Geom. Funct. Anal. Vol. 25 (2015) 580–657
DOI: 10.1007/s00039-015-0310-2
Published online February 10, 2015

GAFA Geometric And Functional Analysis

ALGEBRAIC TWISTS OF MODULAR FORMS AND HECKE ORBITS

Étienne Fouvry, Emmanuel Kowalski and Philippe Michel

Dedicated to Peter Sarnak on his 61st birthday, with admiration

Abstract. We consider the question of the correlation of Fourier coefficients of modular forms with functions of algebraic origin. We establish the absence of correlation in considerable generality (with a power saving of Burgess type) and a corresponding equidistribution property for twisted Hecke orbits. This is done by exploiting the amplification method and the Riemann Hypothesis over finite fields, relying in particular on the ℓ-adic Fourier transform introduced by Deligne and studied by Katz and Laumon.

Contents

1 Introduction and Statement of Results

This paper concerns a certain type of sums involving Fourier coefficients of modular forms, which we call "algebraic twists". Their study can be naturally motivated

Keywords and phrases: Modular forms, Fourier coefficients, Hecke eigenvalues, Hecke orbits, horocycles, ℓ-adic Fourier transform, Riemann Hypothesis over finite fields

Mathematics Subject Classification: 11F11,11F32,11F37,11T23,11L05

P. Michel was partially supported by the SNF (grant 200021-137488) and the ERC (Advanced Research Grant 228304). É. Fouvry thanks ETH Zürich, EPF Lausanne and the Institut Universitaire de France for financial support.

either from a point of view coming from analytic number theory, or from geometric considerations involving Hecke orbits on modular curves. We will present them using the first approach, and discuss the geometric application in Section 2.3.

We will be considering either holomorphic cusp forms or Maass forms. Precisely, the statement f *is a cusp form* will mean, unless otherwise indicated, that f is either (1) a non-zero holomorphic cusp form of some even weight $k \geqslant 2$ (sometimes denoted k_f) and some level $N \geqslant 1$; or (2) a non-zero Maass cusp form of weight 0, level N and Laplace eigenvalue written $1/4 + t_f^2$. In both cases, we assume f has trivial Nebentypus for simplicity.

The statement that a cusp form f of level N is *a Hecke eigenform* will also, unless otherwise indicated, mean that f is an eigenfunction of the Hecke operators T_n with $(n, N) = 1$.

1.1 Algebraic twists of modular forms. Let $f : \mathbf{H} \to \mathbf{C}$ be a cusp form (as discussed above). We have $f(z+1) = f(z)$, so f that admits a Fourier expansion at infinity, and we denote the n-th Fourier coefficient of f by $\varrho_f(n)$. Explicitly, if f is holomorphic of weight k, the Fourier expansion takes the form

$$f(z) = \sum_{n \geqslant 1} n^{(k-1)/2} \varrho_f(n) e(nz),$$

and if f is a Maass form, the Fourier expansion is normalized as in (3.8) below. It follows from Rankin-Selberg theory that the Fourier coefficients $\varrho_f(n)$ are bounded on average, namely

$$\sum_{n \leqslant x} |\varrho_f(n)|^2 = c_f x + O(x^{3/5}) \tag{1.1}$$

for some $c_f > 0$. For individual terms, we have

$$\varrho_f(n) \ll_{\varepsilon, f} n^{7/64+\varepsilon} \tag{1.2}$$

for any $\varepsilon > 0$ by the work of Kim and Sarnak [KS03], and moreover, if f is holomorphic, it follows from Deligne's proof of the Ramanujan-Petersson conjecture that the $\varrho_f(n)$ are almost bounded, so that

$$\varrho_f(n) \ll_{\varepsilon, f} n^{\varepsilon}$$

for any $\varepsilon > 0$.

On the other hand, it is also well-known that the Fourier coefficients oscillate quite substantially, as the estimate

$$\sum_{n \leqslant x} \varrho_f(n) e(\alpha n) \ll x^{1/2} (\log 2x) \tag{1.3}$$

valid for $x \geqslant 1$ and $\alpha \in \mathbf{R}$, with an implied constant depending on f only, shows (see, e.g., [Iwa97, Th. 5.3] and [Iwa95, Th. 8.1]).

One may ask, more generally, whether the sequence $(\varrho_f(n))_{n\geqslant 1}$ *correlates* with another bounded (or essentially bounded) sequence $K(n)$. This may be defined formally as follows: $(K(n))$ does *not* correlate with the Fourier coefficients of f if we have

$$\sum_{n\leqslant x}\varrho_f(n)K(n)\ll x(\log x)^{-A}$$

for all $A\geqslant 1$, the implied constant depending on A.[1] There are many known examples, of which we list only a few particularly interesting ones:

- For $K(n)=\mu(n)$, the Möbius function, the non-correlation is an incarnation of the Prime Number Theorem, and is a consequence of the non-vanishing of the Hecke L-function $L(f,s)$ for $\Re s=1$ when f is primitive; more generally, for $K(n)=\mu(n)e(n\alpha)$ where $\alpha\in\mathbf{R}/\mathbf{Z}$, non-correlation has been obtained recently by Fouvry and Ganguly [FG14];
- When $K(n)=\overline{\varrho_g(n)}$ for g any modular form which is orthogonal to f, non-correlation is provided by Rankin-Selberg theory;
- For $K(n)=\varrho_g(n+h)$ with $h\neq 0$ and g any modular form, whether it is orthogonal to f or not, non-correlation follows from the study of *shifted-convolution sums*, and has crucial importance in many studies of automorphic L-functions.

In this paper we are interested in the absence of correlation of the coefficients $(\varrho_f(n))_n$ against sequences $(K(n))_{n\geqslant 1}$ where

$$K\,:\,\mathbf{Z}/p\mathbf{Z}\to\mathbf{C}$$

is a function defined modulo p, for some prime p, which is extended to all of $\mathbf{Z}$ by periodicity. We will then consider sums of the shape

$$\sum_{n\leqslant p}\varrho_f(n)K(n),$$

or rather smoothed versions of these, which we denote

$$\mathcal{S}(f,K;p)=\mathcal{S}_V(f,K;p)=\sum_{n\geqslant 1}\varrho_f(n)K(n)V(n/p),$$

for V a smooth compactly supported function on $]0,+\infty[$ (often V will be omitted from the notation).

By (1.1), the trivial bound for these sums is

$$\mathcal{S}(f,K;p)\ll p\left(\frac{1}{p}\sum_{n\leqslant p}|K(n)|^2\right)^{1/2}\ll p\max_{1\leqslant n\leqslant p}|K(n)|,$$

[1] It is not enough to ask that the sum be $o(x)$ because this is then true for $K(n)$ equal to the sign of $\varrho_f(n)$, see for instance [EMS84].

where the implied constant depends on f and V, and our aim will be to improve this bound; we will prove estimates of the shape

$$\mathcal{S}(f, K; p) \ll p^{1-\delta} \tag{1.4}$$

for some absolute $\delta > 0$, where the implied constant depends only on f, V and easily controlled invariants of K, such as

$$\|K\|_2 = \left(\frac{1}{p}\sum_{n \leqslant p} |K(n)|^2\right)^{1/2} \quad \text{or} \quad \|K\|_\infty = \max |K(n)|.$$

A first (slightly degenerate) example is a (normalized) *Dirac* function located at some $u \in \mathbf{F}_p$, i.e., $K(n) = p^{1/2}\delta_{n \equiv u \,(\mathrm{mod}\, p)}$. Here $\|K\|_\infty = p^{1/2}$ is large, but $\|K\|_2 = 1$ and

$$\mathcal{S}(f, K; p) = p^{1/2} \sum_{n \equiv u \,(\mathrm{mod}\, p)} \varrho_f(n) V(n/p) \ll p^{1-\delta} \tag{1.5}$$

for any $\delta < 1 - 7/64$ by (1.2).

Another non-trivial choice (somewhat simpler than the previous one) is an additive character modulo p given by $K(n) = e(an/p)$ for some fixed $a \in \mathbf{Z}$. In that case, $|K(n)| \leqslant 1$ and the bound (1.3) gives (1.4) for any $\delta < 1/2$, with an implied constant depending only on f and V.

A third interesting example is given by $K(n) = \chi(n)$, where χ is a non-trivial Dirichlet character modulo p (extended by 0 at p). In that case, the bound (1.4), with an implied constant depending only on f and V, is essentially equivalent to a *subconvex* bound for the twisted L-function $L(f \otimes \chi, s)$ in the level aspect, i.e., to a bound

$$L(f \otimes \chi, s) \ll_{s,f} p^{1/2-\delta'},$$

for some $\delta' > 0$ and any fixed s on the critical line. Such an estimate was obtained for the first time by Duke-Friedlander-Iwaniec in [DFI93] for any $\delta' < 1/22$. This bound was subsequently improved to any $\delta' < 1/8$ (a Burgess type exponent) by Bykovski and Blomer-Harcos[2] [Byk98, BH08], and to $\delta' < 1/6$ (a Weyl type exponent) when χ is quadratic by Conrey-Iwaniec [CI00].

There are many other functions which occur naturally. We highlight two types here. First, given rational functions ϕ_1, ϕ_2, say

$$\phi_i(X) = \frac{R_i(X)}{S_i(X)} \in \mathbf{Q}(X), \quad i = 1, 2$$

[2] We are very grateful to G. Harcos for pointing out the relevance of these two papers for the present one.

with $R_i,\ S_i \in \mathbf{Z}[X]$ coprime (in $\mathbf{Q}[X]$), and given a non-trivial Dirichlet character $\chi \pmod p$, one can form

$$K(n) = \begin{cases} e\left(\frac{\phi_1(n)}{p}\right)\chi(\phi_2(n)), & \text{if } p \nmid S_1(n)S_2(n), \\ 0, & \text{otherwise,} \end{cases} \tag{1.6}$$

where inverses are computed modulo p and with the usual convention $\chi(0) = 0$. We will show that (1.4) holds for such functions with an absolute exponent of Burgess type (see Corollary 2.2 below). The proof depends ultimately on the Riemann Hypothesis over finite fields, which is applied in order to estimate exponential sums in 3 variables with square-root cancellation, using Deligne's results [Del80].

Second, for $m \geqslant 1$ and $a \in \mathbf{F}_p^\times$ let

$$\mathrm{Kl}_m(a;p) = \frac{1}{p^{\frac{m-1}{2}}} \sum_{\substack{x_1 \dots x_m = a \\ x_i \in \mathbf{F}_p}} \cdots \sum e\left(\frac{x_1 + \cdots + x_m}{p}\right)$$

be the normalized hyper-Kloosterman sum in $m-1$ variables. Recall that by the work of Deligne [Del77, Sommes Trig., (7.1.3)] we have

$$|\mathrm{Kl}_m(a;p)| \leqslant m,$$

and sums involving Kloosterman sums or hyper-Kloosterman sums are frequent visitors of analytic number theorists. Consider now, for $\phi = \frac{R(X)}{S(X)} \in \mathbf{Q}[X]$ a non-constant rational function with $R, S \in \mathbf{Z}[X]$, $S \neq 0$ and $\Phi(U,V) \in \mathbf{C}[U,V]$ a polynomial in two variables, the function

$$K(n) = \begin{cases} \Phi\big(\mathrm{Kl}_m(\phi(n);p), \overline{\mathrm{Kl}_m(\phi(n);p)}\big), & \text{if } p \nmid S(n) \\ 0 & \text{otherwise.} \end{cases} \tag{1.7}$$

We will also show a bound of the type (1.4) for these rather wild functions.

