bar{m}) \widehat{f}_s(\psi). \tag{5.11}$$

We need to analyze the integral $\mathcal{I}_{s,c}$ and the character sum $\mathcal{L}_{s,c}$. The integral $\mathcal{I}_{s,c}$ will be computed by an (archimedean) stationary phase argument, while the character sum $\mathcal{L}_{s,c}$ will be evaluated by an involved non-archimedean stationary phase computation. This is the content of the following two lemmas, whose proof we postpone to the next two sections. We recall the general notation at the beginning of this section and in particular the conditions (5.2) and (5.3).

Lemma 2. *Let $s = (a, b, k) \in S^0$ be such that $A \leqslant |a| \leqslant 2A$, $B \leqslant b \leqslant 2B$. Let $m \geqslant 1$ and $2 \leqslant c \leqslant n - \ell - |r| - k$. Let the number M and the function W be as in Theorem 1. Fix $0 < \varepsilon < 1/100$. Then the function $\mathcal{I}_{s,c}(m)$ defined in (5.9) is $O((qm)^{-100})$ unless*

$$m \leqslant \left(p^{2c}\left(\frac{B^2Z^2}{M} + \frac{A^2M}{p^{2n}}\right)\right)^{1+\varepsilon} q^{\varepsilon} \ll p^{2c}\left(\frac{B^2Z^2}{M} + \frac{A^2M}{p^{2n}}\right) q^{3\varepsilon} =: \mathcal{M}q^{3\varepsilon}. \tag{5.12}$$

In the range (5.12) one has

$$\mathcal{I}_{s,c}(m) = \left(\frac{\mathcal{M}q^{3\varepsilon}}{m}\right)^{1/4} \min\left(M, \frac{BZp^n}{A}\right) e(\vartheta_{s,c}m) W_{s,c}(m) + O(q^{-100}) \tag{5.13}$$

where $W_{s,c}$ is smooth and satisfies

$$m^j \frac{d^j}{dm^j} W_{s,c}(m) \ll_j q^{3\varepsilon}(Z^2 q^{5\varepsilon})^j \tag{5.14}$$

and where

$$\vartheta_{s,c} = \begin{cases} -\frac{p^{n-2c}}{ab}, & \frac{AM}{BZ^2p^n} \geqslant 1, \\ 0, & \text{else.} \end{cases}$$

The statement of the lemma looks a bit artificial, but it is most useful for the rest of the argument. Although the proof gives slightly more information, the lemma claims no asymptotic formula, but only an upper bound for $e(-\vartheta_{s,c}m)\mathcal{I}_{s,c}(m)$ and all its derivatives. The function $W_{s,c}(m)$ depends on whether $AM/(BZ^2p^n) \geqslant 1$ or not, and hence implicitly on A, B, M, Z, but this is not displayed in the notation.

Lemma 3. *Let $s = (a, b, k) \in S^0$, and, for $m \in \mathbb{Z}_p^\times$, let $f_s(m)$ be defined as in (5.4). Further, let $2 \leqslant c \leqslant n - \ell - |r| - k$, and, for every primitive Dirichlet character ψ modulo p^c, let $\widehat{f}_s(\psi)$ be defined as in (5.6). Finally, let $\mathcal{L}_{s,c}(m)$ be defined as in (5.11). Then*

$$\mathcal{L}_{s,c}(m) = \begin{cases} \gamma p^{\frac{n+c}{2}-\ell-|r|-k}\chi(\bar{a}b) \sum_{\varepsilon\in\{\pm 1\}} \Phi_c^\varepsilon(m/ab), & \alpha bm/a \in \mathbb{Z}_p^{\times 2}, \\ 0, & \text{else,} \end{cases}$$

where γ is a constant of absolute value $1 - p^{-1}$ which depends only on the parity of n, and $\Phi_c^\varepsilon : \alpha\mathbb{Z}_p^{\times 2} \to \mathbb{C}$ is a function of absolute value 1 given explicitly in (7.1).

5.4. **Extracting cancellation on average.** We insert (5.10), Lemma 2, and Lemma 3 into (5.5), obtaining

$$L \ll q^\varepsilon \max_{\substack{0\leqslant k\leqslant \ell-|r| \\ 2\leqslant c\leqslant n-\ell-|r|-k}} \max_{\substack{A\leqslant p^{k+2r^+} \\ B\leqslant p^{k+2r^-}}} \left(|L_{A,B,k,c}| + (ABq^\varepsilon)E + q^{-90}\right), \tag{5.15}$$

where E is as in (5.8), and

$$L_{A,B,k,c} := \frac{\min(M, BZp^n/A)}{p^{(n+c)/2}} \sum_{m=1}^{[q^{3\varepsilon}\mathcal{M}]} \left(\frac{\mathcal{M}q^{3\varepsilon}}{m}\right)^{1/4} \sum_{\substack{s=(a,b,k)\in S^0,\ \alpha bm/a\in\mathbb{Z}_p^{\times 2} \\ A\leqslant |a|\leqslant 2A,\ B\leqslant b\leqslant 2B}} \frac{a(m)\chi(\bar{a}b)}{b} e\Bigg(\Big(\frac{\bar{a}p^n\overline{p^{2c}}}{b} + \vartheta_{s,c}\Big)m\Bigg) W_{s,c}(m) \sum_\varepsilon \Phi_c^\varepsilon(m/ab).$$

For $s_1 = (a_1, b_2, k), s_2 = (a_2, b_2, k) \in S^0$, let

$$\Xi_{s_1,s_2} = \sum_{\substack{1\leqslant m\leqslant q^{3\varepsilon}\mathcal{M} \\ \alpha b_1m/a_1,\ \alpha b_2m/a_2\in\mathbb{Z}_p^{\times 2}}} e(\omega_{s_1,s_2,c}m) W_{s_1,c}(m)\overline{W}_{s_2,c}(m) \sum_{\varepsilon_1,\varepsilon_2} \Phi_c^{\varepsilon_1}(m/a_1b_1)\overline{\Phi_c^{\varepsilon_2}(m/a_2b_2)}, \tag{5.16}$$

where

$$\omega_{s_1,s_2,c} = \frac{\bar{a}_1p^n\overline{p^{2c}}}{b_1} - \frac{\bar{a}_2p^n\overline{p^{2c}}}{b_2} + \vartheta_{s_1,c} - \vartheta_{s_2,c}.$$

By the Cauchy-Schwarz inequality and the Rankin-Selberg bound (2.9), we obtain

(5.17)

$$L_{A,B,k,c} \ll \frac{\min(M, BZp^n/A)}{p^{(n+c)/2}B} (q^{3\varepsilon}\mathcal{M})^{\frac{1}{2}} \Bigg(\sum_{\substack{s_1,s_2\in S^0 \\ A\leqslant |a_j|\leqslant 2A \\ B\leqslant b_j\leqslant 2B}} |\Xi_{s_1,s_2}|\Bigg)^{\frac{1}{2}} \ll M^{\frac{1}{2}} Z q^{2\varepsilon} p^{\frac{c-n}{2}} \Bigg(\sum_{\substack{s_1,s_2\in S^0 \\ A\leqslant |a_j|\leqslant 2A \\ B\leqslant b_j\leqslant 2B}} |\Xi_{s_1,s_2}|\Bigg)^{\frac{1}{2}}.$$

In order to bound $L_{A,B,k,c}$, the crucial remaining step is to bound the sum Ξ_{s_1,s_2}. The proof of the following lemma is an application of the second derivative test for p-adic exponential sums that we develop in Section 8 below; it will be given in Section 9. Recall our convention from Section 2.1 regarding $\mathrm{ord}_p\, 0 = \infty$.

Lemma 4. *Let $s_j = (a_j, b_j, k) \in S^0$ (for $j = 1, 2$) be such that $A \leqslant |a_j| \leqslant 2A$, $B \leqslant b_j \leqslant 2B$. Let $2 \leqslant c \leqslant n - \ell - |r| - k$. Let Ξ_{s_1,s_2} be defined as in (5.16), where $\mathcal{M}$, $W_{s,c}$, and Φ_c^ε are as in Lemmas 2 and 3. Then*

$$\Xi_{s_1,s_2} = \sum_{\Omega \in \{0, \mathrm{ord}_p(a_1b_1 - a_2b_2)\}} \Xi_{s_1,s_2,\Omega},$$

where the summands $\Xi_{s_1,s_2,\Omega}$ are defined in (9.10) and satisfy

$$\Xi_{s_1,s_2,\Omega} \ll \begin{cases} q^{17\varepsilon} Z^2 p \left(p^{\frac{\Omega - c}{2}} \mathcal{M} + p^{\frac{c-\Omega}{2}} \right), & \Omega \leqslant c - 2, \\ q^{9\varepsilon} \mathcal{M}, & c - 1 \leqslant \Omega \leqslant \infty. \end{cases}$$

5.5. **The end game.** We are now prepared to complete the proof of Theorem 1. Splitting the Ξ_{s_1,s_2} terms in (5.17) into $\Xi_{s_1,s_2,\Omega}$ for various Ω and regrouping, we have that

$$L_{A,B,k,c} \ll M^{\frac{1}{2}} Z q^{2\varepsilon} p^{\frac{c-n}{2}} \Bigg(\sum_{\substack{s_1,s_2 \in S^0 \\ A \leqslant |a_j| \leqslant 2A \\ B \leqslant |b_j| \leqslant 2B}} |\Xi_{s_1,s_2,0}| + \sum_{\substack{\Omega = 1 \\ p^\Omega \leqslant 8AB}}^{c-2} \sum_{\substack{s_1,s_2 \in S^0 \\ A \leqslant |a_j| \leqslant 2A,\ B \leqslant b_j \leqslant 2B \\ \mathrm{ord}_p(a_1b_1 - a_2b_2) = \Omega}} |\Xi_{s_1,s_2,\Omega}|$$
$$+ \sum_{\substack{\Omega = c-1 \\ p^\Omega \leqslant 8AB}}^{\infty} \sum_{\substack{s_1,s_2 \in S^0 \\ A \leqslant |a_j| \leqslant 2A,\ B \leqslant b_j \leqslant 2B \\ \mathrm{ord}_p(a_1b_1 - a_2b_2) = \Omega}} |\Xi_{s_1,s_2,\Omega}| + \sum_{\substack{s_1,s_2 \in S^0 \\ A \leqslant |a_j| \leqslant 2A,\ B \leqslant b_j \leqslant 2B \\ a_1b_1 = a_2b_2}} |\Xi_{s_1,s_2,\infty}| \Bigg)^{1/2}.$$

Here, both Ω-sums may be restricted to $p^\Omega \leqslant 8AB$ in light of $p^\Omega \mid (a_1b_1 - a_2b_2)$ and $|a_j| \leqslant 2A$, $|b_j| \leqslant 2B$. To estimate the number of terms in the corresponding a_j, b_j-sums, we see that, for each of the $\ll AB$ choices of a_1 and b_1, there are $\ll AB/p^\Omega + 1 \ll AB/p^\Omega$ choices for the (clearly non-zero) product a_2b_2 and hence no more than $(AB/p^\Omega)(AB)^\varepsilon \ll q^\varepsilon (AB/p^\Omega)$ choices for a_2 and b_2 by the divisor bound; this gives a total of $\ll q^\varepsilon AB(AB/p^\Omega)$ terms. The number of terms in the fourth sum is analogously estimated as $\ll q^\varepsilon AB$. Applying Lemma 4 and recalling the definition of $\mathcal{M}$ in (5.12), we thus obtain

$$L_{A,B,k,c} \ll M^{\frac{1}{2}} Z q^{11\varepsilon} p^{\frac{c-n}{2}} \left(\sum_{\Omega=0}^{\infty} AB \frac{AB}{p^\Omega} p \left(p^{\frac{\Omega - c}{2}} \mathcal{M} + p^{\frac{c - \Omega}{2}} \right) Z^2 + \sum_{\Omega = c-1}^{\infty} AB \frac{AB}{p^\Omega} \mathcal{M} + AB\mathcal{M} \right)^{1/2}$$
$$\ll M^{\frac{1}{2}} Z^2 q^{11\varepsilon} p^{\frac{3c}{4} - \frac{n}{2} + \frac{1}{2}} \left[\left(ABp^{c/2} + (AB)^{1/2} p^{\frac{3c}{4} - \frac{1}{2}} \right) \left(\frac{B^2 Z^2}{M} + \frac{A^2 M}{p^{2n}} \right)^{1/2} + AB \right].$$