The precise common feature of these examples is that they arise as linear combination of *Frobenius trace functions* of certain ℓ-adic sheaves over the affine line $\mathbf{A}^1_{\mathbf{F}_p}$ (for some prime $\ell \neq p$). We therefore call these functions *trace functions*, and we give the precise definition below. To state our main result, it is enough for the moment to know that we can measure the complexity of a trace function modulo p with a numerical invariant called its *conductor* $\mathrm{cond}(K)$. Our result is, roughly, that when $\mathrm{cond}(K)$ remains bounded, $K(n)$ does not correlate with Fourier coefficients of modular forms.

As a last step before stating our main result, we quantify the properties of the test function V that we handle. Given $P > 0$ and $Q \geqslant 1$ real numbers, we define:

Definition 1.1 (Condition $(V(C,P,Q))$). *Let $P > 0$ and $Q \geqslant 1$ be real numbers and let $C = (C_\nu)_{\nu \geqslant 0}$ be a sequence of non-negative real numbers. A smooth compactly supported function V on $[0, +\infty[$ satisfies* Condition $(V(C,P,Q))$ *if*

(1) *The support of V is contained in the dyadic interval $[P, 2P]$;*
(2) *For all $x > 0$ and all integers $\nu \geqslant 0$ we have the inequality*

$$\left| x^\nu V^{(\nu)}(x) \right| \leqslant C_\nu Q^\nu.$$

In particular, $|V(x)| \leqslant C_0$ for all x.

Remark. A smooth dyadic sum corresponds to cases where $P = 1/2$ and Q is absolutely bounded. This is the most important situation to consider, in a first reading at least. In other situations, we have in mind that PQ is also absolutely bounded.

As a referee pointed out, the sequence $C = (C_\nu)_{\nu \geqslant 0}$ should grow sufficiently fast in order for the set of functions satisfying $(V(C, P, Q))$ be non-trivial: for instance if $(C_\nu)_{\nu \geqslant 0}$, any such function V would have to be analytic hence identically zero since compactly supported.

Our main result is:

Theorem 1.2. *Let f be a Hecke eigenform, p be a prime number and V a function satisfying $(V(C, P, Q))$. Let K be an* isotypic *trace function of conductor* $\mathrm{cond}(K)$, *as defined in Section 1.3.*

There exists $s \geqslant 1$ absolute such that we have

$$\mathcal{S}_V(f, K; p) \ll \mathrm{cond}(K)^s p^{1-\delta} (PQ)^{1/2} (P + Q)^{1/2}$$

for any $\delta < 1/8$, where the implied constant depends only on C, f and δ.

Remark 1.3. The Burgess type subconvex bounds for $L(f \otimes \chi, 1/2)$ of Bykovski and Blomer-Harcos mentioned above can easily be retrieved from the special case $K(n) = \chi(n)$.

As a consequence of this and (1.1), one has the following non-trivial estimate for sums over intervals, whose proof is given in Section 2.1:

Corollary 1.4. *Under the same assumptions as above, for any interval $I \subset [1, p]$, we have*

$$\sum_{n \in I} \varrho_f(n) K(n) \ll \mathrm{cond}(K)^s p^{1-\delta/2} \tag{1.8}$$

for any $\delta < 1/8$, where the implied constant depends only on f and δ.

This result applies almost directly to the functions (1.6) and (1.7) and to a wide range of algebraic exponential sums. We refer to Section 2 for these and for more elaborate applications.

An important point is that estimates like (1.4) are obviously linear with respect to K, but the notion of an isotypic function is not. This justifies the following definition:

DEFINITION 1.5 (Trace norms). *Let p be a prime number, and let $K : \mathbf{F}_p \longrightarrow \mathbf{C}$ be any function defined modulo p. Let $s \geqslant 1$ be an integer. The* s-trace norm *of K is*

$$\|K\|_{\mathrm{tr},s} = \inf\left\{ \sum_i |\lambda_i| \operatorname{cond}(K_i)^s + \sum_j |\mu_j| + \sum_k |\eta_k| \right\}$$

where the infimum runs over all decompositions of K as a finite linear combination

$$K(x) = \sum_i \lambda_i K_i(x) + \sum_j \mu_j p^{1/2} \delta_{a_j}(x) + \sum_k \eta_k e\left(\frac{b_k x}{p}\right), \tag{1.9}$$

where λ_i, μ_j, $\eta_k \in \mathbb{C}$, a_j, $b_k \in \mathbf{F}_p$, and K_i is an isotypic trace function.

The decomposition of a function in Dirac functions shows that these norms are well-defined. We then have:

COROLLARY 1.6. *(Trace norm estimate) There exists an absolute constant $s \geqslant 1$ with the following property: for any cusp form f, any prime p, any function K modulo p, for any function V satisfying $(V(C, P, Q))$, we have*

$$\mathcal{S}_V(f, K; p) \ll \|K\|_{\mathrm{tr},s} p^{1-\delta} (PQ)^{1/2} (P+Q)^{1/2},$$

for any $\delta < 1/8$, where the implied constant depends only on (C, f, δ).

Proof. Indeed, for a decomposition (1.9), we can apply Theorem 1.2 for the isotypic trace functions K_i, with the value of s given in that theorem, while we use (1.3) for the components $\eta_k e(b_k x/p)$, and (1.2) for the delta functions. □

REMARK 1.7. It is important to remark that this depends on (1.3), and thus this corollary does not hold for Eisenstein series. For the latter, one can define analogues of the trace norms which consider decompositions (1.9) with no additive characters.

1.2 Good functions and correlating matrices. To deal with the level of generality we consider, it is beneficial at first to completely forget all the specific properties that K might have, and to proceed abstractly. Therefore we consider the problem of bounding the sum $\mathcal{S}_V(f, K; p)$ for $K : \mathbf{Z}/p\mathbf{Z} \to \mathbf{C}$ a general function, assuming only that we know that $|K(n)| \leqslant M$ for some M that we think as fixed.

For the case of Dirichlet characters, Duke, Friedlander and Iwaniec [DFI93] amplified $K(n) = \chi(n)$ among characters with a fixed modulus. Given the absence of structure on K in our situation, this strategy seems difficult to implement. Instead, we use an idea found in [CI00]:[3] we consider K "fixed", and consider the family of sums $\mathcal{S}_V(g, K; p)$ for g varying over a basis of modular cusp forms of level Np, viewing f (suitably normalized) as an old form at p. Estimating the amplified second moment of $\mathcal{S}_V(g, K; p)$ over that family by the Petersson-Kuznetzov formula and the

[3] As pointed out in [CI00], this idea occured already in the work of Bykovsky [Byk98] and was also used by Blomer and Harcos [BH08].

Poisson formula, we ultimately have to confront some sums which we call *correlation sums*, which we now define.

We denote by $\hat{K}$ the (unitarily normalized) Fourier transform modulo p of K, given by

$$\hat{K}(z) = \frac{1}{p^{1/2}} \sum_{x \,(\mathrm{mod}\, p)} K(x) e\left(\frac{zx}{p}\right).$$

For any field L, we let $\mathrm{GL}_2(L)$ and $\mathrm{PGL}_2(L)$ act on $\mathbf{P}^1(L) = L \cup \{\infty\}$ by fractional linear transformations as usual. Now for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{F}_p)$ or in $\mathrm{PGL}_2(\mathbf{F}_p)$, we define the correlation sum $\mathcal{C}(K;\gamma)$ by

$$\mathcal{C}(K;\gamma) = \sum_{\substack{z \in \mathbf{F}_p \\ z \neq -d/c}} \hat{K}(\gamma \cdot z)\overline{\hat{K}(z)}. \tag{1.10}$$

The matrices γ which arise in our amplification are the reduction modulo p of integral matrices parameterized by various coefficients from the amplifier, and we need the sums $\mathcal{C}(K;\gamma)$ to be as small as possible.

If $\|K\|_\infty \leqslant M$ (or even $\|K\|_2 \leqslant M$), then the Cauchy-Schwarz inequality and the Parseval formula show that

$$|\mathcal{C}(K;\gamma)| \leqslant M^2 p. \tag{1.11}$$

This bound is, unsurprinsingly, insufficient. Our method is based on the idea that $\mathcal{C}(K;\gamma)$ should be significantly smaller for most of the γ which occur (even by a factor $p^{-1/2}$, according to the square-root cancellation philosophy) and that we can control the γ where this cancellation does *not* occur. By this, we mean that these matrices (which we call the set of *correlation matrices*) is nicely structured and rather small, unless $\hat{K}$ is constant, a situation which means that $K(n)$ is proportional to $e(\frac{an}{p})$ for some $a \in \mathbf{Z}$, in which case we can use (1.3) anyway.

In this paper, the structure we obtain is algebraic. To discuss it, we introduce the following notation concerning the algebraic subgroups of PGL_2:

- we denote by $B \subset \mathrm{PGL}_2$ the subgroup of upper-triangular matrices, the stabilizer of $\infty \in \mathbf{P}^1$;
- we denote by $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ the Weyl element, so that Bw (resp. wB) is the set of matrices mapping 0 to ∞ (resp ∞ to 0);
- we denote by $\mathrm{PGL}_{2,par}$ the subset of matrices in PGL_2 which are parabolic, i.e., which have a single fixed point in $\mathbf{P}^1$;
- Given $x \neq y$ in $\mathbf{P}^1$, the pointwise stabilizer of x and y is denoted $\mathrm{T}^{x,y}$ (this is a maximal torus), and its normalizer in PGL_2 (or the stabilizer of the set $\{x, y\}$) is denoted $\mathrm{N}^{x,y}$.

DEFINITION 1.8 (Correlation matrices and good functions). *Let p be a prime and $K : \mathbf{F}_p \to \mathbf{C}$ an arbitrary function. Let $M \geqslant 1$ be such that $\|K\|_2 \leqslant M$.*

(1) *We let*

$$\mathbf{G}_{K,M} = \{\gamma \in \mathrm{PGL}_2(\mathbf{F}_p) \mid |\mathcal{C}(K;\gamma)| > Mp^{1/2}\}, \tag{1.12}$$

the set of M-correlation matrices.