This is our final estimate for $L_{A,B,k,c}$. Referring to (5.15), we have that

$$\max_{\substack{A \leqslant p^{k+2r^+} \\ B \leqslant p^{k+2r^-}}} |L_{A,B,k,c}| \ll M^{\frac{1}{2}} Z^2 q^{11\varepsilon} p^{\frac{3c}{4} - \frac{n}{2} + \frac{1}{2}} \left[\left(p^{2k+2|r|} p^{\frac{c}{2}} + p^{k+|r|} p^{\frac{3c}{4} - \frac{1}{2}} \right) p^k \left(\frac{Z^2}{M} p^{4r^-} + \frac{M}{p^{2n}} p^{4r^+} \right)^{1/2} + p^{2k+2|r|} \right].$$

For every fixed $0 \leqslant k \leqslant \ell - |r|$, the above expression is monotone in c, so that

$$\max_{2\leqslant c\leqslant n-\ell-|r|-k} \max_{\substack{A\leqslant p^{k+2r^+}\\ B\leqslant p^{k+2r^-}}} |L_{A,B,k,c}|$$
$$\ll M^{\frac{1}{2}} Z^2 q^{11\varepsilon} p^{\frac{1-n}{2}} \left[\left(p^{\frac{5}{4}(n-\ell)+\frac{3}{4}(k+|r|)} + p^{\frac{3}{2}(n-\ell)-\frac{1}{2}(k+|r|+1)} \right) p^{k+|r|} \left(\frac{Z}{M^{1/2}p^r} + \frac{M^{1/2}p^r}{p^n} \right) + p^{\frac{3}{4}(n-\ell)+\frac{5}{4}(k+|r|)} \right].$$

Applying monotonicity in k, we find that

$$\max_{\substack{0\leqslant k\leqslant \ell-|r|\\ 2\leqslant c\leqslant n-\ell-|r|-k}} \max_{\substack{A\leqslant p^{k+2r^+}\\ B\leqslant p^{k+2r^-}}} |L_{A,B,k,c}| \ll M^{\frac{1}{2}} Z^2 q^{11\varepsilon} p^{\frac{1-n}{2}} \left[\left(p^{\frac{5}{4}n+\frac{1}{2}\ell} + p^{\frac{3}{2}n-\ell-\frac{1}{2}} \right) \left(\frac{Z}{M^{1/2}p^r} + \frac{M^{1/2}p^r}{p^n} \right) + p^{\frac{3}{4}n+\frac{1}{2}\ell} \right].$$

The above bound holds for all $\ell \in \mathbb{N}$ and $-\ell \leqslant r \leqslant \ell$, subject only to the constraint (5.2). We choose

$$\ell \in \left[\frac{n}{6} - \frac{1}{2}, \frac{n}{6} + \frac{1}{3} \right] \cap \left[1, \frac{n}{4} \right) \cap \mathbb{N}. \tag{5.18}$$

It is easily verified that such a choice is possible for every $n \geqslant 5$. Also, our basic condition (5.3) guarantees that $p^{-2(n/6-1/2)-1} \ll Zp^n/M \ll p^{2(n/6-1/2)+1}$ (in other words, $Zq^{2/3} \ll M \ll Zq^{4/3}$) and consequently that

$$p^{-2\ell-1} \ll \frac{Zp^n}{M} \ll p^{2\ell+1}.$$

It follows that we can choose an integer r such that $-\ell \leqslant r \leqslant \ell$ and $p^{2r-1} \ll Zp^n/M \ll p^{2r+1}$, so that

$$p^{-1/2} \left(\frac{Zp^n}{M} \right)^{1/2} \ll p^r \ll p^{1/2} \left(\frac{Zp^n}{M} \right)^{1/2}. \tag{5.19}$$

We first show that with these choices of ℓ and r the term $ABq^{\varepsilon}E$ in (5.15) is negligible. Indeed, the bounds on M in (5.3) imply $Z^4p^{7/3} \leqslant q^{1/3}(Zq)^{\varepsilon}$, and hence a fortiori

$$p^{11/6}Z^{1/2} \leqslant q^{11/42+\varepsilon}.$$

By (5.8), (5.3), (5.19) and (5.18) and the size conditions on A and B in (5.15), we conclude

$$ABq^{2\varepsilon}E \ll Mp^2q^{4\varepsilon} \left(1 + \frac{p^{1+\ell-r}}{\sqrt{M}} \right)^{j+\frac{1}{2}} \left(\frac{p^{1+\frac{1}{3}+\frac{1}{2}}Z^{1/2}}{p^{n/3}} \right)^j \leqslant Mp^2q^{4\varepsilon}q^{-j/15} \ll q^{-100} \tag{5.20}$$

for $j \geqslant 2000$. Hence (5.15) yields

$$L \ll M^{\frac{1}{2}}Z^2q^{11\varepsilon}p^{-\frac{n}{2}+\frac{1}{2}} \left[p^{\frac{4}{3}n+\frac{1}{6}+\frac{1}{2}} \left(\frac{Z}{p^n} \right)^{1/2} + p^{\frac{5}{6}n+\frac{1}{6}} \right] \ll M^{\frac{1}{2}}Z^{\frac{5}{2}}p^{\frac{7}{6}}q^{\frac{1}{3}+11\varepsilon}.$$

This completes the proof of Theorem 1. □

5.6. **Proof of Theorem 2.** Theorem 2 is now an easy consequence. By a standard approximate functional equation [18, Theorem 5.3] we have under the assumptions of Theorem 2 that

$$L(f \otimes \chi, 1/2 + it) = \sum_m \frac{a(m)\chi(m)}{m^{1/2+it}} V_t \left(\frac{m}{q} \right) + \frac{\tau(\chi)^2}{q} \sum_m \frac{a(m)\bar{\chi}(m)}{m^{1/2-it}} V_{-t} \left(\frac{m}{q} \right)$$

where $V_{\pm t}$ is a smooth weight function satisfying $x^jV_{\pm t}^{(j)}(x) \ll_{j,A} (1 + x/|t|)^{-A}$ for all $j, A \in \mathbb{N}_0$. By symmetry it is enough to estimate the first term on the right hand side. We can assume without loss of generality $0 \leqslant t \leqslant q$ (for Theorem 2 follows from the convexity bound if $|t| \geqslant q$). We apply a smooth partition of unity and need to bound

$$\frac{1}{M^{1/2}} \sum_m a(m)\chi(m) W\left(\frac{m}{M}\right),$$

where W is a smooth weight function with support in $[1,2]$ satisfying $W^{(j)}(x) \ll_j t^j$, and $M \leqslant (tq)^{1+\varepsilon}$. An application of Theorem 1 completes the proof of Theorem 2. □

6. Archimedean stationary phase computation

In this section we give a *proof of Lemma 2*. We use two general results on exponential integrals from [3, Section 8]: Lemma 8.1, which shows that an integral is very small by a general elaboration of the integration by parts argument, and Proposition 8.2, a general stationary phase estimate which extracts the principal term and a finite number of secondary principal terms with a very small error term.

It follows directly from (2.10) with $Z_0 = Z + AM/(Bp^n)$ and $\alpha = 4\pi\sqrt{m}/(bp^c)$ that $\mathcal{I}_{s,c}(m)$ is negligible outside the range (5.12). More precisely, we have that

$$\mathcal{I}_{s,c}(m) \ll M\left(1 + \frac{Bp^c}{\sqrt{Mm}}\right)^{j+\frac{1}{2}} \left(\frac{(Z + AM/(Bp^n))Bp^c}{\sqrt{Mm}}\right)^j \ll M(qm)^{\frac{-\varepsilon j}{2(1+\varepsilon)}} \ll (qm)^{-100},$$

upon choosing $j = \lceil 500(1+\varepsilon)/\varepsilon \rceil$.

From now on, we assume (5.12). As a preparation for the proof of (5.13) and (5.14), let us momentarily assume

$$\frac{AM}{Bp^n} \geqslant Zq^{2\varepsilon}. \tag{6.1}$$

In this case we insert the representation (2.11) into (5.9) getting

$$\begin{aligned} \mathcal{I}_{s,c}(m) = &\int_0^\infty W\left(\frac{x}{M}\right) e\left(\frac{a}{bp^n}x + \frac{2\sqrt{mx}}{bp^c}\right) \Omega_\kappa^\pm\left(\frac{4\pi\sqrt{mx}}{bp^c}\right) dx \\ &+ \int_0^\infty W\left(\frac{x}{M}\right) e\left(\frac{a}{bp^n}x - \frac{2\sqrt{mx}}{bp^c}\right) \overline{\Omega_\kappa^\pm}\left(\frac{4\pi\sqrt{mx}}{bp^c}\right) dx. \end{aligned} \tag{6.2}$$

The integral $\mathcal{I}_{s,c}(m)$ in (6.2) will be estimated using the above mentioned Lemma 8.1 from [3]. Without loss of generality, we assume $a > 0$ (the other case being identical). The first term of (6.2) has no stationary point, and we use [3, Lemma 8.1] with

$$X = q^\varepsilon, \quad U = M/Z, \quad Q = M, \quad Y = \frac{AM}{Bp^n} + \frac{\sqrt{mM}}{Bp^c} \ll q^{\frac{3}{2}\varepsilon}\frac{AM}{Bp^n}, \quad R = \frac{A}{Bp^n},$$

so that $\min(RU, QRY^{-1/2}) \gg q^{\varepsilon/4}$. Hence by [3, (8.3)] the first term is negligible. By the same argument, the second term is negligible, unless

$$\frac{a}{2p^n} \leqslant \frac{\sqrt{m}}{\sqrt{M}p^c} \leqslant \frac{2a}{p^n}. \tag{6.3}$$

We keep this in mind, and proceed now to the proof of (5.13) and (5.14) under the assumption (5.12). We distinguish the two ranges $AM/(Bp^n) \geqslant Z^2q^{2\varepsilon}$ and $AM/(Bp^n) < Z^2q^{2\varepsilon}$, according to whether the exponential in (5.9) oscillates visibly or not. Let us first assume

$$\frac{AM}{Bp^n} < Z^2q^{2\varepsilon}. \tag{6.4}$$

Then we find by (2.12) that

$$m^j \frac{d^j}{dm^j}\mathcal{I}_{s,c}(m) \ll_j M\Big(\frac{\sqrt{mM}}{Bp^c}\Big)^{-1/2}\Big(\frac{\sqrt{M\mathcal{M}q^{3\varepsilon}}}{Bp^c}\Big)^j \ll M\Big(\frac{\sqrt{mM}}{Bp^c}\Big)^{-1/2}(Z^2q^{4\varepsilon})^j. \tag{6.5}$$

If $AM/(Bp^n) \leqslant Zq^{2\varepsilon}$, this is

$$\ll M\left(\frac{\mathcal{M}}{m}\right)^{1/4}(Z^2q^{4\varepsilon})^j \leqslant \min\left(M, \frac{BZp^n}{A}\right)q^{2\varepsilon}\left(\frac{\mathcal{M}q^{3\varepsilon}}{m}\right)^{1/4}(Z^2q^{4\varepsilon})^j.$$

If $AM/(Bp^n) > Zq^{2\varepsilon}$, we recall (6.3) and estimate (6.5) by

$$\ll M^{1/2}\left(\frac{Bp^n}{A}\right)^{1/2}(Z^2q^{4\varepsilon})^j \leqslant \min\left(M, \frac{BZp^n}{A}\right)q^{2\varepsilon}\left(\frac{\mathcal{M}q^{3\varepsilon}}{m}\right)^{1/4}(Z^2q^{4\varepsilon})^j.$$

In addition, in this range one has (recall (5.12))

$$m^j\frac{d^j}{dm^j}e(\vartheta_{s,c}m) \ll \left(\Big(\frac{BZ^2p^n}{AM}+\frac{AM}{Bp^n}\Big)q^{3\varepsilon}\right)^j \ll (Z^2q^{5\varepsilon})^j.$$

The preceding three bounds confirm (5.13) and (5.14) under the present assumption (6.4).

We proceed to prove (5.13) and (5.14) if (6.4) is not satisfied, i.e. if

$$AM/(Bp^n) \geqslant Z^2q^{2\varepsilon}. \tag{6.6}$$

In particular, (6.1) holds, and hence $\mathcal{I}_{s,c}(m)$ is negligible unless (6.3) is satisfied, which we assume from now on. Then the phase $e\big(ax/bp^n \pm 2\sqrt{mx}/bp^c\big)$ in (6.2) has a stationary point at

$$x_0 = \frac{mp^{2n-2c}}{a^2} \asymp M.$$

Recalling (2.12) and (5.3) and applying [3, Prop. 8.2] with

$$X = \Big(\frac{\sqrt{mM}}{Bp^c}\Big)^{-1/2} \asymp \Big(\frac{p^nB}{AM}\Big)^{1/2}, \quad V_1 = M, \quad V \asymp M/Z,$$
$$Y = \frac{\sqrt{mM}}{Bp^c} \asymp \frac{AM}{Bp^n}, \quad Q = M, \quad p^{2n/3} \leqslant \mathsf{Z} \ll p^{2n}, \quad \delta = \frac{\varepsilon}{3}$$

(satisfying [3, (8.7)] by our present assumption (6.6)), it follows that

$$\mathcal{I}_{s,c}(m) = e\left(-\frac{mp^{n-2c}}{ba}\right)\frac{Bp^n}{A}P_{s,c}(m) + O(q^{-100})$$

where $P_{s,c}^{(j)}(m) \ll (m/Z)^{-j}$ by [3, (8.11)]. This confirms (5.13) and (5.14) in the case (6.6) and completes the proof of the lemma. □

7. p-ADIC STATIONARY PHASE COMPUTATION

In this section we give a proof of Lemma 3. Our method actually works in great generality. The functions entering the complete and incomplete exponential sums which we consider in this section are p-adic analytic functions, and this allows for a beautiful analogy on which this paper and [26] are built. However, we will see that, for our particular purposes, we require quite a bit less information than full analyticity.