(2) *We say that K is (p,M)-good if there exist at most M pairs (x_i,y_i) of distinct elements in $\mathbf{P}^1(\bar{\mathbf{F}}_p)$ such that*

$$\mathbf{G}_{K,M} = \mathbf{G}^b_{K,M} \cup \mathbf{G}^p_{K,M} \cup \mathbf{G}^t_{K,M} \cup \mathbf{G}^w_{K,M}, \tag{1.13}$$

where

$$\mathbf{G}^b_{K,M} \subset B(\mathbf{F}_p) \cup B(\mathbf{F}_p)w \cup wB(\mathbf{F}_p), \quad \mathbf{G}^p_{K,M} \subset \mathrm{PGL}_{2,par}(\mathbf{F}_p)$$
$$\mathbf{G}^t_{K,M} \subset \bigcup_i \mathrm{T}^{x_i,y_i}(\mathbf{F}_p), \quad \mathbf{G}^w_{K,M} \subset \bigcup_i (\mathrm{N}^{x_i,y_i} - \mathrm{T}^{x_i,y_i})(\mathbf{F}_p).$$

In other words: given $M \geqslant 1$ and p a prime, a p-periodic function K is (p,M)-good if the only matrices for which the estimate $|\mathcal{C}(K;\gamma)| \leqslant Mp^{1/2}$ fails are either (1) upper-triangular or sending 0 to ∞ or ∞ to 0; or (2) parabolic; or (3) elements which permute two points defined by at most M integral quadratic (or linear) equations. We note that if we fix such data, a "generic" matrix is *not* of this type.

This notion has little content if M is larger that $p^{1/2}$, but we will already present below some elementary examples of (p,M)-good functions, together with their sets of correlation matrices for M fixed and p arbitrary large (not surprisingly, all these examples come from trace functions).

Given a (p,M)-good function K, we next show using counting arguments that the set of matrices γ constructed from the amplifier does not intersect the set of correlating matrices in a too large set and we eventually obtain our main technical result:

Theorem 1.9 (Bounds for good twists). *Let f be a Hecke eigenform, p be a prime number and V a function satisfying $(V(C,P,Q))$. Let $M \geqslant 1$ be given, and let K be a (p,M)-good function modulo p with $\|K\|_\infty \leqslant M$.*

There exists $s \geqslant 1$ absolute such that

$$\mathcal{S}_V(f,K;p) \ll M^s p^{1-\delta}(PQ)^{1/2}(P+Q)^{1/2},$$

for any $\delta < 1/8$, where the implied constant depends only on (C,f,δ).

REMARK 1.10. Although it is an elementary step [compare (5.14) and (5.15) in the proof] the beautiful modular interpretation of correlation sums is a key observation for this paper. It gives a group theoretic interpretation and introduce symmetry into sums, the estimation of which might otherwise seem to be hopeless.

1.3 Trace functions of ℓ-adic sheaves. The class of functions to which we apply these general considerations are the *trace functions* modulo p, which we now define formally.

Let p be a prime number and $\ell \neq p$ an auxiliary prime. The functions $K(x)$ modulo p that we consider are the trace functions of suitable constructible sheaves on $\mathbf{A}^1_{\mathbf{F}_p}$ evaluated at $x \in \mathbf{F}_p$. To be precise, we will consider ℓ-adic constructible sheaves on $\mathbf{A}^1_{\mathbf{F}_p}$. The trace function of such a sheaf $\mathcal{F}$ takes values in an ℓ-adic field so we also fix an isomorphism $\iota : \bar{\mathbf{Q}}_\ell \longrightarrow \mathbf{C}$, and we consider the functions of the shape

$$K(x) = \iota((\operatorname{tr}\mathcal{F})(\mathbf{F}_p, x)) \tag{1.14}$$

for $x \in \mathbf{F}_p$, as in [Kat90, 7.3.7].

Definition 1.11 (*Trace sheaves*).

(1) *A constructible $\bar{\mathbf{Q}}_\ell$-sheaf $\mathcal{F}$ on $\mathbf{A}^1_{\mathbf{F}_p}$ is a* trace sheaf *if it is a middle-extension sheaf whose restriction to any non-empty open subset $U \subset \mathbf{A}^1_{\mathbf{F}_p}$ where $\mathcal{F}$ is lisse and* pointwise ι-pure *of weight* 0.

(2) *A trace sheaf $\mathcal{F}$ is called a* Fourier trace sheaf *if, in addition, it is a Fourier sheaf in the sense of Katz [Kat88, Def. 8.2.2].*

(3) *A trace sheaf is an* isotypic trace sheaf *if it is a Fourier sheaf and if, for any open set U as in* (1)*, the restriction of $\mathcal{F}$ to U is* geometrically isotypic *when seen as a representation of the geometric fundamental group of U: it is the direct sum of several copies of some (necessarily non-trivial) irreducible representation of the geometric fundamental group of U (see [Kat88, §8.4]).*

If $\mathcal{F}$ is geometrically irreducible (instead of being geometrically isotypic), the sheaf will be called an irreducible trace sheaf.

We use similar terminology for the trace functions:

Definition 1.12 (Trace function). *Let p be a prime number. A p-periodic function $K(n)$ defined for $n \geqslant 1$, seen also as a function on $\mathbf{F}_p$, is a* trace function *(resp.* Fourier trace function, isotypic trace function*) if there is some trace sheaf (resp. Fourier trace sheaf, resp. isotypic trace sheaf) $\mathcal{F}$ on $\mathbf{A}^1_{\mathbf{F}_p}$ such that K is given by (1.14).*

We need an invariant to measure the geometric complexity of a trace function, which may be defined in greater generality.

Definition 1.13 (Conductor). *For an ℓ-adic constructible sheaf $\mathcal{F}$ on $\mathbf{A}^1_{\mathbf{F}_p}$, of rank* $\operatorname{rank}(\mathcal{F})$ *with $n(\mathcal{F})$ singularities in $\mathbf{P}^1$, and with*

$$\operatorname{Swan}(\mathcal{F}) = \sum_x \operatorname{Swan}_x(\mathcal{F})$$

the (finite) sum being over all singularities of $\mathcal{F}$, we define the (analytic) conductor *of $\mathcal{F}$ to be*

$$\operatorname{cond}(\mathcal{F}) = \operatorname{rank}(\mathcal{F}) + n(\mathcal{F}) + \operatorname{Swan}(\mathcal{F}). \tag{1.15}$$

If $K(n)$ is a trace function modulo p, its conductor *is the smallest conductor of a trace sheaf $\mathcal{F}$ with trace function K.*

With these definitions, our third main result, which together with Theorem 1.9 immediately implies Theorem 1.2, is very simple to state:

Theorem 1.14 (Trace functions are good). *Let p be a prime number, $N \geqslant 1$ and $\mathcal{F}$ an isotypic trace sheaf on $\mathbf{A}^1_{\mathbf{F}_p}$, with conductor $\leqslant N$. Let K be the corresponding isotypic trace function. Then K is (p, aN^s)-good for some absolute constants $a \geqslant 1$ and $s \geqslant 1$.*

Remark 1.15. (1) This sweeping result encompasses the functions (1.6) and (1.7) and a wide range of algebraic exponential sums, as well as point-counting functions for families of algebraic varieties over finite fields. From our point of view, the uniform treatment of trace functions is one of the main achievements in this paper. In fact our results can be read as much as being primarily about trace functions, and not Fourier coefficients of modular forms. Reviewing the literature, we have, for instance, found several fine works in analytic number theory that exploit bounds on exponential sums which turn out to be special cases of the correlation sums (1.10) (see [FI85, Hea86, Iwa90, Pit95, Mun13]). Recent works of the authors confirm the usefulness of this notion (see [FKM14, FKM]).

(2) Being isotypic is of course not stable under direct sum, but using Jordan-Hölder components, any Fourier trace function can be written as a sum (with non-negative integral multiplicities) of isotypic trace functions, which allows us to extend many results to general trace functions (see Corollary 1.6).

1.4 The ℓ-adic Fourier transform and the Fourier–Möbius group. We now recall the counterpart of the Fourier transform at the level of sheaves, which was discovered by Deligne and developped especially by Laumon [Lau87]. This plays a crucial role in our work.

Fix a non-trivial additive character ψ of $\mathbf{F}_p$ with values in $\bar{\mathbf{Q}}_\ell$. For any Fourier sheaf $\mathcal{F}$ on $\mathbf{A}^1$, we denote by $\mathcal{G}_\psi = \mathrm{FT}_\psi(\mathcal{F})(1/2)$ its (normalized) *Fourier transform sheaf*, where the Tate twist is always defined using the choice of square root of p in $\bar{\mathbf{Q}}_\ell$ which maps to $\sqrt{p} > 0$ under the fixed isomorphism ι (which we denote $\sqrt{p}$ or $p^{1/2}$). We will sometimes simply write $\mathcal{G}$, although one must remember that this depends on the choice of the character ψ. Then $\mathcal{G}$ is another Fourier sheaf, such that

$$(\mathrm{tr}\,\mathcal{G})(\mathbf{F}_p, y) = -\frac{1}{p^{1/2}} \sum_{x \in \mathbf{F}_p} (\mathrm{tr}\,\mathcal{F})(\mathbf{F}_p, x)\psi(xy)$$

for any $y \in \mathbf{F}_p$ (see [Kat90, Th. 7.3.8, (4)]).

In particular, if K is given by (1.14) and ψ is such that

$$\iota(\psi(x)) = e\left(\frac{x}{p}\right)$$

for $x \in \mathbf{F}_p$ (we will call such a ψ the "standard character" relative to ι), then we have

$$\iota((\operatorname{tr} \mathcal{G})(\mathbf{F}_p, y)) = -\hat{K}(y) \tag{1.16}$$

for y in $\mathbf{Z}$.

A key ingredient in the proof of Theorem 1.14 is the following geometric analogue of the set of correlation matrices:

Definition 1.16 (Fourier–Möbius group). *Let p be a prime number, and let $\mathcal{F}$ be an isotypic trace sheaf on $\mathbf{A}^1_{\mathbf{F}_p}$, with Fourier transform $\mathcal{G}$ with respect to ψ. The* Fourier–Möbius group $\mathbf{G}_{\mathcal{F}}$ *is the subgroup of* $\mathrm{PGL}_2(\bar{\mathbf{F}}_p)$ *defined by*

$$\mathbf{G}_{\mathcal{F}} = \{\gamma \in \mathrm{PGL}_2(\bar{\mathbf{F}}_p) \mid \gamma^*\mathcal{G} \text{ is geometrically isomorphic to } \mathcal{G}\}.$$

The crucial feature of this definition is that $\mathbf{G}_{\mathcal{F}}$ is visibly a group (it is in fact even an algebraic subgroup of $\mathrm{PGL}_{2,\mathbf{F}_p}$, as follows from constructibility of higher-direct image sheaves with compact support, but we do not need this in this paper; it is however required in the sequel [FKM14]). The fundamental step in the proof of Theorem 1.14 is the fact that, for $\mathcal{F}$ of conductor $\leqslant M$, the set $\mathbf{G}_{K,M}$ of correlation matrices is, for p large enough in terms of M, a subset of $\mathbf{G}_{\mathcal{F}}$. This will be derived from the Riemann Hypothesis over finite fields in its most general form (see Corollary 9.2).