7.1. **Preliminaries.** The following three lemmas are essentially known (see e.g. [18, pp. 320-322]), but for completeness we include full proofs.

Lemma 5 (Gauss sum)**.** *Let p be an odd prime, $A \in \mathbb{Z}_p^\times$, $B \in p^{-n}\mathbb{Z}_p$, $s \in \{0,1\}$, $n \geqslant s$, and let*

$$S = \sum_{x \bmod p^n} \theta\big(Ap^{-s}x^2 + Bx\big).$$

Then $S = 0$ unless $B \in p^{-s}\mathbb{Z}_p$, in which case

$$S = p^{n-s/2}\epsilon(A,p^s)\theta\Big(-\frac{B^2p^s}{4A}\Big),$$

where

$$\epsilon(A,p^s) = \begin{cases} 1, & s=0,\\ \big(\frac{A}{p}\big), & s=1,\ p\equiv 1 \pmod 4,\\ \big(\frac{A}{p}\big)i, & s=1,\ p\equiv 3 \pmod 4.\end{cases}$$

Proof. Note that the summand is indeed $p^n\mathbb{Z}_p$-periodic. If $s=0$, then $S=0$ if $B \notin \mathbb{Z}_p$ and $S = p^n$ otherwise. If, on the other hand, $s=1$, then

$$S = \sum_{x \bmod p}\sum_{t \bmod p^{n-1}} \theta\big(Ap^{-1}(x+pt)^2 + B(x+pt)\big) = \sum_{x \bmod p}\theta\big(Ap^{-1}x^2+Bx\big)\sum_{t \bmod p^{n-1}}\theta\big(Bpt\big),$$

so that $S=0$ if $B \notin p^{-1}\mathbb{Z}_p$. In the case $B \in p^{-1}\mathbb{Z}_p$, we find that

$$S = p^{n-1}\sum_{x \bmod p}\theta\left(Ap^{-1}(x+(2A)^{-1}Bp)^2\right)\theta\left(-(4A)^{-1}B^2p\right) = p^{n-\frac{1}{2}}\epsilon(A,p)\theta\Big(-\frac{B^2p}{4A}\Big),$$

by the classical evaluation of the quadratic Gauss sum (see e.g. [18, (3.29) and (3.22)]). ☐

Lemma 6 (p-adic stationary phase)**.** *Let $n \geqslant \kappa$, let $A \subseteq \mathbb{Z}_p$ be such that $(A + p^\kappa\mathbb{Z}_p) \subseteq A$, and let $f : A/p^n\mathbb{Z}_p \to \mathbb{C}^\times$, $g_1, g_2 : A \to \mathbb{Q}_p$ be functions such that, for every $t \in \mathbb{Z}_p$,*

$$f\big(x+p^\kappa t\big) = f(x)\theta\Big(g_1(x)\cdot p^\kappa t + \tfrac{1}{2}g_2(x)\cdot p^{2\kappa}t^2\Big).$$

Assume that $\mathrm{ord}_p\, g_1(x) \geqslant -n$ and $\mathrm{ord}_p\, g_2(x) = \mu$ for every $x \in A$, and that $-2n \leqslant \mu \leqslant -2\kappa$. Write $\mu = -2r-\rho$ with $r \in \mathbb{Z}$ and $\rho \in \{0,1\}$. Then

$$\sum_{x \bmod p^n,\, x\in A} f(x) = p^{n+(\mu/2)} \sum_{\substack{x \bmod p^r,\, x\in A\\ g_1(x)\in p^{-r-\rho}\mathbb{Z}_p}} f(x)\epsilon\big(\bar{2}(g_2(x))_0, p^\rho\big)\theta\left(-\frac{g_1(x)^2}{2g_2(x)}\right).$$

We make a very important remark that, even though this may not be immediately obvious from its shape, the summand on the right-hand side *is* $p^r\mathbb{Z}_p$-periodic, as will be clear from the proof. Conditional sums on both sides are understood in the sense of Section 2.1. In particular, in applying the lemma, one can substitute on the right-hand side arbitrary representatives of the congruence classes modulo $p^r\mathbb{Z}_p$, including, of course, those which are most convenient.

Proof. Let S denote the sum on the left-hand side. Note that our assumptions imply that $\kappa \leqslant r \leqslant n-\rho$, so that we may write

$$\begin{aligned} S &= \sum_{x \bmod p^r,\, x\in A}\ \sum_{t \bmod p^{n-r}} f\big(x+p^rt\big)\\ &= \sum_{x \bmod p^r,\, x\in A} f(x) \sum_{t \bmod p^{n-r}} \theta\Big(\tfrac{1}{2}g_2(x)p^{2r}t^2 + p^rg_1(x)t\Big).\end{aligned}$$

Since $r+\operatorname{ord}_p g_1(x)\geqslant -(n-r)$ and $2r+\mu=-\rho$, Lemma 5 can be applied to the inner sum, yielding

$$S=p^{n-r-\rho/2}\sum_{\substack{x \bmod p^r,\, x\in A\\ g_1(x)\in p^{-r-\rho}\mathbb{Z}_p}} f(x)\epsilon\big(\bar{2}(g_2(x))_0,p^\rho\big)\theta\left(-\frac{g_1(x)^2p^{2r+\rho}}{2(g_2(x))_0}\right). \qquad \square$$

Lemma 7 (Kloosterman sum evaluation)**.** *Let p be an odd prime, let $u\in\mathbb{Z}_p^\times$, let $m\geqslant 2$, and let*

$$S(1,u;p^m)=\sideset{}{^*}\sum_{x \bmod p^m}\theta\left(\frac{x+u/x}{p^m}\right)$$

be the Kloosterman sum. Then, $S(1,u;p^m)=0$ unless $u\in\mathbb{Z}_p^{\times 2}$, in which case, denoting $\rho=0$ or 1 according to whether m is even or odd,

$$S(1,u;p^m)=p^{m/2}\sum_{\pm}\epsilon(\pm u_{1/2},p^\rho)\theta\left(\pm\frac{2u_{1/2}}{p^m}\right).$$

Proof. Note that, for every $x\in\mathbb{Z}_p^\times$, $t\in\mathbb{Z}_p$, and $\kappa\geqslant 1$,

$$\big(x+p^\kappa t\big)\cdot\left(\frac{1}{x}-\frac{1}{x^2}p^\kappa t+\frac{1}{x^3}p^{2\kappa}t^2\right)\in 1+p^{3\kappa}\mathbb{Z}_p,$$

so that

$$\big(x+p^\kappa t\big)^{-1}\equiv\frac{1}{x}-\frac{1}{x^2}p^\kappa t+\frac{1}{x^3}p^{2\kappa}t^2 \pmod{p^{3\kappa}},$$

and the function $g_u(x):=\theta\big((x+u/x)/p^m\big)$ satisfies

$$g_u\big(x+p^\kappa t\big)=g_u(x)\theta\bigg(\Big(1-\frac{u}{x^2}\Big)p^{\kappa-m}t+\frac{u}{x^3}p^{2\kappa-m}t^2\bigg)$$

as long as $3\kappa\geqslant m$. We may apply Lemma 6 with $\mu=-m$ as long as $-2m\leqslant\mu=-m\leqslant-2\kappa$, that is, whenever $m\geqslant 2\kappa$. We make an arbitrary choice of $\kappa\geqslant 1$ with $\kappa\in[m/3,m/2]$; such a choice can be made for every $m\geqslant 2$. Writing $m=2r+\rho$ with $r\geqslant 1$ and $\rho\in\{0,1\}$ as in the statement of our lemma, we have that

$$S(1,u;p^m)=p^{m/2}\sideset{}{^*}\sum_{\substack{x \bmod p^r\\ 1-u/x^2\equiv 0 \pmod{p^{m-r-\rho}}}}\theta\left(\frac{x+u/x}{p^m}\right)\epsilon\big(u\bar{x}^3,p^\rho\big)\theta\Big(-\frac{x^3}{4u}\Big(1-\frac{u}{x^2}\Big)^2\frac{1}{p^m}\Big).$$

The summation condition is equivalent to $x^2\equiv u \pmod{p^r}$. Since $r\geqslant 1$, it follows that $S(1,u;p^m)=0$ unless $u\in\mathbb{Z}_p^{\times 2}$, in which case the condition is equivalent to $x\equiv\pm u_{1/2} \pmod{p^r}$, so that the sum has exactly two terms. Their contributions may (by the remarked periodicity) be evaluated by substituting exact values of $\pm u_{1/2}$; this gives the announced result. $\square$

7.2. **Proof of Lemma 3.** We return to the situation in Lemma 3 and recall our notational conventions. Let $\ell<n/4$ be a positive integer satisfying (5.2), and let r be an integer with $-\ell\leqslant r\leqslant\ell$. We recall that the set $\mathbb{Z}_p^\times[a,b,k]$ was defined by the condition $m-\alpha b/a\in p^{\ell+|r|+k}\mathbb{Z}_p$. For $s=(a,b,k)\in S^0$, write

$$\ell_s=\ell+|r|+k\leqslant n/2$$

by (5.2). Recall that χ is a fixed primitive character modulo p^n. According to (2.5), we have

$$\chi\big(1+p^\kappa t\big)=\theta\left(\frac{\alpha}{p^n}\big(p^\kappa t-\tfrac{1}{2}p^{2\kappa}t^2\big)\right)$$

for every κ with $3\kappa\geqslant n+\iota'$ and every $t\in\mathbb{Z}_p$.

We split the proof of Lemma 3 into two steps, which are treated in Lemmas 8 and 9 below. Lemma 3 follows immediately by combining these two statements.

Lemma 8 is a purely algebraic and spectral statement, in which $\mathcal{L}_{s,c}(m)$ is replaced by its dual sum via discrete harmonic analysis. In other words, Lemma 8 is an expression of discrete Parseval's identity, with the Kloosterman sum (the multiplicative convolution of $\theta(\cdot/p^n)$ and $\theta(\bar{\cdot}/p^n)$, which can be seen as the discrete analogue of the Bessel function) appearing on the dual side as the transform of the square of the Gauss sum.

The resulting sum is a complete exponential sum; it is *exactly* evaluated in the analytic Lemma 9 by using the p-adic method of stationary phase, Lemma 6, and exploiting p-adic local information; this is also facilitated by an explicit evaluation of the Kloosterman sum in Lemma 7. The resulting explicit evaluation of $\mathcal{L}_{s,c}(m)$ in Lemma 9 is a sum of at most two terms $\Phi_c^{\varepsilon}(x)$ defined in (7.1) below, each of which is (upon recalling (2.2)) essentially an exponential with a completely explicit p-adically analytic phase. (The p-adically analytic phase implicit in (7.1) is entirely analogous to Jutila's $\phi(x)$ in [20, (4.1.6)].) We will develop a general machinery for estimating sums involving terms of this nature in Section 8.

Lemma 8. *Let $m \in \mathbb{Z}_p^{\times}$. For $s = (a, b, k) \in S^0$, let $f_s(m)$ be defined as in (5.4). Further, let $2 \leqslant c \leqslant n - \ell_s$, and, for every primitive Dirichlet character ψ modulo p^c, let $\widehat{f}_s(\psi)$ be defined as in (5.6). Finally, let $\mathcal{L}_{s,c}(m)$ be defined as in (5.11). Then,*

$$\mathcal{L}_{s,c}(m) = \frac{1}{\delta_p} \sum_{\substack{x \bmod p^{n-\ell_s} \\ x \in \mathbb{Z}_p^{\times}[a,b,k]}} \chi(x)\theta\left(-\frac{a/b}{p^n}x\right) S\big(1, mb^{-2}x; p^c\big),$$

where $\delta_p = \big(1 - p^{-1}\big)^{-1}$.

Proof. The definition of $\mathcal{L}_{s,c}(m)$ in (5.11) features a sum over all primitive characters modulo p^c. In preparation for passage to dual sums, we observe that, for every $(u, p) = 1$ and every $c \geqslant 2$, one has

$$\frac{\delta_p}{p^c} \sum_{\substack{\psi \bmod p^c \\ \psi \text{ primitive}}} \psi(u) = \frac{\delta_p}{p^c} \sum_{\psi \bmod p^c} \psi(u) - \frac{\delta_p}{p^c} \sum_{\psi \bmod p^{c-1}} \psi(u) = \delta_{p^c}(u) - \frac{1}{p}\delta_{p^{c-1}}(u),$$

where δ_{p^c} is the characteristic function of $1 + p^c\mathbb{Z}_p$. On the other hand, for any character ψ modulo p^c and any $w \in \mathbb{Z}_p^{\times}$,

$$\tau(\psi)^2\overline{\psi(w)} = \sum\sum_{u_1,u_2 \bmod p^c} \psi(u_1u_2w^{-1})\theta\left(\frac{u_1+u_2}{p^c}\right) = \sum_{u \bmod p^c} \psi(u)S(1, wu; p^c).$$

Returning to $\mathcal{L}_{s,c}(m)$ and opening up $\hat{f}_s(\psi)$, we thus obtain

$$\begin{aligned}\mathcal{L}_{s,c}(m) &= \frac{1}{p^c} \sum_{x \bmod p^{n-\ell_s}} \sum_{u \bmod p^c} f_s(x)S(1, mb^{-2}u; p^c) \sum_{\substack{\psi \bmod p^c \\ \psi \text{ primitive}}} \overline{\psi(x)}\psi(u) \\ &= \frac{1}{\delta_p} \sum_{x \bmod p^{n-\ell_s}} f_s(x)S(1, mb^{-2}x; p^c) - \frac{1}{p\delta_p} \sum_{x \bmod p^{n-\ell_s}} f_s(x) \sum_{\substack{\sigma \bmod p \\ (x+p^{c-1}\sigma, p)=1}} S(1, mb^{-2}(x + p^{c-1}\sigma); p^c).\end{aligned}$$

Since the inner sum in the second term vanishes trivially, we obtain the desired result. ☐

Lemma 9. *For $s = (a, b, k) \in S^0$, $2 \leqslant c \leqslant n - \ell_s$, and $m \in \mathbb{Z}_p^{\times}$, let*

$$\mathscr{S} = \sum_{\substack{x \bmod p^{n-\ell_s} \\ x \in \mathbb{Z}_p^{\times}[a,b,k]}} \chi(x)\theta\left(-\frac{a/b}{p^n}x\right) S(1, mxb^{-2}; p^c)$$

be the sum featured in Lemma 8. Then $\mathscr{S} = 0$ unless $\alpha bm/a \in \mathbb{Z}_p^{\times 2}$, in which case $\mathscr{S}$ can be exactly evaluated as follows. Let ρ resp. ρ_1 be 0 or 1 according as c resp. n is even or odd. For $\varepsilon \in \{\pm 1\}$ and

$\rho \in \{0,1\}$, *define* $\Phi_c^\varepsilon(x)$ *for* $x \in \alpha\mathbb{Z}_p^{\times 2}$ *as*

$$\begin{aligned}\Phi_c^\varepsilon(x) &:= \epsilon\big(\varepsilon(\alpha x)_{1/2}, p^\rho\big)\chi\Big(\alpha + \tfrac{1}{2}p^{2(n-c)}x + \varepsilon p^{n-c}\big(\alpha x + \tfrac{1}{4}p^{2(n-c)}x^2\big)_{1/2}\Big) \\ &\quad \times \theta\bigg(\frac{1}{p^c}\Big(\tfrac{1}{2}p^{n-c}x + \varepsilon\big(\alpha x + \tfrac{1}{4}p^{2(n-c)}x^2\big)_{1/2}\Big)\bigg).\end{aligned} \tag{7.1}$$

Then

$$\mathscr{S} = p^{(n+c)/2-\ell_s}\chi(\bar{a}b)\theta\Big(-\frac{\alpha}{p^n}\Big)\epsilon\big(-\bar{2}\alpha, p^{\rho_1}\big)\sum_{\varepsilon\in\{\pm1\}^2}\Phi_c^\varepsilon\Big(\frac{m}{ab}\Big).$$

Proof. We can evaluate the Kloosterman sum by Lemma 7. We find that $S(1, mxb^{-2}; p^c) = 0$ unless $mxb^{-2} \in \mathbb{Z}_p^{\times 2}$; in light of $x - \alpha b/a \in p^{\ell_s}\mathbb{Z}_p$ for every $x \in \mathbb{Z}_p^\times[a,b,k]$, this is equivalent to $\alpha bm/a \in \mathbb{Z}_p^{\times 2}$. If this condition is satisfied, then

$$\mathscr{S} = p^{c/2}\sum_{\substack{x \bmod p^{n-\ell_s}\\ x\in\mathbb{Z}_p^\times[a,b,k]}}\chi(x)\theta\left(-\frac{a}{bp^n}x\right)\sum_{\varepsilon}\epsilon\big(\varepsilon(mx)_{1/2}\bar{b}, p^\rho\big)\theta\left(\varepsilon\frac{2(mx)_{1/2}}{bp^c}\right), \tag{7.2}$$

with ρ as in the statement of the lemma. Here, we replaced for convenience $(mxb^{-2})_{1/2}$ by $(mx)_{1/2}b^{-1}$, since they differ by a unit factor $\delta \in \{\pm 1\}$ that is the same for all $x \in \alpha b/a + p\mathbb{Z}_p$ and consequently absorbed by the ε-sum. Also, note that the ϵ-term only depends on $x \bmod p^\rho$.

Using (2.5) and (2.6), it follows that the function $f_{s,m,c}^\varepsilon(x)$, defined for $x \in \mathbb{Z}_p^\times[a,b,k]$ as

$$f_{s,m,c}^\varepsilon(x) := \chi(x)\theta\left(-\frac{a}{bp^n}x\right)\epsilon\big(\varepsilon(mx)_{1/2}\bar{b}, p^\rho\big)\theta\left(\varepsilon\frac{2(mx)_{1/2}}{bp^c}\right),$$

satisfies

$$\begin{aligned}f_{s,m,c}^\varepsilon(x+p^\kappa t) &= f_{s,m,c}^\varepsilon(x)\theta\bigg(\frac{\alpha}{p^n}\Big[\frac{1}{x}p^\kappa t - \frac{1}{2x^2}p^{2\kappa}t^2\Big] - \frac{a}{bp^n}p^\kappa t + \frac{\varepsilon}{bp^c}\Big[\frac{1}{(mx)_{1/2}}p^\kappa mt - \frac{1}{(mx)_{1/2}^3}p^{2\kappa}m^2t^2\Big]\bigg) \\ &= f_{s,m,c}^\varepsilon(x)\theta\bigg(\Big[\Big(\frac{\alpha}{x} - \frac{a}{b}\Big)p^{-\ell_s} + \varepsilon\frac{mp^{n-\ell_s-c}}{(mx)_{1/2}b}\Big]p^{\kappa-(n-\ell_s)}t + \Big[-\frac{\alpha}{2x^2} - \varepsilon\frac{m^2p^{n-c}}{4(mx)_{1/2}^3b}\Big]p^{2\kappa-n}t^2\bigg)\end{aligned}$$

for every $t \in \mathbb{Z}_p$ and every $\kappa \geqslant \ell_s$ (which ensures that $x + p^\kappa t \in \mathbb{Z}_p^\times[a,b,k]$ if and only if $x \in \mathbb{Z}_p^\times$) with $3\kappa \geqslant n + \iota'$. (In particular, recalling that $\alpha/x - a/b \in p^{\ell_s}\mathbb{Z}_p$, we can confirm that $f_{s,m,c}^\pm$ is $p^{n-\ell_s}\mathbb{Z}_p$-periodic in light of $n \geqslant 2\ell_s$.)

We now apply Lemma 6 to $\mathscr{S}$, with $\mu = -n$, which we may do as long as $n - \ell_s \geqslant \kappa$ and $-2(n-\ell_s) \leqslant -n \leqslant -2\kappa$, that is, $n \geqslant 2\kappa$. In light of $n \geqslant 2\ell_s$, we may choose any $\kappa \in [\max((n+\iota')/3, \ell_s), n/2]$ (such a choice is always possible, since $n \geqslant 4$ is assured by either (5.3) or $\ell < n/4$). Writing $n = 2\nu + \rho_1$, we find that

$$\mathscr{S} = p^{c/2+(n-\ell_s)-n/2}\sum_x\sum_\varepsilon f_{s,m,c}^\varepsilon(x)\epsilon(-\bar{2}\alpha, p^{\rho_1})\theta\bigg(\frac{x^2}{\alpha}\Big[\Big(\frac{\alpha}{x} - \frac{a}{b}\Big)p^{-\ell_s} + \varepsilon\frac{mp^{n-\ell_s-c}}{(mx)_{1/2}b}\Big]^2 p^{3\ell_s-n}\bigg),$$

where summation is over all $x \in \mathbb{Z}_p^\times[a,b,k]$, $x \bmod p^\nu$, such that

$$\Big(\frac{\alpha}{x} - \frac{a}{b}\Big) + \varepsilon\frac{mp^{n-c}}{(mx)_{1/2}b} \in p^{n-\nu-\rho_1}\mathbb{Z}_p = p^\nu\mathbb{Z}_p.$$

This condition can be written equivalently as

$$\frac{a}{b}mx - \varepsilon\frac{mp^{n-c}}{b}(mx)_{1/2} - \alpha m \equiv 0 \pmod{p^\nu}.$$

Denote $\xi = (mx)_{1/2} \in \mathbb{Z}_p^\times$. Recalling that $x \in \alpha b/a + p^{\ell_s}\mathbb{Z}_p$ and $\alpha mb/a \in \mathbb{Z}_p^{\times 2}$, we have that $\xi \in (\alpha mb/a)_{1/2} + p^{\ell_s}\mathbb{Z}_p$ is such that

$$\frac{a}{b}\xi^2 - \varepsilon\frac{mp^{n-c}}{b}\xi - \alpha m \equiv 0 \pmod{p^\nu},$$
$$\Big(\xi - \varepsilon\frac{mp^{n-c}}{2a}\Big)^2 \equiv \frac{\alpha mb}{a} + \frac{m^2p^{2(n-c)}}{4a^2} \pmod{p^\nu}.$$

This congruence in ξ has two solutions, of which exactly one is in the requisite class modulo p^{ℓ_s} and yields the corresponding stationary point x:

$$\xi \equiv \varepsilon\frac{mp^{n-c}}{2a} + \varepsilon\Big(\frac{\alpha mb}{a} + \frac{m^2p^{2(n-c)}}{4a^2}\Big)_{1/2} \pmod{p^\nu},$$
$$x \equiv \frac{\alpha b}{a} + \frac{mp^{2(n-c)}}{2a^2} + \varepsilon\frac{p^{n-c}}{a}\Big(\frac{\alpha mb}{a} + \frac{m^2p^{2(n-c)}}{4a^2}\Big)_{1/2} \pmod{p^\nu}.$$

Returning to the result of the stationary phase evaluation of $\mathscr{S}$, we see that the sum over x has exactly two summands. Keeping in mind the remark immediately following the statement of Lemma 6, we may further evaluate $\mathscr{S}$ as

$$\begin{aligned}\mathscr{S} &= p^{(n+c)/2-\ell_s}\sum_{\varepsilon\in\{\pm1\}}\epsilon\big(\varepsilon(\alpha m\bar{a}\bar{b})_{1/2}, p^\rho\big)\epsilon\big(-\bar{2}\alpha, p^{\rho_1}\big)\chi\bigg(\frac{\alpha b}{a} + \frac{mp^{2(n-c)}}{2a^2} + \varepsilon\frac{bp^{n-c}}{a}\Big(\frac{\alpha m}{ab} + \frac{m^2p^{2(n-c)}}{4a^2b^2}\Big)_{1/2}\bigg)\\ &\quad\theta\bigg(-\frac{1}{p^n}\Big[\alpha + \frac{mp^{2(n-c)}}{2ab} + \varepsilon p^{n-c}\Big(\frac{\alpha m}{ab} + \frac{m^2p^{2(n-c)}}{4a^2b^2}\Big)_{1/2}\Big] + \frac{1}{p^c}\Big[\frac{mp^{n-c}}{ab} + 2\varepsilon\Big(\frac{\alpha m}{ab} + \frac{m^2p^{2(n-c)}}{4a^2b^2}\Big)_{1/2}\Big]\bigg)\\ &= p^{(n+c)/2-\ell_s}\chi\Big(\frac{b}{a}\Big)\theta\Big(-\frac{\alpha}{p^n}\Big)\epsilon\big(-\bar{2}\alpha, p^{\rho_1}\big)\sum_{\varepsilon\in\{\pm1\}}\epsilon\big(\varepsilon(\alpha m\bar{a}\bar{b})_{1/2}, p^\rho\big)\\ &\quad\chi\bigg(\alpha + \frac{p^{2(n-c)}m}{2ab} + \varepsilon p^{n-c}\Big(\frac{\alpha m}{ab} + \frac{p^{2(n-c)}m^2}{4a^2b^2}\Big)_{1/2}\bigg)\theta\bigg(\frac{1}{p^c}\Big[\frac{p^{n-c}m}{2ab} + \varepsilon\Big(\frac{\alpha m}{ab} + \frac{p^{2(n-c)}m^2}{4a^2b^2}\Big)_{1/2}\Big]\bigg),\end{aligned}$$

by replacing ε by $\delta\varepsilon$ (with δ as in the remark after (7.2)). This evaluation of $\mathscr{S}$ is equivalent to the statement of the lemma. ☐