1.5 Basic examples. We present here four examples where $\mathbf{G}_{K,M}$ can be determined "by hand", though sometimes this may require Weil's results on exponential sums in one variable or even optimal bounds on exponential sums in *three* variables. This already gives interesting examples of good functions.

(1) Let $K(n) = e(un/p)$. Then $\hat{K}(v) = p^{1/2}\delta_{v\equiv -u \,(\mathrm{mod}\, p)}$, so that $\mathcal{C}(K;\gamma) = 0$ unless $\gamma \cdot (-u) = -u$, and in the last case we have $\mathcal{C}(K;\gamma) = p$. Thus, if $M \geqslant 1$, we have

$$\mathbf{G}_{K,M} = \{\gamma \in \mathrm{PGL}_2(\mathbf{F}_p) \mid \gamma \cdot (-u) = -u\}$$

and, for $1 \leqslant M < p^{1/2}$, the function K is *not* (p, M)-good (yet non-correlation holds).

Dually, we may consider the function

$$K(n) = p^{1/2}\delta_{n\equiv u \,(\mathrm{mod}\, p)}$$

for some fixed $u \in \mathbf{F}_p$, for which the Fourier transform is $\hat{K}(v) = e(uv/p)$. Then we get

$$\mathcal{C}(K;\gamma) = \sum_{z\neq -d/c} e\left(u\frac{z-(az+b)\overline{(cz+d)}}{p}\right) \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

If $u = 0$, this sum is $\geqslant p-1$ for *every* γ and for $1 \leqslant M < p^{1/2} - 1$, the function K is *not* (p, M)-good.

For $u \neq 0$, we get $|\mathcal{C}(K;\gamma)| = p$ if $a-d=c=0$, $\mathcal{C}(K;\gamma)=0$ if $a-d\neq 0$ and $c=0$ and otherwise, the sum is a Kloosterman sum so that $|\mathcal{C}(K;\gamma)| \leqslant 2p^{1/2}$, by Weil's bound. In particular, for $M \geqslant 3$ and p such that $p > 3\sqrt{p}$,

$$\mathbf{G}_{K,M} = \left\{ \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \right\} \subset \mathrm{PGL}_2(\mathbf{F}_p).$$

Thus K is $(p,3)$-good for all $p \geqslant 17$.

(2) Recall that the classical Kloosterman sums are defined by

$$S(e,f;q) = \sum_{x\in(\mathbf{Z}/q\mathbf{Z})^\times} e\left(\frac{ex+f\bar{x}}{q}\right)$$

for $q \geqslant 1$ an integer and $e, f \in \mathbf{Z}$.

We consider $K(n) = S(1,n;p)/\sqrt{p}$ for $1 \leqslant n \leqslant p$. By Weil's bound for Kloosterman sums, we have $|K(n)| \leqslant 2$ for all n. We get $\hat{K}(v) = 0$ for $v = 0$ and

$$\hat{K}(v) = e\left(-\frac{\bar{v}}{p}\right)$$

otherwise. For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(\mathbf{F}_p)$, we find

$$\mathcal{C}(K;\gamma) = \sum_z{}^{*}\, e\left(\frac{\bar{z} - (cz+d)\overline{(az+b)}}{p}\right)$$

where $\sum^*$ restricts the sum to those $z \notin \{0, -d/c, -b/a\}$ in $\mathbf{F}_p$. According to the results of Weil, we have

$|\mathcal{C}(K;\gamma)| \leqslant 2p^{1/2}$ *unless* the rational function

$$\frac{1}{X} - \frac{cX+d}{aX+b} \in \mathbf{F}_p(X) \tag{1.17}$$

is of the form $\phi(X)^p - \phi(X) + t$ for some constant $t \in \mathbf{F}_p$ and $\phi \in \mathbf{F}_p(X)$ (and of course, in that case the sum is $\geqslant p-3$). Looking at poles we infer that in that later case ϕ is necessarily constant. Therefore, for $M \geqslant 3$ and p such that $p-3 > 3\sqrt{p}$, the set $\mathbf{G}_{K,M}$ is the set of γ for which (1.17) is a constant. A moment's thought then shows that

$$\mathbf{G}_{K,M} = \left\{ \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \right\} \subset \mathrm{PGL}_2(\mathbf{F}_p).$$

Thus K is $(p,3)$-good for all $p \geqslant 17$.

(3) Let $K(n) = e(n^2/p)$. For p odd, we get

$$\hat{K}(v) = \frac{\tau_p}{p^{1/2}} e\left(-\frac{\bar{4}v^2}{p}\right)$$

by completing the square, where τ_p is the quadratic Gauss sum.

Since $|\tau_p|^2 = p$, we find for $\gamma \in \mathrm{PGL}_2(\mathbf{F}_p)$ as above the formula

$$\mathcal{C}(K;\gamma) = \sum_{z \neq -d/c} e\left(\frac{\bar{4}(z^2 - (az+b)^2\overline{(cz+d)}^2)}{p}\right).$$

For $p \geqslant 3$, Weil's theory shows that $|\mathcal{C}(K;\gamma)| \leqslant 2p^{1/2}$ for all γ such that the rational function

$$X^2 - \frac{(aX+b)^2}{(cX+d)^2}$$

is not constant and otherwise $|\mathcal{C}(K;\gamma)| \geqslant p-1$.

Thus for $M \geqslant 2$ and $p \geqslant 7$ (when $p-1 > 2p^{1/2}$), the set $\mathbf{G}_{K,M}$ is the set of γ for which this function is constant: this requires $c = 0$ (the second term cannot have a pole), and then we get the conditions $b = 0$ and $(a/d)^2 = 1$, so that

$$\mathbf{G}_{K,M} = \left\{1, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\right\} \subset B(\mathbf{F}_p) \subset \mathrm{PGL}_2(\mathbf{F}_p).$$

Thus that function K is $(p,2)$-good for all primes $p \geqslant 7$.

(4) Let $K(n) = \chi(n)$ where χ is a non-trivial Dirichlet character modulo p. Then we have $\hat{K}(v) = \bar{\chi}(v)\frac{\tau(\chi)}{p^{1/2}}$ for all v, where

$$\tau(\chi) = \sum_{x \in \mathbf{F}_p} \chi(x) e\left(\frac{x}{p}\right)$$

is the Gauss sum associated to χ. Then for γ as above, we have

$$\mathcal{C}(K;\gamma) = \sum_{z \neq -b/a} \bar{\chi}(\gamma \cdot z)\chi(z) = \sum_{z \neq -b/a} \chi\left(z\frac{cz+d}{az+b}\right).$$

Again from Weil's theory, we know that $|\mathcal{C}(K;\gamma)| \leqslant 2p^{1/2}$ *unless* the rational function

$$\frac{X(cX+d)}{(aX+b)}$$

is of the form $tP(X)^h$ for some $t \in \mathbf{F}_p$ and $P \in \mathbf{F}_p(X)$, where $h \geqslant 2$ is the order of χ (and in that case, the sum has modulus $\geqslant p-3$). This means that for $M \geqslant 2$, and $p \geqslant 11$, the set $\mathbf{G}_{K,M}$ is the set of those γ where this condition is true. Looking at

the order of the zero or pole at 0, we see that this can only occur if either $b = c = 0$ (in which case the function is the constant da^{-1}) or, in the special case $h = 2$, when $a = d = 0$ (and the function is $cb^{-1}X^2$). In other words, for $p \geqslant 11$ and $M \geqslant 2$, we have

$$\mathbf{G}_{K,M} = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \right\}$$

if $h \neq 2$, and

$$\mathbf{G}_{K,M} = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \right\}$$

if χ is real-valued. In both cases, these matrices are all in $B(\mathbf{F}_p) \cup B(\mathbf{F}_p)w$, so that the function $\chi(n)$ is $(p, 2)$-good, for all $p \geqslant 11$.

1.6 Notation. As usual, $|X|$ denotes the cardinality of a set, and we write $e(z) = e^{2i\pi z}$ for any $z \in \mathbf{C}$. If $a \in \mathbf{Z}$ and $n \geqslant 1$ are integers and $(a, n) = 1$, we sometimes write $\bar{a}$ for the inverse of a in $(\mathbf{Z}/n\mathbf{Z})^\times$; the modulus n will always be clear from context. We write $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

By $f \ll g$ for $x \in X$, or $f = O(g)$ for $x \in X$, where X is an arbitrary set on which f is defined, we mean synonymously that there exists a constant $C \geqslant 0$ such that $|f(x)| \leqslant Cg(x)$ for all $x \in X$. The "implied constant" refers to any value of C for which this holds. It may depend on the set X, which is usually specified explicitly, or clearly determined by the context. We write $f(x) \asymp g(x)$ to mean $f \ll g$ and $g \ll f$. The notation $n \sim N$ means that the integer n satisfies the inequalities $N < n \leqslant 2N$. We denote the divisor function by $d(n)$.

Concerning sheaves, for $a \neq 0$, we will write $[\times a]^*\mathcal{F}$ for the pullback of a sheaf $\mathcal{F}$ on $\mathbf{P}^1$ under the map $x \mapsto ax$.

For a sheaf $\mathcal{F}$ on $\mathbf{P}^1/k$, where k is an algebraic closure of a finite field, and $x \in \mathbf{P}^1$, we write $\mathcal{F}(x)$ for the representation of the inertia group at x on the geometric generic fiber of $\mathcal{F}$, and $\mathcal{F}_x$ for the stalk of $\mathcal{F}$ at x.

For $\mathcal{F}$ a sheaf on $\mathbf{P}^1/k$, where now k is a finite field of characteristic p, and for ν an integer or $\pm 1/2$, we also write $\mathcal{F}(\nu)$ for the Tate twist of $\mathcal{F}$, with the normalization of the half-twist as discussed in Section 1.4 using the underlying isomorphism $\iota : \bar{\mathbf{Q}}_\ell \to \mathbf{C}$. From context, there should be no confusion between the two possible meanings of the notation $\mathcal{F}(x)$.

2 Some Applications

2.1 Proof of Corollary 1.4. We explain here how to derive bounds for sums over intervals with sharp cut-offs from our main results.

Taking differences, it is sufficient to prove the following slightly more precise bound: for any $\delta < 1/8$ and any $1 \leqslant X \leqslant p$, we have

$$\sum_{1\leqslant n\leqslant X} \varrho_f(n)K(n) \ll_{\mathrm{cond}(K),f,\delta} X^{3/4}p^{1/4-\delta/2},$$

since the right-hand side is always $\ll p^{1-\delta/2}$.

Remark 2.1. Observe that, by taking δ close enough to $1/8$, we obtain here a stronger bound than the "trivial" estimate of size $\ll_{\mathrm{cond}(K),f} X$ coming from (1.1), as long as $X \geqslant p^{3/4+\eta}$ for some $\eta > 0$.