8. p-adic van der Corput estimates

The main result of this section is Theorem 5 below, which is a broad generalization of Corollary 4 stated in the introduction. Our theorem provides an estimate for an exponential sum of the form

$$\sum_{m\in\mathscr{M}} e(\omega m)f(m)W(m),$$

where $\omega \in \mathbb{R}$, $\mathscr{M}$ is (roughly speaking) an interval (subject to finitely many congruence conditions), and $f : \mathscr{M} \to \mathbb{C}$ is a function satisfying

$$f(x + p^\kappa t) \approx f(x)\cdot\theta\big(g_1(x)\cdot p^\kappa t + \tfrac{1}{2}g_2(x)\cdot p^{2\kappa}t^2\big).$$

We precede Theorem 5 with two auxiliary results in different directions. Lemma 10 is purely local in nature. It allows us to extract information about the "first derivative" $g_1(x)$ if sufficient information about the size of the "second derivative" $g_2(x)$ and the remainder term $\boldsymbol{\mu}$ is available. (The reader is reminded that no analyticity is assumed on f and that, in any case, no Mean Value Theorem or similar statements are available in the p-adic situation.) Lemma 11, on the other hand, is analytic in nature and presents an estimate for the sum of a function defined on integers for which only a good first-order linear model is assumed in arithmetic progressions to moduli which are very high powers of p.

Lemma 10. *Let κ, ω be nonnegative integers, let $A \subseteq \mathbb{Z}_p$ be such that $(A+p^\kappa\mathbb{Z}_p) \subseteq A$, and let $f : A \to \mathbb{C}^\times$, $g_1, g_2 : A \to \mathbb{Q}_p$ be functions such that, for every $t \in \mathbb{Z}_p$,*

$$f\big(x + p^\kappa t\big) = f(x)\theta\Big(g_1(x) \cdot p^\kappa t + \tfrac{1}{2} g_2(x) \cdot p^{2\kappa} t^2\Big)\boldsymbol{\mu}_{p^\omega}.$$

Then, for every $t \in \mathbb{Z}_p$,

$$g_1\big(x + p^\kappa t\big) - g_1(x) \in g_2(x) \cdot p^\kappa t + p^{-\kappa-\omega}\mathbb{Z}_p.$$

Proof. Let $u \in \mathbb{Z}_p$ be arbitrary. Then

$$\begin{aligned} f\big(x + p^\kappa ut\big) &= f(x)\theta\Big(g_1(x) \cdot p^\kappa ut + \tfrac{1}{2} g_2(x) \cdot p^{2\kappa} u^2 t^2\Big)\boldsymbol{\mu}_{p^\omega}, \text{ as well as} \\ f\big(x + p^\kappa ut\big) &= f\Big(\big(x + p^\kappa t\big) + p^\kappa(u-1)t\Big)\boldsymbol{\mu}_{p^\omega} \\ &= f\big(x + p^\kappa t\big)\theta\Big(g_1\big(x + p^\kappa t\big) \cdot p^\kappa(u-1)t + \tfrac{1}{2} g_2\big(x + p^\kappa t\big) \cdot p^{2\kappa}(u-1)^2 t^2\Big)\boldsymbol{\mu}_{p^\omega} \\ &= f(x)\theta\left(\Big[g_1(x) + (u-1)g_1\big(x + p^\kappa t\big)\Big] \cdot p^\kappa t + \tfrac{1}{2}\Big[g_2(x) + (u-1)^2 g_2\big(x + p^\kappa t\big)\Big] \cdot p^{2\kappa} t^2\right)\boldsymbol{\mu}_{p^\omega}. \end{aligned}$$

It follows that

$$(u-1)\Big[g_1\big(x + p^\kappa t\big) - g_1(x)\Big] \cdot p^\kappa t - \tfrac{1}{2}(u-1)\Big[(u+1)g_2(x) - (u-1)g_2\big(x + p^\kappa t\big)\Big] \cdot p^{2\kappa} t^2 \in p^{-\omega}\mathbb{Z}_p,$$

so that, assuming that $u - 1 \in \mathbb{Z}_p^\times$ and writing $\tau = \operatorname{ord}_p t$,

$$g_1\big(x + p^\kappa t\big) - g_1(x) - g_2(x) \cdot p^\kappa t + \tfrac{1}{2}(u-1)\Big[g_2\big(x + p^\kappa t\big) - g_2(x)\Big] \cdot p^\kappa t \in p^{-\kappa-\omega-\tau}\mathbb{Z}_p.$$

The above holds for every $u \in \mathbb{Z}_p$ such that $u - 1 \in \mathbb{Z}_p^\times$. In particular, it is possible to choose such u_1, u_2 with $u_1 - u_2 \in \mathbb{Z}_p^\times$ (for example, $u_1 = 0$, $u_2 = 2$). Comparing the above conclusion with these choices for u_1 and u_2, we infer that

$$\Big[g_2\big(x + p^\kappa t\big) - g_2(x)\Big] \cdot p^\kappa t \in p^{-\kappa-\omega-\tau}\mathbb{Z}_p,$$

and hence that

$$g_1\big(x + p^\kappa t\big) - g_1(x) - g_2(x) \cdot p^\kappa t \in p^{-\kappa-\omega-\tau}\mathbb{Z}_p.$$

If $t \in \mathbb{Z}_p^\times$, then $\tau = 0$ and we are done. If $t \in p\mathbb{Z}_p$, then we may choose a t_1 with $t_1, (t - t_1) \in \mathbb{Z}_p^\times$ (for example, $t_1 = 1$). This gives

$$g_1\Big(\big(x + p^\kappa t_1\big) + p^\kappa(t - t_1)\big)\Big) - g_1\big(x + p^\kappa t_1\big) - g_2\big(x + p^\kappa t_1\big) \cdot p^\kappa(t - t_1) \in p^{-\kappa-\omega}\mathbb{Z}_p,$$

hence

$$g_1\big(x + p^\kappa t\big) - g_1(x) - g_2(x) \cdot p^\kappa t - \Big[g_2\big(x + p^\kappa t_1\big) - g_2(x)\Big] \cdot p^\kappa(t - t_1) \in p^{-\kappa-\omega}\mathbb{Z}_p.$$

Since the third summand is in $p^{-\kappa-\omega}\mathbb{Z}_p$, the statement of the lemma follows. □

Lemma 11 (Pre-second derivative test)**.** *Let $\omega \in \mathbb{R}$, and let $\kappa, \varphi \in \mathbb{N}_0$ and $\Phi : \mathbb{Z} \to \mathbb{C}^\times$, $\Phi_1 : \mathbb{Z} \to p^{-\varphi}\mathbb{Z}$ be such that $|\Phi(x)| \leqslant \Phi_0$ and*

$$\Phi\big(x + p^\kappa t\big) = \Phi(x)e\big(\Phi_1(x)p^\kappa t\big) = \Phi(x)\theta\big(\Phi_1(x)p^\kappa t\big)$$

for every $x, t \in \mathbb{Z}$. Let $\mathscr{M} \subset \mathbb{Z}$ be the intersection of an interval $[M_1, M_2]$ with a union of arithmetic progressions modulo p^μ for some $\mu \in \mathbb{N}_0$. We write $M_0 = M_2 - M_1$. Let $j \geqslant \max(\kappa, \mu)$, let $\mathscr{M}_{(j)}$ be a full set of representatives of those congruence classes modulo p^j which occur in $\mathscr{M}$, and suppose that

$$\big|\{x \in \mathscr{M}_{(j)} : \Phi_1(x) \in f + p^{-j}\mathbb{Z}\}\big| \ll p^\beta$$

for every $f \in p^{-\varphi}\mathbb{Z}$ and some $\beta \geqslant 0$.

Then, for every continuously differentiable function $W : [M_1, M_2] \to \mathbb{C}$,

$$\sum_{m \in \mathscr{M}} e(\omega m)\Phi(m)W(m) \ll \Phi_0\big(M_0 + p^\varphi + p^j\big)\big(\|W\|_\infty + \|W'\|_1\big)p^{\beta-j}\log(2 + M_0).$$

Proof. Note that, for every $x, t \in \mathbb{Z}$, one has $\Phi(x+2p^jt) = \Phi(x)e(2\Phi_1(x)p^jt)$ and $\Phi(x+2p^jt) = \Phi(x+p^jt)e(\Phi_1(x)p^jt) = \Phi(x)e\big((\Phi_1(x)+\Phi_1(x+p^jt))p^jt\big)$, so that $\Phi_1(x+p^jt)-\Phi_1(x) \in p^{-j}\mathbb{Z}$. In particular, for any given $f \in p^{-\varphi}\mathbb{Z}$, the condition that $\Phi_1(x) \in f + p^{-j}\mathbb{Z}$ does not depend on the choice of the representative x of a congruence class modulo p^j.

We first estimate

$$\begin{aligned} S = \sum_{m \in \mathscr{M}} e(\omega m)\Phi(m) &= \sum_{m \in \mathscr{M}_{(j)}} \sum_{t : m+p^jt \in \mathscr{M}} e\Big(\omega\big(m+p^jt\big)\Big)\Phi\big(m+p^jt\big) \\ &= \sum_{m \in \mathscr{M}_{(j)}} e(\omega m)\Phi(m) \sum_{t : m+p^jt \in \mathscr{M}} e\Big(\big(\omega+\Phi_1(m)\big)p^jt\Big) \\ &\ll \Phi_0 \sum_{m \in \mathscr{M}_{(j)}} \min\left(\frac{M_0}{p^j}+1, \big\|\big(\omega+\Phi_1(m)\big)p^j\big\|^{-1}\right). \end{aligned}$$

Here, in light of $j \geqslant \mu$, the inner sums are over an interval of values for t and are estimated as the sum of a finite geometric progression as usual, with $\|\cdot\|$ denoting the distance to the nearest integer. This basic estimate for S is a sort of a "first derivative test", in that an exponential sum over each small (p-adic) neighborhood around m is estimated in terms of the value of (essentially) the first derivative of the phase. The estimate obtained for the local sum around m seriously depends on $\big\|\big(\omega+\Phi_1(m)\big)p^j\big\|$.

We proceed to exploit the given information about the distribution of values of Φ_1 to estimate the total sum of $e(\omega m)\Phi(m)$ over $\mathscr{M}$. Denoting $X = M_0/p^j+1$ and picking a parameter $Y>0$, we have by adapting a standard argument that

$$\begin{aligned} S &\ll \Phi_0 \cdot X \cdot \big|\{x \in \mathscr{M}_{(j)} : \Phi_1(x) \in (-\omega-Y, -\omega+Y)+p^{-j}\mathbb{Z}\}\big| \\ &\qquad + \Phi_0 \sum_{1 \leqslant r \ll p^{-j}Y^{-1}} \frac{1}{rY\cdot p^j} \cdot \big|\{x \in \mathscr{M}_{(j)} : \Phi_1(x) \in -\omega \pm (rY, (r+1)Y)+p^{-j}\mathbb{Z}\}\big| \\ &\ll p^\beta\Phi_0\left(\frac{Y}{p^{-\varphi}}+1\right)\left(X+\frac{1}{Yp^j}\log(2+p^{-j}Y^{-1})\right) \\ &\ll p^\beta\Phi_0\left(p^{\varphi-j}X^{-1}+1\right)\left(X+\frac{1}{X^{-1}}\log(2+X)\right) \\ &\ll \Phi_0\big(X+p^{\varphi-j}\big)p^\beta\log(2+X) \\ &\ll \Phi_0\big(M_0+p^\varphi+p^j\big)p^{\beta-j}\log(2+M_0), \end{aligned}$$

by choosing $Y = p^{-j}X^{-1}$. (We note that $\log(2+M_0)$ can be replaced by $\log(2+p^{(\varphi-j)^+})$, if desired, since at most $\mathrm{O}(p^{(\varphi-j)^+})$ terms in the above sum do not vanish. However, this is a minor point for us.)