By a dyadic decomposition it is sufficient to prove that for $1 \leqslant X \leqslant p/2$, we have

$$\sum_{X\leqslant n\leqslant 2X} \varrho_f(n)K(n) \ll_{\mathrm{cond}(K),f,\delta} X^{3/4}p^{1/4-\delta/2}$$

for any $\delta < 1/8$. We may assume that

$$X > 16p^{1-2\delta} \tag{2.1}$$

for otherwise the trivial bound (see the previous remark) implies the required bound.

Let $\Delta < 1/2$ be a parameter, and let $W : [0, +\infty[\longrightarrow [0, 1]$ be a smooth function with $0 \leqslant W \leqslant 1$, compactly supported on the interval $[1 - \Delta, 2 + \Delta]$, equal to 1 on $[1, 2]$ and satisfying

$$x^j W^{(j)}(x) \ll \Delta^{-j}$$

for any $j \geqslant 0$. Then, provided $\Delta X \gg p^{3/5}$, we deduce from (1.1) that

$$\sum_{X\leqslant n\leqslant 2X} \varrho_f(n)K(n) = \sum_{n\geqslant 1} \varrho_f(n)K(n)W\left(\frac{n}{X}\right) + O(\|K\|_\infty \Delta X),$$

where the implied constant depends only on f. By Theorem 1.2 applied to $V(x) = W(px/X)$ with $Q = \Delta^{-1} > 2$ and $P = X/p \leqslant 1$, we have

$$\begin{aligned}\sum_{n\geqslant 1} \varrho_f(n)K(n)W\left(\frac{n}{X}\right) &\ll p^{1-\delta}(PQ)^{1/2}(P+Q)^{1/2}\\ &\ll \Delta^{-1}X^{1/2}p^{1/2-\delta}\end{aligned}$$

for any $\delta < 1/8$ where the implied constant depends on f, $\mathrm{cond}(K)$ and δ. Hence we derive

$$\sum_{X\leqslant n\leqslant 2X} \varrho_f(n)K(n) \ll X\Big(\Delta + \Delta^{-1}p^{1/2-\delta}X^{-1/2}\Big).$$

We pick

$$\Delta = \left(p^{1/2-\delta}X^{-1/2}\right)^{1/2}.$$

which is $< 1/2$ by (2.1).Then we get

$$\Delta X \geqslant p^{-\delta/2}X \geqslant p^{1-5\delta/2} > p^{11/16} > p^{3/5}$$

so the above inequality applies to give

$$\sum_{X\leqslant n\leqslant 2X} \varrho_f(n)K(n) \ll X^{3/4}p^{1/4-\delta/2}.$$

as we wanted.

2.2 Characters and Kloosterman sums. We first spell out the examples of the introduction involving the functions (1.6) and (1.7). We give the proof now to illustrate how concise it is given our results, referring to later sections for some details.

COROLLARY 2.2. *Let f be any cusp form, p a prime and K given by*

$$K(n) = \begin{cases} e\left(\frac{\phi_1(n)}{p}\right)\chi(\phi_2(n)), & \text{if } p\nmid S_1(n)S_2(n) \\ 0 & \text{otherwise} \end{cases}$$

or by

$$K(n) = \begin{cases} \Phi\big(\mathrm{Kl}_m(\phi(n);p), \overline{\mathrm{Kl}_m(\phi(n);p)}\big), & \text{if } p\nmid S(n) \\ 0 & \text{otherwise.} \end{cases}$$

Let V satisfy $(V(C,P,Q))$. Then for any $\delta < 1/8$, we have

$$\mathcal{S}(f,K;p) \ll p^{1-\delta}(PQ)^{1/2}(P+Q)^{1/2},$$

and

$$\sum_{n\in I} \varrho_f(n)K(n) \ll p^{1-\delta/2}$$

for any interval $I \subset [1,p]$, where the implied constant depends only on C, f, δ, ϕ_1 and ϕ_2 or ϕ and Φ.

Proof. The first case follows directly from Theorem 1.2 if ϕ_1 and ϕ_2 satisfy the assumption of Theorem 10.1. Otherwise we have $K(n) = e(\frac{an+b}{p})$ and the bound follows from (1.3).

In the second case, we claim that $\|K\|_{\mathrm{tr},s} \ll 1$, where the implied constant depends only on (m,ϕ,Φ), so that Corollary 1.6 applies. Indeed, the triangle inequality shows that we may assume that $\Phi(U,V) = U^uV^v$ is a non-constant monomial. Let

$\mathcal{K}\ell_{m,\phi}$ be the hyper-Kloosterman sheaf discussed in §10.3, $\widetilde{\mathcal{K}\ell}_{m,\phi}$ its dual. We consider the sheaf of rank m^{u+v} given by

$$\mathcal{F} = \mathcal{K}\ell_{m,\phi}^{\otimes u} \otimes \widetilde{\mathcal{K}\ell}_{m,\phi}^{\otimes v}$$

with associated trace function

$$K(n) = \Big((-1)^{m-1}\,\mathrm{Kl}_m(\phi(n);p)\Big)^u \Big((-1)^{m-1}\overline{\mathrm{Kl}_m}(\phi(n);p)\Big)^v.$$

We have

$$\mathrm{cond}(\mathcal{F}) \leqslant 5^{\alpha_{u+v}}(2m+1+\deg(RS))^{\beta_{u+v}}$$

by combining Proposition 10.3 and 8.2 (3) for some constants α_n and β_n (determined by $\alpha_0 = 0$, $\alpha_{n+1} = 2\alpha_n + 1$, $\beta_0 = 1$, $\beta_{n+1} = 2\beta_n + 2$; note that this rought bound could be improved easily).

We replace $\mathcal{F}$ by its semisimplification (without changing notation), and we write

$$\mathcal{F} = \mathcal{F}_1 \oplus \mathcal{F}_2, \qquad K = K_1 + K_2$$

where $\mathcal{F}_2$ is the direct sum of the irreducible components of $\mathcal{F}$ which are geometrically isomorphic to Artin-Schreier sheaves $\mathcal{L}_\psi$, and $\mathcal{F}_1$ is the direct sum of the other components. The trace function K_2 of $\mathcal{F}_2$ is a sum of at most m^{u+v} additive characters (times complex numbers of modulus 1) so

$$\|K_2\|_{\mathrm{tr},s} \leqslant m^{u+v}.$$

On the other hand, each geometrically isotypic component of $\mathcal{F}_1$ have conductor bounded by that of $\mathcal{F}$, and therefore

$$\|K_1\|_{\mathrm{tr},s} \leqslant (5m)^{u+v}(2m+1+\deg(RS))^{2s(u+v)}$$

(Compare with Proposition 8.3).

2.3 Distribution of twisted Hecke orbits and horocycles. We present here a geometric consequence of our main result. Let $Y_0(N)$ denote the modular curve $\Gamma_0(N)\backslash\mathbf{H}$. For a prime p coprime to N, we denote by $\tilde{T}_p$ the geometric Hecke operator that acts on complex-valued functions f defined on $Y_0(N)$ by the formula

$$\tilde{T}_p(f)(z) = \frac{1}{p+1}\sum_{t\in\mathbf{P}^1(\mathbf{F}_p)} f(\gamma_t\cdot z)$$

where

$$\gamma_\infty = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \quad \gamma_t = \begin{pmatrix} 1 & t \\ 0 & p \end{pmatrix}, \quad \text{for } t \in \mathbf{F}_p$$

[note that this differs from the usual Hecke operator $T_p = (p+1)p^{-1/2}\tilde{T}_p$ acting on Maass forms, defined in (3.2)].

As we will also recall more precisely in Section 3, the L^2-space

$$\mathcal{L}^2(N) = \left\{ g : Y_0(N) \longrightarrow \mathbf{C} \mid \int_{Y_0(N)} |g(z)|^2 \frac{dxdy}{y^2} < +\infty \right\},$$

has a basis consisting of $\tilde{T}_p$-eigenforms f, which are either constant functions, Maass cusp forms or combinations of Eisenstein series, with eigenvalues $\nu_f(p)$ such that

$$|\nu_f(p)| \leqslant 2p^{\theta-1/2} \tag{2.2}$$

for some absolute constant $\theta < 1/2$ (e.g., one can take $\theta = 7/64$ by the work of Kim and Sarnak [KS03]). This bound implies the well-known equidistribution of the Hecke orbits $\{\gamma_t \cdot \tau\}$ for a fixed $\tau \in Y_0(N)$, as p tends to infinity. Precisely, let

$$\mu_{p,\tau} = \frac{1}{p+1} \sum_{t \in \mathbf{P}^1(\mathbf{F}_p)} \delta_{\Gamma_0(N)\gamma_t \cdot \tau}$$

where, for any $\tau \in \mathbf{H}$, $\delta_{\Gamma_0(N)\tau}$ denotes the Dirac measure at $\Gamma_0(N)\tau \in Y_0(N)$. Then

$$\mu_{p,\tau} \to \mu$$

as $p \to +\infty$, in the weak-$*$ sense, where μ is the hyperbolic probability measure on $Y_0(N)$.

Note that all but one point of the Hecke orbit lie on the horocycle at height $\Im(\tau)/p$ in $Y_0(N)$ which is the image of the segment $x + i\Im(\tau)/p$ where $0 \leqslant x \leqslant 1$, so this can also be considered as a statement on equidistribution of discrete points on such horocycles.

We can then consider a variant of this question, which is suggested by the natural parameterization of the Hecke orbit by the $\mathbf{F}_p$-rational points of the projective line. Namely, given a complex-valued function

$$K : \mathbf{F}_p \to \mathbf{C}$$

and a point $z \in Y_0(N)$, we define a *twisted measure*

$$\mu_{K,\tau} = \frac{1}{p} \sum_{t \in \mathbf{F}_p} K(t) \delta_{\Gamma_0(N)\gamma_t \cdot \tau}, \tag{2.3}$$

which is now a (finite) signed measure on $Y_0(N)$.

We call these "algebraic twists of Hecke orbits", and we ask how they behave when p is large. For instance, K could be a characteristic function of some subset $A_p \subset \mathbf{F}_p$, and we would be attempting to detect whether the subset A_p is somehow biased in such a way that the corresponding fragment of the Hecke orbit always lives in a certain corner of the curve $Y_0(N)$. We will prove that, when 1_{A_p} can be expressed or approximated by a linear combination of the constant function 1 and

trace functions with bounded conductors, this type of behavior is forbidden. For instance if $A_p = \square(p)$ is the set of quadratic residues modulo p one has

$$1_{\square(p)}(t) = \frac{1}{2}\left(1 + \left(\frac{t}{p}\right)\right),$$

for $(\frac{\cdot}{p})$ the Legendre symbol; this case is discussed in [MV10, §1.2, 1.3], where it is pointed out that it is intimately related to the Burgess bound for short character sums and to subconvexity bounds for Dirichlet L-functions of real characters and twists of modular forms by such characters.