Denoting $S(x) = \sum_{m \in \mathscr{M} \cap [M_1, x]} e(\omega m)\Phi(m)$, it follows by summation by parts that

$$\begin{aligned} \sum_{m \in \mathscr{M}} e(\omega m)\Phi(m)W(m) &= S(M_2)W(M_2) - \int_{M_1}^{M_2} S(t)W'(t)\,\mathrm{d}t \\ &\ll \Phi_0\big(M_0+p^\varphi+p^j\big)p^{\beta-j}\log(2+M_0)\left(|W(M_2)|+\int_{M_1}^{M_2}|W'(t)|\,\mathrm{d}t\right), \end{aligned}$$

which immediately implies the announced bound. □

The following theorem is our main result on p-adic van der Corput theory. Its proof combines Lemma 11 to estimate an exponential sum involving sufficiently well-understood p-adic fluctuations in terms of the frequency with which the derivative of the phase ($g_1(x)$ in the language of Theorem 5) enters a specific short "bad" range and Lemma 10 to control this frequency in terms of the size of the second derivative, $g_2(x)$, and information on the quality of the approximation.

Theorem 5 (Second derivative test). *Let $\omega\in\mathbb{R}$, let $\kappa_0,\phi,\lambda\in\mathbb{N}_0$ and $A\subseteq\mathbb{Z}_p$ be such that $(A+p^{\kappa_0}\mathbb{Z}_p)\subseteq A$, and let $f:A\to\mathbb{C}^\times$, $g_1:A\to p^{-\varphi}\mathbb{Z}_p$, $g_2:A\to p^{-\lambda}\mathbb{Z}_p^\times$, and $\Omega:\{\kappa\in\mathbb{N}_0:\kappa\geqslant\kappa_0\}\to\mathbb{N}_0$ be functions such that $|f(x)|\leqslant f_0$,*

$$f\big(x+p^\kappa t\big)=f(x)\theta\Big(g_1(x)\cdot p^\kappa t+\tfrac12 g_2(x)\cdot p^{2\kappa}t^2\Big)\boldsymbol{\mu}_{p^{\Omega(\kappa)}}$$

for every $x\in A$, $t\in\mathbb{Z}_p$, $\kappa\geqslant\kappa_0$, and

$$\Omega(\kappa)\leqslant(\lambda-2\kappa-1)^+\quad\text{for every }\kappa\geqslant\kappa_0.$$

Let $\mathscr{M}\subset A\cap\mathbb{Z}$ be the intersection of an interval $[M_1,M_2]$ with a union of arithmetic progressions modulo p^μ for some $\mu\in\mathbb{N}_0$. Let $\tilde\kappa=\max(\kappa_0,\mu)$, $\kappa_1=\max(\lambda/2,\kappa_0,\mu)$, $M_0=M_2-M_1$.

Then, for every continuously differentiable function $W:[M_1,M_2]\to\mathbb{C}$,

$$\sum_{m\in\mathscr{M}}e(\omega m)f(m)W(m)\ll f_0\big(M_0+p^\varphi+p^{\kappa_1}\big)\big(\|W\|_\infty+\|W'\|_1\big)p^{\min(\kappa_1-\lambda+\tilde\kappa,0)}\log(2+M_0).$$

Before proceeding to the proof, we note that Theorem 5 has been formulated with a number of parameters for flexibility in use. However, in a typical situation (thinking of f as an exponential with a p-adically analytic phase), the parameters κ_0 and μ will be small (for example, equal to 1): they account for the fact that f may have several different branches modulo a small power of p, that its true p-adic analytic nature shows up only in sufficiently small neighborhoods, or that we are summing only in specific congruence classes modulo a small power of p. The parameter λ, on the other hand, measures the size of the second derivative of the phase and will typically be large in a depth-aspect problem. For example, if f equals a primitive character χ of conductor p^n as in (2.2), then $\lambda=n$. Therefore, typically one has $\kappa_1=\lambda/2$. Moreover, Theorem 5 is proved by splitting the sum into arithmetic progressions of difference p^{κ_1}; thus, nontrivial information can be expected in the principal range $M_0\gg p^{\kappa_1}$. The upper bound provided by Theorem 5 is thus roughly $\ll M_0p^{-\lambda/2}=M_0\|g_2(x)\|_p^{-1/2}$; this is exactly what one expects from a second derivative test (compare with [14, Theorem 2.2]).

Proof. In light of $2\kappa_1-\lambda\geqslant0$ and $\Omega(\kappa_1)=0$, we have that

$$f\big(x+p^{\kappa_1}t\big)=f(x)\theta\big(g_1(x)\cdot p^{\kappa_1}t\big)$$

for every $x\in A$, $t\in\mathbb{Z}_p$. We will be applying Lemma 11 with $\Phi_1=g_1 \bmod p^{-\kappa_1}$ and $j=\kappa_1$.

According to Lemma 10, for every $\kappa_0\leqslant\kappa\leqslant\kappa_1$, we have that

$$g_1\big(x+p^\kappa t\big)-g_1(x)\in g_2(x)\cdot p^\kappa t+p^{-\kappa-\Omega(\kappa)}\mathbb{Z}_p$$

for every $x\in A$, $t\in\mathbb{Z}_p$.

From here, we claim that $g_1(x+p^\kappa t)-g_1(x)\in p^{-\kappa_1}\mathbb{Z}_p$ if and only if $g_2(x)\cdot p^\kappa t\in p^{-\kappa_1}\mathbb{Z}_p$. Note that this claim only depends on the value of the product $p^\kappa t$ (rather than on the separate values of $\kappa\in[\kappa_0,\kappa_1]$ and $t\in\mathbb{Z}_p$). Therefore, by rewriting $p^\kappa t=p^{\min(\kappa+\mathrm{ord}_p t,\kappa_1)}\cdot t/p^{\min(\mathrm{ord}_p t,\kappa_1-\kappa)}$, we may assume that $\kappa=\kappa_1$ or that $t\in\mathbb{Z}_p^\times$. We then distinguish two cases according to the value of $\Omega(\kappa)$. If $\Omega(\kappa)=0$ (as is the case when $\kappa=\kappa_1$), the claim is clear in light of $p^{-\kappa}\mathbb{Z}_p\subseteq p^{-\kappa_1}\mathbb{Z}_p$. Otherwise, we must have $t\in\mathbb{Z}_p^\times$ and $\Omega(\kappa)\leqslant\lambda-2\kappa-1$, in which case $-\kappa-\Omega(\kappa)>-\lambda+\kappa$ and our claim follows from $\mathrm{ord}_p\big(g_2(x)\cdot p^\kappa t+p^{-\kappa-\Omega(\kappa)}\mathbb{Z}_p\big)=-\lambda+\kappa=\mathrm{ord}_p\big(g_2(x)\cdot p^\kappa t\big)$.

Further, the condition that $g_2(x)\cdot p^\kappa t\in p^{-\kappa_1}\mathbb{Z}_p$ holds if and only if

$$t\in p^{(\lambda-\kappa-\kappa_1)^+}\mathbb{Z}_p.$$

In particular, $g_1(x+p^{\tilde\kappa}t)-g_1(x)\in p^{-\kappa_1}\mathbb{Z}_p$ if and only if

$$p^{\tilde\kappa}t\in p^{\max(\lambda-\kappa_1,\tilde\kappa)}\mathbb{Z}_p.$$

Let $\mathscr{M}_{(\kappa_1)}$ be a full set of representatives of those congruence classes modulo p^{κ_1} which occur in $\mathscr{M}$, and let $\mathscr{M}_{(\tilde\kappa)}$ be a subset of $\mathscr{M}_{(\kappa_1)}$ which is a full set of representatives of congruence classes modulo $p^{\tilde\kappa}$

occurring in $\mathscr{M}$. For every $f \in p^{-\varphi}\mathbb{Z}_p$, we have that

$$|\{x \in \mathscr{M}_{(\kappa_1)} : g_1(x) \in f + p^{-\kappa_1}\mathbb{Z}_p\}|$$
$$= \sum_{x \in \mathscr{M}_{(\tilde{\kappa})}} |\{t \in \mathbb{Z}/p^{\kappa_1 - \tilde{\kappa}}\mathbb{Z} : x + p^{\tilde{\kappa}}t \in \mathscr{M}_{(\kappa_1)},\, g_1\big(x + p^{\tilde{\kappa}}t\big) \in f + p^{-\kappa_1}\mathbb{Z}_p\}| \leqslant p^{\min(2\kappa_1 - \lambda + \tilde{\kappa}, \kappa_1)}.$$

Applying Lemma 11, we conclude that

$$\sum_{m \in \mathscr{M}} e(\omega m)\Phi(m)W(m) \ll f_0\big(M_0 + p^{\varphi} + p^{\kappa_1}\big)\big(\|W\|_\infty + \|W'\|_1\big)p^{\min(\kappa_1 - \lambda + \tilde{\kappa}, 0)} \log(2 + M_0),$$

as announced. □

9. Estimation of the sum of Ξ_{s_1,s_2}

In this final section, we prove Lemma 4 and thereby complete the proofs of Theorems 1 and 2. The sum Ξ_{s_1,s_2}, introduced in (5.16), will be estimated using the tools of Section 8. To prepare ground for this application, for any $0 \leqslant c < n$, denote $\nu = n - c$, and let, for $\varepsilon \in \{\pm 1\}$ and $x \in \alpha\mathbb{Z}_p^{\times 2}$,

$$\tilde{\Phi}_\nu^\varepsilon(x) := \chi\Big(\alpha + \tfrac{1}{2}p^{2\nu}x + \varepsilon p^\nu\big(\alpha x + \tfrac{1}{4}p^{2\nu}x^2\big)_{1/2}\Big)\theta\bigg(\frac{1}{p^c}\Big(\tfrac{1}{2}p^\nu x + \varepsilon\big(\alpha x + \tfrac{1}{4}p^{2\nu}x^2\big)_{1/2}\Big)\bigg). \tag{9.1}$$

Further, for any $(\varepsilon_1, \varepsilon_2) \in \{\pm 1\}^2$ and any $a_1, b_1, a_2, b_2 \in \mathbb{Z}_p^\times$ such that $a_1b_1a_2b_2 \in \mathbb{Z}_p^{\times 2}$, consider the function

$$\mathbf{\Phi}_{a_1,b_1,a_2,b_2,c}^{\varepsilon_1,\varepsilon_2}(x) := \tilde{\Phi}_{n-c}^{\varepsilon_1}\Big(\frac{x}{a_1b_1}\Big)\overline{\tilde{\Phi}_{n-c}^{\varepsilon_2}\Big(\frac{x}{a_2b_2}\Big)}. \tag{9.2}$$

For $s_1 = (a_1, b_1, k_1)$, $s_2 = (a_2, b_2, k_2)$ in the set S of Theorem 3, we also write $\mathbf{\Phi}_{s_1,s_2,c}^{\varepsilon_1,\varepsilon_2}(x) := \mathbf{\Phi}_{a_1,b_1,a_2,b_2,c}^{\varepsilon_1,\varepsilon_2}(x)$. With this notation, and denoting

$$\boldsymbol{W}_{s_1,s_2,c}(x) := W_{s_1,c}(x)\overline{W_{s_2,c}(x)},$$

where $W_{s,c}$ is the weight function from Lemma 2, which satisfies (5.14), we have by (5.16) and (7.1) that

$$\Xi_{s_1,s_2} = \sum_{(\varepsilon_1,\varepsilon_2) \in \{\pm 1\}^2} \sum_{\substack{m \leqslant q^{3\varepsilon}\mathcal{M} \\ \alpha b_1 m/a_1,\, \alpha b_2 m/a_2 \in \mathbb{Z}_p^{\times 2}}} \boldsymbol{\epsilon}_{s_1,s_2,c}^{\varepsilon_1,\varepsilon_2}(m)e\big(\omega_{s_1,s_2,c}m\big)\mathbf{\Phi}_{s_1,s_2,c}^{\varepsilon_1,\varepsilon_2}(m)\boldsymbol{W}_{s_1,s_2,c}(m), \tag{9.3}$$

where

$$\boldsymbol{\epsilon}_{s_1,s_2,c}^{\varepsilon_1,\varepsilon_2}(m) = \epsilon(\varepsilon_1(\alpha m\bar{a}_1\bar{b}_1)_{1/2}, p^\rho)\bar{\epsilon}(\varepsilon_2(\alpha m\bar{a}_2\bar{b}_2)_{1/2}, p^\rho)$$

(with $\rho \in \{0, 1\}$ being the parity of c) depends only on the class of m modulo p; in particular, $\boldsymbol{\epsilon}_{s_1,s_2,c}^{\varepsilon_1,\varepsilon_2}(m + p^\kappa t) = \boldsymbol{\epsilon}_{s_1,s_2,c}^{\varepsilon_1,\varepsilon_2}(m)$ for every $\kappa \geqslant 1$.