Our result is the following:

Theorem 2.3. *Let $M \geqslant 1$. For each prime p, let K_p be an isotypic trace function modulo p with conductor $\leqslant M$ and $I_p \subset [1,p]$ an interval.*

Let $\mu_{K_p,I_p,\tau}$ be the signed measure

$$\mu_{K_p,I_p,\tau} = \frac{1}{|I_p|}\sum_{t\in I_p} K_p(t)\delta_{\Gamma_0(N)\gamma_t\cdot\tau}.$$

Then, for any given $\tau \in \mathbf{H}$, and I_p such that $|I_p| \geqslant p^{1-\delta}$ for some fixed $\delta < 1/8$, the measures $\mu_{K_p,I_p,\tau}$ converge to 0 as $p \to +\infty$.

Here is a simple application where we twist the Hecke orbit by putting a multiplicity on the γ_t corresponding to the value of a polynomial function on $\mathbf{F}_p$.

Corollary 2.4 (Polynomially-twisted Hecke orbits). *Let $\phi \in \mathbf{Z}[X]$ be an arbitrary non-constant polynomial. For any $\tau \in Y_0(N)$ and any interval of length $|I_p| \geqslant p^{1-\delta}$ for some fixed $\delta < \frac{1}{8}$, the sequence of measures*

$$\frac{1}{|I_p|}\sum_{\substack{x\in\mathbf{F}_p\\ \phi(x)\in I_p}} \delta_{\Gamma_0(N)\gamma_{\phi(x)}\cdot\tau} \tag{2.4}$$

converge to the hyperbolic probability measure μ on $Y_0(N)$ as $p \to +\infty$.

For ϕ non-constant, the set $A_p = \{\phi(t) \mid t \in \mathbf{F}_p\} \subset \mathbf{F}_p$ of values of ϕ has positive density in $\mathbf{F}_p$ for p large, but the limsup of the density $|A_p|/p$ is usually strictly less than 1. The statement means, for instance, that the points of the Hecke orbit of τ parameterized by A_p can not be made to almost all lie in some fixed "half" of $Y_0(N)$, when ϕ is fixed.

These result could also be interpreted in terms of equidistribution of weighted p-adic horocycles; similar questions have been studied in different contexts for rather different weights in [Str04, Ven10, SU] (e.g., for short segments of horocycles). Also, as pointed out by P. Sarnak, the result admits an elementary interpretation in terms

of representations of p by the quaternary quadratic form $\det(a,b,c,d) = ad - bc$ (equivalently in terms of of integral matrices of determinant p). Let

$$M_2^{(p)}(\mathbf{Z}) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}) \mid ad - bc = p \right\}.$$

It is well-known that the non-trivial bound (2.2) implies the equidistribution of $p^{-1/2} M_2^{(p)}(\mathbf{Z})$ on the hyperboloid

$$M_2^{(1)}(\mathbf{R}) = \left\{ \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in M_2(\mathbf{R}) \mid xt - yz = 1 \right\} = \mathrm{SL}_2(\mathbf{R})$$

with respect to the Haar measure on $\mathrm{SL}_2(\mathbf{R})$ (see [Sar91] for much more general statements). Now, any matrix $\gamma \in M_2^{(p)}(\mathbf{Z})$ defines a non-zero singular matrix modulo p and determines a point $z(\gamma)$ in $\mathbf{P}^1(\mathbf{F}_p)$, which is defined as the kernel of this matrix (e.g. $z(\gamma_t) = -t$). By duality, our results imply the following refinement: for any non-constant polynomial $\phi \in \mathbf{Z}[X]$, the subsets

$$M_2^{(p),\phi}(\mathbf{Z}) = \{\gamma \in M_2^{(p)}(\mathbf{Z}) \mid z(\gamma) \in \phi(\mathbf{F}_p)\},$$

are still equidistributed as $p \to \infty$ (compare with [SU, Cor. 1.4]).

2.4 Trace functions over the primes. In the paper [FKM14], we build on our results and on further ingredients to prove the following statement:

Theorem 2.5. *Let K be an isotypic trace function modulo p, associated to a sheaf $\mathcal{F}$ with conductor $\leqslant M$, and such that $\mathcal{F}$ is not geometrically isomorphic to a direct sum of copies of a tensor product $\mathcal{L}_{\chi(X)} \otimes \mathcal{L}_{\psi(X)}$ for some multiplicative character χ and additive character ψ. Then for any $X \geqslant 1$, we have*

$$\sum_{\substack{q \text{ prime} \\ q \leqslant X}} K(q) \ll X(1 + p/X)^{1/12} p^{-\eta},$$

and

$$\sum_{n \leqslant X} \mu(n) K(n) \ll X(1 + p/X)^{1/12} p^{-\eta}$$

for any $\eta < 1/48$. The implicit constants depend only on η and M. Moreover, the dependency M is at most polynomial.

These bounds are non-trivial as long as $X \geqslant p^{3/4+\varepsilon}$ for some $\varepsilon > 0$, and for $X \geqslant p$, we save a factor $\gg_\varepsilon p^{1/48-\varepsilon}$ over the trivial bound. In other terms, trace functions of bounded conductor do not correlate with the primes or the Möbius function when $X \geqslant p^{3/4+\varepsilon}$.

This theorem itself has many applications when specialized to various functions. We refer to [FKM14] for these.

3 Preliminaries Concerning Automorphic Forms

3.1 Review of Kuznetsov formula. We review here the formula of Kuznetsov which expresses averages of products of Fourier coefficients of modular forms in terms of sums of Kloosterman sums. The version we will use here is taken mostly from [BHM07], though we use a slightly different normalization of the Fourier coefficients.

3.1.1 Hecke eigenbases. Let $q \geqslant 1$ be an integer, $k \geqslant 2$ an even integer. We denote by $\mathcal{S}_k(q)$, $\mathcal{L}^2(q)$ and $\mathcal{L}^2_0(q) \subset \mathcal{L}^2(q)$, respectively, the Hilbert spaces of holomorphic cusp forms of weight k, of Maass forms and of Maass cusp forms of weight $k = 0$, level q and trivial Nebentypus (which we denote χ_0), with respect to the Petersson norm defined by

$$\|g\|_q^2 = \int_{\Gamma_0(q)\backslash \mathbf{H}} |g(z)|^2 y^{k_g} \frac{dxdy}{y^2}, \tag{3.1}$$

where k_g is the weight for g holomorphic and $k_g = 0$ if g is a Maass form.

These spaces are endowed with the action of the (commutative) algebra $\mathbf{T}$ generated by the Hecke operators $\{T_n \mid n \geqslant 1\}$, where

$$T_n g(z) = \frac{1}{\sqrt{n}} \sum_{\substack{ad=n \\ (a,q)=1}} \left(\frac{a}{d}\right)^{k_g/2} \sum_{0 \leqslant b < d} g\left(\frac{az+b}{d}\right), \tag{3.2}$$

where $k_g = 0$ if $g \in \mathcal{L}^2(q)$ and $k_g = k$ if $g \in \mathcal{S}_k(q)$ (compare with the geometric operator $\tilde{T}_p$ of Section 2.3).

Moreover, the operators $\{T_n \mid (n,q) = 1\}$ are self-adjoint, and generate a subalgebra denoted $\mathbf{T}^{(q)}$. Therefore, the spaces $\mathcal{S}_k(q)$ and $\mathcal{L}^2_0(q)$ have an orthonormal basis made of eigenforms of $\mathbf{T}^{(q)}$ and such a basis can be chosen to contain all L^2-normalized Hecke newforms (in the sense of Atkin–Lehner theory). We denote such bases by $\mathcal{B}_k(q)$ and $\mathcal{B}(q)$, respectively, and in the remainder of this paper, we tacitly assume that any basis we select satisfies these properties.

The orthogonal complement to $\mathcal{L}^2_0(q)$ in $\mathcal{L}^2(q)$ is spanned by the Eisenstein spectrum $\mathcal{E}(q)$ and the one-dimensional space of constant functions. The space $\mathcal{E}(q)$ is continuously spanned by a "basis" of Eisenstein series indexed by some finite set which is usually taken to be the set $\{\mathfrak{a}\}$ of cusps of $\Gamma_0(q)$. It will be useful for us to employ another basis of Eisenstein series formed of Hecke eigenforms: the adelic reformulation of the theory of modular forms provides a natural spectral expansion of the Eisenstein spectrum in which the Eisenstein series are indexed by a set of parameters of the form

$$\{(\chi, g) \mid g \in \mathcal{B}(\chi)\}, \tag{3.3}$$

where χ ranges over the characters of modulus q and $\mathcal{B}(\chi)$ is some finite (possibly empty) set depending on χ (specifically, $\mathcal{B}(\chi)$ corresponds to an orthonormal basis

in the space of the principal series representation induced from the pair $(\chi, \overline{\chi})$, but we need not be more precise).

With this choice, the spectral expansion for $\psi \in \mathcal{E}(q)$ can be written

$$\psi(z) = \sum_{\substack{\chi \\ g \in \mathcal{B}(\chi)}} \sum \int_{\mathbf{R}} \langle \psi, E_{\chi,g}(t) \rangle E_{\chi,g}(t) \frac{dt}{4\pi}$$

where the Eisenstein series $E_{\chi,g}(t)$ is itself a function from $\mathbf{H}$ to $\mathbf{C}$. When needed, we denote its value at $z \in \mathbf{H}$ by $E_{\chi,g}(z,t)$.

The main advantage of these Eisenstein series is that they are Hecke eigenforms for $\mathbf{T}^{(q)}$: for $(n,q)=1$, one has

$$T_n E_{\chi,g}(t) = \lambda_\chi(n,t) E_{\chi,g}(t)$$

with

$$\lambda_\chi(n,t) = \sum_{ab=n} \chi(a)\overline{\chi(b)} \left(\frac{a}{b}\right)^{it}.$$

3.1.2 Multiplicative and boundedness properties of Hecke eigenvalues. Let f be any Hecke eigenform of $\mathbf{T}^{(q)}$, and let $\lambda_f(n)$ denote the corresponding eigenvalue for T_n, which is real. Then for $(mn,q)=1$, we have

$$\lambda_f(m)\lambda_f(n) = \sum_{d|(m,n)} \lambda_f(mn/d^2). \tag{3.4}$$

This formula (3.4) is valid for all m, n if f is an eigenform for all of $\mathbf{T}$, with an additional multiplicative factor $\chi_0(d)$ in the sum.