The following lemma will be essential in estimating Ξ_{s_1,s_2} in (9.3) using Theorem 5, the Second Derivative Test. Recall our convention from Section 2.1 regarding $\mathrm{ord}_p\, 0 = \infty$.

Lemma 12. *Let $0 \leqslant c < n$, let $a_1, b_1, a_2, b_2 \in \mathbb{Z}_p^\times$ be such that $a_1b_1a_2b_2 \in \mathbb{Z}_p^{\times 2}$. For any pair $(\varepsilon_1, \varepsilon_2) \in \{\pm 1\}^2$, there are $\Omega \in \mathbb{N}_0 \cup \{\infty\}$ and functions $g_{1,s_1,s_2,c}^{\varepsilon_1,\varepsilon_2}$, $g_{2,s_1,s_2,c}^{\varepsilon_1,\varepsilon_2} : \alpha a_1 b_1 \mathbb{Z}_p^{\times 2} \to p^\Omega\mathbb{Z}_p^\times$ such that the function $\mathbf{\Phi}_{a_1,b_1,a_2,b_2,c}^{\varepsilon_1,\varepsilon_2}(x)$ defined in (9.2) satisfies*

$$\mathbf{\Phi}_{s_1,s_2,c}^{\varepsilon_1,\varepsilon_2}\big(x + p^\kappa t\big) = \mathbf{\Phi}_{s_1,s_2,c}^{\varepsilon_1,\varepsilon_2}(x)\theta\left(\frac{1}{p^c}g_{1,s_1,s_2,c}^{\varepsilon_1,\varepsilon_2}(x) \cdot p^\kappa t + \frac{1}{2p^c}g_{2,s_1,s_2,c}^{\varepsilon_1,\varepsilon_2}(x) \cdot p^{2\kappa}t^2 + \mathbf{M}_{p^{\Omega + 3\kappa - c}}\right), \tag{9.4}$$

for every $x \in \alpha a_1 b_1 \mathbb{Z}_p^{\times 2}$, $\kappa \geqslant 1$, and $t \in \mathbb{Z}_p$.

Moreover, there are exactly two choices of $(\varepsilon_1, \varepsilon_2) \in \{\pm 1\}^2$ for which $\Omega = \mathrm{ord}_p(a_1b_1 - a_2b_2)$, while for the remaining two choices we have $\Omega = 0$.

Proof. First, we analyze the function $\tilde{\Phi}_\nu^\varepsilon(x)$ introduced in (9.1). Let, for brevity,

$$\gamma=\gamma(x)=\big(\alpha x+\tfrac14 p^{2\nu}x^2\big)_{1/2},$$
$$\beta=\beta(x)=\alpha+\tfrac12 p^{2\nu}x+\varepsilon p^\nu\gamma(x)=\alpha+\tfrac12 p^{2\nu}x+\varepsilon p^\nu\big(\alpha x+\tfrac14 p^{2\nu}x^2\big)_{1/2},$$

so that

$$\tilde{\Phi}_\nu^\varepsilon(x)=\chi(\beta(x))\theta\Big(\frac{1}{p^c}\big(\tfrac12 p^\nu x+\varepsilon\gamma(x)\big)\Big). \tag{9.5}$$

Recalling the expansion (2.7) and (2.1), we find that

$$\begin{aligned}\gamma(x+p^\kappa t)&=\Big(\alpha(x+p^\kappa t)+\tfrac14 p^{2\nu}(x+p^\kappa t)^2\Big)_{1/2}\\ &=\Big(\big(\alpha x+\tfrac14 p^{2\nu}x^2\big)+\big(\alpha p^\kappa t+\tfrac12 p^{2\nu+\kappa}xt+\tfrac14 p^{2\kappa+2\nu}t^2\big)\Big)_{1/2}\\ &=\gamma+\frac{1}{2\gamma}\big(\alpha p^\kappa t+\tfrac12 p^{2\nu+\kappa}xt+\tfrac14 p^{2\kappa+2\nu}t^2\big)-\frac{1}{8\gamma^3}\big(\alpha p^\kappa t+\tfrac12 p^{2\nu+\kappa}xt\big)^2+\mathbf{M}_{p^{3\kappa}}[x,t]\\ &=\gamma+\frac{1}{2\gamma}\big(\alpha+\tfrac12 p^{2\nu}x\big)p^\kappa t+\frac{1}{8\gamma^3}\Big(\big(\alpha x+\tfrac14 p^{2\nu}x^2\big)p^{2\nu}-\big(\alpha+\tfrac12 p^{2\nu}x\big)^2\Big)p^{2\kappa}t^2+\mathbf{M}_{p^{3\kappa}}[x,t]\\ &=\gamma+\frac{1}{2\gamma}\big(\alpha+\tfrac12 p^{2\nu}x\big)p^\kappa t-\frac{1}{8\gamma^3}\alpha^2p^{2\kappa}t^2+\mathbf{M}_{p^{3\kappa}}[x,t].\end{aligned}$$

Further, recalling also (2.3) as well as $\kappa,\nu\geqslant 1$, $\kappa+\nu\geqslant 2$, we conclude that

$$\begin{aligned}&\chi\big(\beta(x+p^\kappa t)\big)\\ &\quad=\chi\Big(\alpha+\tfrac12 p^{2\nu}(x+p^\kappa t)+\varepsilon p^\nu\cdot\gamma(x+p^\kappa t)\Big)\\ &\quad=\chi\Big(\alpha+\tfrac12 p^{2\nu}x+\tfrac12 p^{2\nu+\kappa}t+\varepsilon p^\nu\gamma+\frac{\varepsilon}{2\gamma}\big(\alpha+\tfrac12 p^{2\nu}x\big)p^{\kappa+\nu}t-\frac{\varepsilon}{8\gamma^3}\alpha^2p^{2\kappa+\nu}t^2+\mathbf{M}_{p^{3\kappa+\nu}}[x,t]\Big)\\ &\quad=\chi(\beta)\theta\Big(\frac{\alpha}{\beta p^n}\Big(\frac{\varepsilon}{2\gamma}\cdot\big[\alpha+\varepsilon\gamma p^\nu+\tfrac12 p^{2\nu}x\big]p^{\kappa+\nu}t-\frac{\varepsilon}{8\gamma^3}\alpha^2p^{2\kappa+\nu}t^2\Big)\\ &\qquad\qquad-\frac{\alpha}{8\beta^2\gamma^2p^n}\big[\alpha+\varepsilon\gamma p^\nu+\tfrac12 p^{2\nu}x\big]^2p^{2\kappa+2\nu}t^2+\mathbf{M}_{p^{3\kappa+\nu-n}}[x,t]\Big)\\ &\quad=\chi(\beta)\theta\Big(\frac{\varepsilon\alpha}{2\gamma p^n}p^{\kappa+\nu}t-\frac{\alpha}{8\gamma^2p^n}p^{2\kappa+2\nu}t^2-\frac{\varepsilon\alpha}{8\beta\gamma^3p^n}\cdot\alpha^2p^{2\kappa+\nu}t^2+\mathbf{M}_{p^{3\kappa+\nu-n}}[x,t]\Big)\\ &\quad=\chi(\beta)\theta\Big(\frac{\varepsilon\alpha}{2\gamma p^n}p^{\kappa+\nu}t-\frac{\varepsilon\alpha}{8\gamma^3p^n}\big(\alpha+\tfrac12 p^{2\nu}x\big)p^{2\kappa+\nu}t^2+\mathbf{M}_{p^{3\kappa+\nu-n}}[x,t]\Big),\end{aligned}\tag{9.6}$$

since

$$\begin{aligned}\frac{\alpha^2}{\beta\gamma^3}+\frac{\varepsilon p^\nu}{\gamma^2}&=\frac{1}{\beta\gamma^3}\big(\alpha^2+\varepsilon\beta\gamma p^\nu\big)=\frac{1}{\beta\gamma^3}\Big(\alpha^2+\varepsilon\big(\alpha+\tfrac12 p^{2\nu}x\big)\gamma p^\nu+\gamma^2p^{2\nu}\Big)\\ &=\frac{1}{\beta\gamma^3}\Big(\big(\alpha+\tfrac12 p^{2\nu}x\big)^2+\varepsilon\big(\alpha+\tfrac12 p^{2\nu}x\big)\gamma p^\nu\Big)=\frac{\beta}{\beta\gamma^3}\big(\alpha+\tfrac12 p^{2\nu}x\big)=\frac{1}{\gamma^3}\big(\alpha+\tfrac12 p^{2\nu}x\big).\end{aligned}$$

We also obtain, with $c = n - \nu$,

$$\begin{aligned}
&\theta\Big(\frac{1}{p^c}\big(\tfrac{1}{2}p^{\nu}(x+p^{\kappa}t)+\varepsilon\cdot\gamma(x+p^{\kappa}t)\big)\Big)\\
&=\theta\Big(\frac{1}{p^c}\big(\tfrac{1}{2}p^{\nu}x+\tfrac{1}{2}p^{\kappa+\nu}t+\varepsilon\gamma+\frac{\varepsilon}{2\gamma}(\alpha+\tfrac{1}{2}p^{2\nu}x)p^{\kappa}t-\frac{\varepsilon}{8\gamma^3}\alpha^2p^{2\kappa}t^2\big)+\mathbf{M}_{p^{3\kappa-c}}[x,t]\Big)\\
&=\theta\Big(\frac{1}{p^c}\big(\tfrac{1}{2}p^{\nu}x+\varepsilon\gamma\big)\Big)\theta\Big(\frac{\varepsilon}{2\gamma p^n}(\alpha+\tfrac{1}{2}p^{2\nu}x)p^{\kappa+\nu}t+\frac{1}{2p^n}p^{\kappa+2\nu}t-\frac{\varepsilon}{8\gamma^3p^n}\alpha^2p^{2\kappa+\nu}t^2+\mathbf{M}_{p^{3\kappa-c}}[x,t]\Big)\\
&=\theta\Big(\frac{1}{p^c}\big(\tfrac{1}{2}p^{\nu}x+\varepsilon\gamma\big)\Big)\theta\Big(\frac{\varepsilon}{2\gamma p^n}\beta p^{\kappa+\nu}t-\frac{\varepsilon}{8\gamma^3p^n}\alpha^2p^{2\kappa+\nu}t^2+\mathbf{M}_{p^{3\kappa+\nu-n}}[x,t]\Big).
\end{aligned} \tag{9.7}$$

Combining (9.5), (9.6), and (9.7), we find that the function $\tilde{\Phi}^{\varepsilon}_{\nu}(x)$ satisfies

$$\begin{aligned}
\tilde{\Phi}^{\varepsilon}_{\nu}(x+p^{\kappa}t)&=\tilde{\Phi}^{\varepsilon}_{\nu}(x)\theta\Big(\frac{\varepsilon}{2\gamma p^n}(\alpha+\beta)p^{\kappa+\nu}t-\frac{\varepsilon\alpha}{8\gamma^3p^n}(2\alpha+\tfrac{1}{2}p^{2\nu}x)p^{2\kappa+\nu}t^2+\mathbf{M}_{p^{3\kappa+\nu-n}}[x,t]\Big)\\
&=\tilde{\Phi}^{\varepsilon}_{\nu}(x)\theta\Big(\frac{1}{xp^n}\big(\varepsilon\gamma+\tfrac{1}{2}xp^{\nu}\big)p^{\kappa+\nu}t-\frac{\varepsilon\alpha}{4x\gamma p^n}p^{2\kappa+\nu}t^2+\mathbf{M}_{p^{3\kappa+\nu-n}}[x,t]\Big),
\end{aligned} \tag{9.8}$$

since

$$2\alpha+\tfrac{1}{2}p^{2\nu}x=2x^{-1}\gamma^2,\quad \alpha+\beta=2\alpha+\tfrac{1}{2}p^{2\nu}x+\varepsilon p^{\nu}\gamma=\gamma\cdot(2x^{-1}\gamma+\varepsilon p^{\nu}).$$

In particular, (9.8) shows that $\mathbf{\Phi}^{\varepsilon_1,\varepsilon_2}_{s_1,s_2,c}$ satisfies

$$\begin{aligned}
\mathbf{\Phi}^{\varepsilon_1,\varepsilon_2}_{s_1,s_2,c}(x+p^{\kappa}t)=\mathbf{\Phi}^{\varepsilon_1,\varepsilon_2}_{s_1,s_2,c}(x)\theta\Big(&\frac{1}{xp^c}\Big(\varepsilon_1\gamma\Big(\frac{x}{a_1b_1}\Big)-\varepsilon_2\gamma\Big(\frac{x}{a_2b_2}\Big)+\frac{x}{2}\Big(\frac{1}{a_1b_1}-\frac{1}{a_2b_2}\Big)p^{\nu}\Big)p^{\kappa}t\\
&-\frac{\alpha}{4xp^c}\Big(\frac{\varepsilon_1}{a_1b_1\gamma(x/a_1b_1)}-\frac{\varepsilon_2}{a_2b_2\gamma(x/a_2b_2)}\Big)p^{2\kappa}t^2+\mathbf{M}_{p^{3\kappa+\nu-n}}\Big)
\end{aligned}$$

for every $x\in\alpha a_1b_1\mathbb{Z}_p^{\times 2}$ and every $\kappa\geqslant 1$. We write the above equation as

$$\mathbf{\Phi}^{\varepsilon_1,\varepsilon_2}_{s_1,s_2,c}(x+p^{\kappa}t)=\mathbf{\Phi}^{\varepsilon_1,\varepsilon_2}_{s_1,s_2,c}(x)\theta\left(\frac{1}{p^c}g^{\varepsilon_1,\varepsilon_2}_{1,s_1,s_2,c}(x)\cdot p^{\kappa}t+\frac{1}{2p^c}g^{\varepsilon_1,\varepsilon_2}_{2,s_1,s_2,c}(x)\cdot p^{2\kappa}t^2+\mathbf{M}_{p^{3\kappa+\nu-n}}\right), \tag{9.9}$$

with the obvious definitions for $g^{\varepsilon_1,\varepsilon_2}_{1,s_1,s_2,c}(x)$ and $g^{\varepsilon_1,\varepsilon_2}_{2,s_1,s_2,c}(x)$.