We recall some bounds satisfied by the Hecke eigenvalues. First, if f belongs to $\mathcal{B}_k(q)$ (i.e., is holomorphic) or is an Eisenstein series $E_{\chi,f}(t)$, then we have the Ramanujan-Petersson bound

$$|\lambda_f(n)| \leqslant d(n) \ll_\varepsilon n^\varepsilon \tag{3.5}$$

for any $\varepsilon > 0$. For $f \in \mathcal{B}(q)$, this is not known, but we will be able to work with suitable averaged versions, precisely with the second and fourth-power averages of Fourier coefficients. First, we have

$$\sum_{n \leqslant x} |\lambda_f(n)|^2 \ll x(q(1+|t_f|))^\varepsilon, \tag{3.6}$$

uniformly in f, for any $x \geqslant 1$ and any $\varepsilon > 0$, where the implied constant depends only on ε (see [DFI02, Prop. 19.6]). Secondly, we have

$$\sum_{\substack{n \leqslant x \\ n \text{ squarefree}}} |\lambda_f(n)|^4 \ll_f x(\log x) \tag{3.7}$$

for any $x \geqslant 1$ (see, e.g., [KRW07, (3.3), (3.4)]).

3.1.3 Hecke eigenvalues and Fourier coefficients For $z = x + iy \in \mathbf{H}$, we write the Fourier expansion of a modular form f as follows:

$$f(z) = \sum_{n \geqslant 1} \varrho_f(n) n^{(k-1)/2} e(nz) \quad \text{for} \quad f \in \mathcal{B}_k(q),$$
$$f(z) = \sum_{n \neq 0} \varrho_f(n) |n|^{-1/2} W_{it_f}(4\pi|n|y) e(nx) \quad \text{for} \quad f \in \mathcal{B}(q), \tag{3.8}$$

where $1/4 + t_f^2$ is the Laplace eigenvalue, and

$$E_{\chi,g}(z,t) = c_{1,g}(t) y^{1/2+it} + c_{2,g}(t) y^{1/2-it} + \sum_{n \neq 0} \varrho_g(n,t) |n|^{-1/2} W_{it}(4\pi|n|y) e(nx),$$

where

$$W_{it}(y) = \frac{e^{-y/2}}{\Gamma(it + \frac{1}{2})} \int_0^\infty e^{-x} x^{it-1/2} \left(1 + \frac{x}{y}\right)^{it-1/2} dx \tag{3.9}$$

is a Whittaker function (precisely, it is denoted W_{0,it_f} in [DFI02, §4]; see also [GR94, 9.222.2,9.235.2].)

When f is a Hecke eigenform, there is a close relationship between the Fourier coefficients of f and its Hecke eigenvalues $\lambda_f(n)$: for $(m,q) = 1$ and any $n \geqslant 1$, we have

$$\lambda_f(m) \varrho_f(n) = \sum_{d | (m,n)} \varrho_f\left(\frac{mn}{d^2}\right), \tag{3.10}$$

and moreover, these relations hold for all m, n if f is a newform, with an additional factor $\chi_0(d)$.

In particular, for $(m,q) = 1$, we have

$$\lambda_f(m) \varrho_f(1) = \varrho_f(m). \tag{3.11}$$

3.1.4 The Petersson formula. For $k \geqslant 2$ an even integer, the Petersson trace formula expresses the average of product of Fourier coefficients over $\mathcal{B}_k(q)$ in terms of sums of Kloosterman sums (see, e.g. [Iwa95, Theorem 9.6] and [IK04, Proposition 14.5]): we have

$$\frac{(k-2)!}{(4\pi)^{k-1}} \sum_{f \in \mathcal{B}_k(q)} \varrho_f(n) \overline{\varrho_f(m)} = \delta(m,n) + \Delta_{q,k}(m,n), \tag{3.12}$$

with

$$\Delta_{q,k}(m,n) = 2\pi i^{-k} \sum_{q|c} \frac{1}{c} S(m,n;c) J_{k-1}\left(\frac{4\pi\sqrt{mn}}{c}\right). \tag{3.13}$$

3.1.5 The Kuznetsov formula. Let $\phi : [0, \infty[\to \mathbf{C}$ be a smooth function satisfying

$$\phi(0) = \phi'(0) = 0, \qquad \phi^{(j)}(x) \ll_\varepsilon (1+x)^{-2-\varepsilon} \quad \text{for } 0 \leqslant j \leqslant 3.$$

Let

$$\begin{aligned} \dot{\phi}(k) &= i^k \int_0^\infty J_{k-1}(x)\phi(x)\frac{dx}{x}, \\ \tilde{\phi}(t) &= \frac{i}{2\sinh(\pi t)} \int_0^\infty \left(J_{2it}(x) - J_{-2it}(x)\right)\phi(x)\frac{dx}{x}, \\ \check{\phi}(t) &= \frac{2}{\pi}\cosh(\pi t) \int_0^\infty K_{2it}(x)\phi(x)\frac{dx}{x} \end{aligned} \tag{3.14}$$

be Bessel transforms. Then for positive integers m, n we have the following trace formula due to Kuznetsov:

$$\Delta_{q,\phi}(m,n) = \sum_{q|c} \frac{1}{c} S(m,n;c)\phi\left(\frac{4\pi\sqrt{mn}}{c}\right) \tag{3.15}$$

with

$$\begin{aligned} \Delta_{q,\phi}(m,n) = &\sum\sum_{\substack{k\equiv 0 \,(\mathrm{mod}\, 2),\ k>0 \\ g\in\mathcal{B}_k(q)}} \dot{\phi}(k)\frac{(k-1)!}{\pi(4\pi)^{k-1}}\varrho_g(m)\overline{\varrho_g(n)} + \sum_{g\in\mathcal{B}(q)} \tilde{\phi}(t_g)\frac{4\pi}{\cosh(\pi t_g)} \\ &\times\varrho_g(m)\overline{\varrho_g(n)} + \sum_{\chi}\sum_{g\in\mathcal{B}(\chi)} \int_{-\infty}^{\infty} \tilde{\phi}(t)\frac{1}{\cosh(\pi t)}\varrho_g(m,t)\,\overline{\varrho_g(n,t)}\,dt. \end{aligned} \tag{3.16}$$

3.2 Choice of the test function. For the proof of Theorem 1.9, we will need a function ϕ in Kuznetsov formula such that the transforms $\dot{\phi}(k)$ and $\tilde{\phi}(t)$ are non-negative for $k \in 2\mathbf{N}_{>0}$ and $t \in \mathbf{R} \cup (-i/4, i/4)$. Such ϕ is obtained as a linear combination of the following explicit functions. For $2 \leqslant b < a$ two odd integers, we take

$$\phi_{a,b}(x) = i^{b-a}J_a(x)x^{-b}. \tag{3.17}$$

By [BHM07, (2.21)] we have

$$\begin{aligned} \dot{\phi}_{a,b}(k) &= \frac{b!}{2^{b+1}\pi}\prod_{j=0}^{b}\left\{\left(\frac{a+b}{2}-j\right)^2 - \left(\frac{k-1}{2}\right)^2\right\}^{-1} \asymp_{a,b} \pm k^{-2b-2}, \\ \tilde{\phi}_{a,b}(t) &= \frac{b!}{2^{b+1}\pi}\prod_{j=0}^{b}\left\{t^2 + \left(\frac{a+b}{2}-j\right)^2\right\}^{-1} \asymp_{a,b} (1+|t|)^{-2b-2}. \end{aligned} \tag{3.18}$$

In particular,

$$\begin{cases} \dot{\phi}_{a,b}(k) > 0 & \text{for} \quad 2 \leqslant k \leqslant a-b, \\ (-1)^{(k-(a-b))/2}\dot{\phi}_{a,b}(k) > 0 & \text{for} \quad a-b < k \leqslant a+b, \\ \dot{\phi}_{a,b}(k) > 0 & \text{for} \quad a+b < k \ (\text{since } b+1 \text{ is even}), \\ \tilde{\phi}_{a,b}(t) > 0 & \text{for} \quad t \in \mathbf{R} \cup (-i/4, i/4). \end{cases} \tag{3.19}$$

Notice that if we have the freedom to choose a and b very large, we can ensure that the Bessel transforms of $\phi_{a,b}$ decay faster than the inverse of any fixed polynomial at infinity.

4 The Amplification Method

4.1 Strategy of the amplification. We prove Theorem 1.9 using the *amplification method*; precisely we will embed f in the space of forms of level pN (a technique used very successfully by Iwaniec in various contexts [Iwa87, CI00]), as well as by others [Byk98], [BH08]. The specific implementation of amplification (involving the full spectrum, even for a holomorphic form f) is based on [BHM07].

We consider an automorphic form f of level N, which is either a Maass form with Laplace eigenvalue $1/4 + t_f^2$, or a holomorphic modular form of even weight $k_f \geqslant 2$, and which is an eigenform of all Hecke operators T_n with $(n, pN) = 1$.

By viewing f as being of level 2 or 3 if $N = 1$, we can assume that $N \geqslant 2$, which will turn out to be convenient at some point of the later analysis. We will also assume that f is L^2-normalized with respect to the Petersson inner product (3.1).

Finally, we can also assume that $p > N$, hence p is coprime with N. We will also assume that p is sufficiently large with respect to f and ε.

The form f is evidently a cusp form with respect to the smaller congruence subgroup $\Gamma_0(pN)$ and the function

$$\frac{f(z)}{[\Gamma_0(N) : \Gamma_0(pN)]^{1/2}} = \frac{f(z)}{(p+1)^{1/2}} \tag{4.1}$$

may therefore be embedded in a suitable orthonormal basis of modular cusp forms of level $q = pN$, either $\mathcal{B}(q)$ or $\mathcal{B}_{k_f}(q)$.

Let $a > b \geqslant 2$ be odd integers, to be chosen later (both will be taken to be large), let $\phi = \phi_{a,b}$ be the function (3.17) defined in section 3.2. We define "amplified" second moments of the sums $\mathcal{S}(g, K; p)$, where g runs over suitable bases of $\mathcal{B}(q)$ and $\mathcal{B}_{k_f}(q)$. Precisely, given $L \geqslant 1$ and any coefficients (b_ℓ) defined for $\ell \leqslant 2L$ and supported on $\ell \sim L$, and any modular form h, we define an amplifier $B(h)$ by

$$B(h) = \sum_{\ell \leqslant 2L} b_\ell \lambda_h(\ell) = \sum_{\ell \sim L} b_\ell \lambda_h(\ell).$$

We will also use the notation

$$B(g, t) = B(E_{g,\chi}(t)) \tag{4.2}$$

for χ a Dirichlet character modulo N and $g \in \mathcal{B}(\chi)$.

We then let

$$M(L) = \sum_{k\equiv 0 \,(\mathrm{mod}\, 2),\ k>0} \dot{\phi}(k)(k-1)M(L;k) + \sum_{g\in\mathcal{B}(q)} \tilde{\phi}(t_g)\frac{4\pi}{\cosh(\pi t_g)}|B(g)|^2|\mathcal{S}_V(g,K,p)|^2 + \sum_{\chi}\sum_{g\in\mathcal{B}(\chi)} \int_{-\infty}^{\infty} \tilde{\phi}(t)\frac{1}{\cosh(\pi t)}|B(g,t)|^2|\mathcal{S}_V(E_{\chi,g}(t),K,p)|^2\,dt, \tag{4.3}$$

where

$$M(L;k) = \frac{(k-2)!}{\pi(4\pi)^{k-1}} \sum_{g\in\mathcal{B}_k(q)} |B(g)|^2|\mathcal{S}_V(g,K,p)|^2, \tag{4.4}$$

for any even integer $k \geqslant 2$.