It remains to find $\mathrm{ord}_p\, g^{\varepsilon_1,\varepsilon_2}_{1,s_1,s_2,c}(x)$ and $\mathrm{ord}_p\, g^{\varepsilon_1,\varepsilon_2}_{2,s_1,s_2,c}(x)$. For every $u,v\in\mathbb{Z}_p^{\times}$, we make the trivial remark that

$$(u+v)(u-v)=u^2-v^2,\quad (u^{-1}+v^{-1})(u^{-1}-v^{-1})=-(uv)^{-2}(u^2-v^2).$$

For odd p, it is immediate from here that exactly one of $\mathrm{ord}_p(u+v)$ and $\mathrm{ord}_p(u-v)$ equals $\mathrm{ord}_p(u^2-v^2)$, while the other one is zero, and similarly for $\mathrm{ord}_p(u^{-1}+v^{-1})$ and $\mathrm{ord}_p(u^{-1}-v^{-1})$. (Note that this holds even if $u^2=v^2$, when $\mathrm{ord}_p(u^2-v^2)=\infty$.) Applying this argument with

$$(u,v)=\Big(\gamma\Big(\frac{x}{a_1b_1}\Big),\gamma\Big(\frac{x}{a_2b_2}\Big)\Big)=\Big(\Big(\frac{\alpha x}{a_1b_1}+\frac{p^{2\nu}x^2}{4a_1^2b_1^2}\Big)_{1/2},\Big(\frac{\alpha x}{a_2b_2}+\frac{p^{2\nu}x^2}{4a_2^2b_2^2}\Big)_{1/2}\Big)$$

and $(u',v')=\big(a_1b_1u,a_2b_2v\big)$, respectively, where

$$u^2-v^2,\ u'^2-v'^2\in(a_1b_1-a_2b_2)\mathbb{Z}_p^{\times},\quad \varepsilon_1u'-\varepsilon_2v'=a_1b_1(\varepsilon_1u-\varepsilon_2v)+\varepsilon_2v(a_1b_1-a_2b_2),$$

it follows that there are exactly two choices of $(\varepsilon_1,\varepsilon_2)\in\{\pm1\}^2$ for which

$$\mathrm{ord}_p\, g^{\varepsilon_1,\varepsilon_2}_{1,s_1,s_2,c}(x)=\mathrm{ord}_p\, g^{\varepsilon_1,\varepsilon_2}_{2,s_1,s_2,c}(x)=\mathrm{ord}_p(a_1b_1-a_2b_2),$$

while for the remaining two choices we have

$$\mathrm{ord}_p\, g^{\varepsilon_1,\varepsilon_2}_{1,s_1,s_2,c}(x)=\mathrm{ord}_p\, g^{\varepsilon_1,\varepsilon_2}_{2,s_1,s_2,c}(x)=0.$$

Let $\Omega=\mathrm{ord}_p\, g^{\varepsilon_1,\varepsilon_2}_{1,s_1,s_2,c}(x)=\mathrm{ord}_p\, g^{\varepsilon_1,\varepsilon_2}_{2,s_1,s_2,c}(x)$.

It remains to prove (9.4). This is already established in (9.9) when $\Omega = 0$. If $\Omega > 0$, then

$$\frac{\alpha x}{a_1 b_1} + \frac{p^{2\nu} x^2}{4a_1^2 b_1^2} \equiv \frac{\alpha x}{a_2 b_2} + \frac{p^{2\nu} x^2}{4a_2^2 b_2^2} \pmod{p},$$

and we may assume that the same branch of the square-root is in $\tilde{\Phi}_{n-c}^{\varepsilon_1}(x/a_1b_1)$ and $\tilde{\Phi}_{n-c}^{\varepsilon_2}(x/a_2b_2)$. In that case, $\Omega > 0$ is achieved when $\varepsilon_1 = \varepsilon_2$, so that (9.4) follows from (9.8) upon recalling that $(a_1b_1)^{-1} \equiv (a_2b_2)^{-1} \pmod{p^\Omega}$. We remark that the equation (9.4) is the ultimate fruit of the more precise bookkeeping required by Definition 1. □

We complete our work with the *proof of Lemma 4*. First, we split the sum in (9.3) as

$$\Xi_{s_1,s_2} = \sum_{\Omega \in \{0, \mathrm{ord}_p(a_1b_1 - a_2b_2)\}} \Xi_{s_1,s_2,\Omega} \tag{9.10}$$

according to the value of Ω in the expansion (9.4) for the function $\boldsymbol{\Phi}_{s_1,s_2,c}^{\varepsilon_1;\varepsilon_2}$ corresponding to $(\varepsilon_1, \varepsilon_2)$. In the case $\Omega \leqslant c-2$ (so in particular $a_1b_1 \neq a_2b_2$) we apply Theorem 5 with

$$\varphi = \lambda = c - \Omega, \quad \Omega(\kappa) = (c - \Omega - 3\kappa)^+, \quad \omega = \omega_{s_1,s_2,c}$$

$$\tilde{\kappa} = \mu = \kappa_0 = 1, \quad \kappa_1 = \max(\lambda/2, 1) = \frac{c-\Omega}{2}, \quad M_1 = 1, \quad M_2 = q^{3\varepsilon}\mathcal{M}$$

and note that by (5.14) the archimedean weight $W := \boldsymbol{W}_{s_1,s_2,c}$ satisfies $\|W\|_\infty + \|W'\|_1 \ll Z^2 q^{13\varepsilon}$. We obtain

$$\Xi_{s_1,s_2,\Omega} \ll q^{17\varepsilon} Z^2 \left(\mathcal{M} + p^{c-\Omega}\right) p^{-\frac{c-\Omega}{2}+1}, \tag{9.11}$$

and the first bound of Lemma 4 follows. In the case $c - 1 \leqslant \Omega \leqslant \infty$, one cannot expect a sharp result from the application of the second derivative test. Here we estimate trivially $\Xi_{s_1,s_2,\Omega} \ll q^{9\varepsilon}\mathcal{M}$, which yields the second estimate. (Although in many cases far from optimal, this is the only available estimate in the case $\Omega = \infty$, that is, $a_1b_1 = a_2b_2$.) □

References

[1] M. B. Barban, Yu.V. Linnik, N.G. Tshudakov, *On prime numbers in an arithmetic progression with a prime-power difference*, Acta Arith. **9** (1964), 375-390

[2] V. Blomer, G. Harcos, *Hybrid bounds for twisted L-functions*, J. Reine Angew. Math. **621** (2008), 53-79; addendum, ibid., to appear

[3] V. Blomer, R. Khan, M. Young, *Distribution of mass of holomorphic cusp forms*, Duke Math. J. **162** (2013), 2609-2644

[4] V. Blomer, P. Michel, *Hybrid bounds for automorphic forms on ellipsoids over number fields*, J. Math. Inst. Jussieu **12** (2013), 727-758

[5] V. Blomer, D. Milićević, *Kloosterman sums in residue classes*, J. Eur. Math. Soc., to appear

[6] D. A. Burgess, *On character sums and L-series. II*, Proc. London Math. Soc. **13** (1963), 524-536

[7] V. Bykovskii, *A trace formula for the scalar product of Hecke series and its applications*, J. Math. Sci. (New York) **89** (1998), 915-932.

[8] B. Conrey, H. Iwaniec, *The cubic moment of central values of automorphic L-functions*, Ann. of Math. **151** (2000), 1175-1216

[9] E. Fouvry, E. Kowalski, P. Michel, *Algebraic twists of modular forms and Hecke orbits*, preprint

[10] E. Fouvry, E. Kowalski, P. Michel, *Algebraic trace functions over the primes*, Duke Math. J., to appear

[11] G. Harcos, N. Templier, *On the sup-norm of Maass cusp forms of large level: III*, Math. Ann. **356** (2013), 209-216.

[12] A. Good, *The square mean of Dirichlet series associated with cusp forms*, Mathematika **29** (1982/83), 278-295

[13] I. S. Gradshteyn, I. M. Ryzhik, *Table of integrals, series, and products*, Academic Press Inc. 2000

[14] S. W. Graham, G. Kolesnik, *van der Corput's method of exponential sums*, London Mathematical Society Lecture Note Series, Cambridge University Press, Cambridge, 1991

[15] D. R. Heath-Brown, *Hybrid bounds for Dirichlet L-functions*, Invent. Math. **47** (1978), 149-170

[16] G. Harcos, P. Michel, *The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points. II*, Invent. math. **163** (2006), 581-655

[17] H. Iwaniec, *Topics in classical automorphic forms*, Graduate Texts in Mathematics **17** (1997), AMS, Providence, RI

[18] H. Iwaniec, E. Kowalski, *Analytic Number Theory*, Colloquium Publication **53** (2004), AMS, Providence, RI
[19] H. Iwaniec, P. Michel, *The second moment of the symmetric square L-functions*, Ann. Acad. Scient. Fenn. Math. **26** (2001), 465-482.
[20] M. Jutila, *Lectures on a Method in the Theory of Exponential Sums*, Tata Inst. Fund. Res. Lectures on Math. and Phys. **80**, Springer-Verlag, Berlin, 1987.
[21] M. Jutila, Y. Motohashi, *Uniform bound for Hecke L-functions*, Acta Math. **195** (2005), 61-115
[22] E. Kowalski, P. Michel, J. VanderKam, *Rankin-Selberg L-functions in the level aspect*, Duke Math. J. **114** (2002), 123-191.
[23] E. Landau, *Über die ζ-Funktion und die L-Funktionen*, Math. Z. **20** (1924), 105-125
[24] J. E. Littlewood, *Researches in the theory of the Riemann ζ-function*, Proc. Lond. Math. Soc. (2) **20** (1922), Records, page xxiv
[25] T. Meurman, *On the order of the Maass L-function on the critical line*, in: Number Theory, Vol. I (Budapest, 1987), pp. 325-354. Colloq. Math. Soc. János Bolyai **51**, North-Holland, Amsterdam, 1990.
[26] D. Milićević, *Sub-Weyl subconvexity for Dirichlet L-functions to prime power moduli*, preprint
[27] R. Munshi, *Bounds for twisted symmetric square L-functions III*, Adv. in Math. **235** (2013), 74-91
[28] A. Venkatesh, *Sparse equidistribution problems, period bounds, and subconvexity*, Ann. of Math. **172** (2010), 989-1094.
[29] P. Vishe, *A fast algorithm to compute $L(1/2, f \times \chi)$*, J. Number Theory **133** (2013), 1502-1524.
[30] H. Weyl, *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Ann. **77** (1916), 313-352.

Mathematisches Institut, Bunsenstr. 3-5, D-37073 Göttingen, Germany
E-mail address: `blomer@uni-math.gwdg.de`

Bryn Mawr College, Department of Mathematics, 101 North Merion Avenue, Bryn Mawr, PA 19010, U.S.A.
E-mail address: `dmilicevic@brynmawr.edu`