We will show:

Proposition 4.1 (Bounds for the amplified moment). *Assume that $M \geqslant 1$ is such that K is (p,M)-good. Let V be a smooth compactly supported function satisfying Condition $(V(C,P,Q))$. Let (b_ℓ) be arbitrary complex numbers supported on primes $\ell \sim L$, such that $|b_\ell| \leqslant 2$ for all ℓ.*

For any $\varepsilon > 0$ there exist $k(\varepsilon) \geqslant 2$, such that for any $k \geqslant k(\varepsilon)$ and any integers $a > b > 2$ satisfying

$$a - b \geqslant k(\varepsilon), \quad a \equiv b \equiv 1 \,(\mathrm{mod}\, 2),$$

we have

$$M(L),\ M(L;k) \ll \{p^{1+\varepsilon}LP(P+Q) + p^{1/2+\varepsilon}L^3PQ^2(P+Q)\}M^3 \tag{4.5}$$

provided that

$$p^{\varepsilon}LQ < p^{1/4}. \tag{4.6}$$

The implied constants depend on (C,ε,a,b,k,f).

We will prove Proposition 4.1 in Sections 5 and 6, but first we show how to exploit it to prove the main result.

From now on, we omit the fixed test-function V and use the simplified notation $\mathcal{S}_V(f,K;p) = \mathcal{S}(f,K;p)$. Also (and because we will need the letter C for another variable), we fix the sequence $C = (C_\nu)_\nu$ and we will not mention the dependency in C in our estimates.

4.2 From Proposition 4.1 to Theorem 1.9. We assume here Proposition 4.1 and proceed to the proof of the main theorem.

The amplifier we use is due to Venkatesh. We put

$$b_\ell = \begin{cases} \operatorname{sign}(\lambda_f(\ell)) & \text{if } \ell \nmid pN \text{ is a prime } \ell \sim L \text{ and } \lambda_f(\ell) \neq 0, \\ 0 & \text{otherwise.} \end{cases} \tag{4.7}$$

(note the use of Hecke eigenvalues, and not Fourier coefficients, here).

With this choice, the pointwise bound $|b_\ell| \leqslant 1$ is obvious, and on average we get

$$\sum_{\ell \sim L} |b_\ell| \leqslant \pi(2L) \leqslant 2L.$$

Moreover, for L large enough in terms of f and $L < p$, we have

$$B(f) \gg \frac{L}{(\log L)^2} \tag{4.8}$$

where the implied constant depends on f. Indeed, we have

$$B(f) = \sum_{\substack{\ell \sim L \\ \ell \nmid N}} |\lambda_f(\ell)|,$$

which we bound from below by writing

$$\frac{L}{\log L} \ll \sum_{\substack{\ell \sim L \\ \ell \nmid N}} |\lambda_f(\ell)|^2 \ll \frac{L}{(\log L)^3} + |\mathcal{L}|^{1/2} \left(\sum_{\ell \sim L} |\lambda_f(\ell)|^4 \right)^{1/2}$$

(using the Cauchy-Schwarz inequality and the Prime Number Theorem for the Rankin-Selberg L-function $L(f \otimes f, s)$) where

$$\mathcal{L} = \{\ell \sim L \mid \ell \nmid N,\ |\lambda_f(\ell)| > (\log L)^{-1}\}.$$

Thus by (3.7), we have

$$B(f) \geqslant \frac{|\mathcal{L}|}{\log L} \gg_f \frac{L}{(\log L)^2}. \tag{4.9}$$

Now we apply Proposition 4.1 for this choice. We recall from (3.19) that we have

$$\tilde{\phi}(t),\ \tilde{\phi}(t_g) > 0,$$

in the second and third terms of the sum defining $M(L)$, while for $k \geqslant 2$, even, we have

$$\dot{\phi}(k) > 0 \text{ for } k \leqslant a - b \text{ or } k > a + b$$

under our conditions on a and b.

Given $\varepsilon > 0$, we can choose a, b large enough, both odd, depending on ε, so that $a - b \geqslant k(\varepsilon)$, and we add a finite number of terms to $M(L)$ to form

$$M(L) + 2 \sum_{\substack{a-b<k\leqslant a+b \\ \dot\phi(k)<0}} |\dot\phi(k)|(k-1)M(L;k)$$

which equals

$$\begin{aligned}\sum_{k\equiv 0 \,(\mathrm{mod}\, 2),\ k>0} |\dot\phi(k)|(k-1)M(L;k) + \sum_{g\in\mathcal{B}(q)} \tilde\phi(t_g)\frac{4\pi}{\cosh(\pi t_g)}|B(g)|^2|\mathcal{S}(g,K,p)|^2 \\ + \sum_{\chi}\sum_{g\in\mathcal{B}(\chi)} \int_{-\infty}^{\infty} \tilde\phi(t)\frac{1}{\cosh(\pi t)}|B(g,t)|^2|\mathcal{S}(E_{\chi,g}(t),K,p)|^2\,dt \\ \ll \{p^{1+\varepsilon}LP(P+Q) + p^{1/2+\varepsilon}L^3PQ^2(P+Q)\}M^3, \qquad (4.10)\end{aligned}$$

where the implied constant depends on (f,ε).

Now all the terms of the left-hand side of the equality (4.10) are non-negative. Applying positivity and recalling (4.1), we obtain

$$(p+1)^{-1}|B(f)|^2|\mathcal{S}(f,K;p)|^2 \ll \{p^{1+\varepsilon}LP(P+Q) + p^{1/2+\varepsilon}L^3PQ^2(P+Q)\}M^3$$

and hence

$$|\mathcal{S}(f,K;p)|^2 \ll \left\{p^{2+\varepsilon}\frac{P(P+Q)}{L} + p^{3/2+\varepsilon}LPQ^2(P+Q)\right\}M^3(\log L)^6 \qquad (4.11)$$

by (4.8), where the implied constant depends on (f,ε).

We let

$$L = \frac{1}{2}p^{1/4-\varepsilon}Q^{-1}, \qquad (4.12)$$

for arbitrarily small $\varepsilon > 0$ so that (4.6) is satisfied. Therefore, if L is sufficiently large depending on f, we obtain

$$\mathcal{S}(f,K;p) \ll M^{3/2}p^{7/8+\varepsilon}(PQ)^{1/2}(P+Q)^{1/2}. \qquad (4.13)$$

On the other hand, if $L \ll_f 1$, we have $Q \gg_f \frac{1}{2}p^{1/4-\varepsilon}$, and the estimate (4.13) is trivial. Thus we obtain Theorem 1.9.

Remark 4.2. In [FKM14, p. 1707], we quote a slighlty different choice of L. This was due to a minor slip in the proof of (4.11) in the first draft of this paper, which is corrected above. Using the value (4.12) in [FKM14] does not affect any of the main results of that paper.

4.3 Packets of Eisenstein series. The above argument also yields a similar bound for packets of unitary Eisenstein series, i.e., when f is replaced by

$$E_{\chi,g,\varphi} = \int_{\mathbf{R}} \varphi(t) E_{\chi,g}(t) dt$$

where χ is a Dirichlet character of modulus N, $g \in \mathcal{B}(\chi)$ and φ is some smooth compactly supported function. We have the following:

PROPOSITION 4.3 (Twisted sums of Eisenstein packets). *Let p be a prime number and $M \geqslant 1$. Let K be a (p, M)-good function, and V a function satisfying $(V(C, P, Q))$.*

There exists an absolute constant $s \geqslant 1$ such that

$$\mathcal{S}_V(E_{\chi,g,\varphi}, K; p) \ll M^s p^{1-\delta} (PQ)^{1/2} (P+Q)^{1/2}$$

for any $\delta < 1/8$, where the implied constant depends only on (N, δ, φ).

Proof. Let $T \geqslant 0$ be such that the support of φ is contained in $[-T, T]$. Then we have

$$|\mathcal{S}_V(E_{\chi,g,\varphi}, K; p)| \leqslant \int_{\mathbf{R}} |\mathcal{S}_V(E_{\chi,g}(t), K; p)\varphi(t)| dt \leqslant \|\varphi\|_\infty \int_{-T}^{T} |\mathcal{S}_V(E_{\chi,g}(t), K; p)| dt,$$

and we will bound the right-hand side.

Fix some $t_0 \in [-T, T]$. For $t \in [-T, T]$ we let $B(g, t)$ denote the amplifier (4.2) for the coefficients

$$b_\ell = \begin{cases} \overline{\lambda_\chi(\ell, t_0)} & \text{if } \ell \sim L \text{ is prime and coprime to } pN, \\ 0 & \text{otherwise,} \end{cases}$$

which satisfy $|b_\ell| \leqslant 2$, where we recall that

$$\lambda_\chi(n, t_0) = \sum_{ab=n} \chi\left(\frac{a}{b}\right) \left(\frac{a}{b}\right)^{it_0}$$

gives the Hecke eigenvalues of $E_{\chi,g}(t_0)$.

Let $\alpha_p = \exp(-\sqrt{\log p})$. For t such that $|t - t_0| \leqslant \alpha_p$, and for ℓ prime with $\ell \sim L$, we have

$$\ell^{\pm it} = \ell^{\pm it_0} + O(\alpha_p^{1/2}),$$

from which we deduce

$$\lambda_\chi(\ell, t) = \lambda_\chi(\ell, t_0) + O(\alpha_p^{1/2}),$$

and then

$$B(g, t) = B(g, t_0) + O(L\alpha_p^{1/2}). \tag{4.14}$$

Our next task it to give an analogue of (4.8), namely we prove the lower bound

$$B(g,t_0) \gg_{N,T} \frac{L}{\log^6 L}, \tag{4.15}$$

for $L \geqslant L_0(N,T)$, uniformy for $|t_0| \leqslant T$.

The argument is similar to [FKM14, Lemma 2.4]. We start from the equality

$$B(g,t_0) = \sum_{\ell\sim L} \left|\chi(\ell)\ell^{it_0} + \overline{\chi}(\ell)\ell^{-it_0}\right| \geqslant \frac{1}{2}\sum_{\ell\sim L} \left|\chi(\ell)\ell^{it_0} + \overline{\chi}(\ell)\ell^{-it_0}\right|^2.$$

Restricting the summation to the primes $\ell \equiv 1 \bmod N$, we obtain the lower bound

$$B(g,t_0) \geqslant 2 \sum_{\substack{\ell\sim L\\ \ell\equiv 1 \bmod N}} \cos^2(t_0\log\ell). \tag{4.16}$$

In [FKM14, p. 1705], the corresponding sum without the condition $\ell \equiv 1 \bmod N$ is shown to be $\gg L/(\log L)^6$. Since N is fixed, it is easy to include this condition in the proof of loc. cit., using the Prime Number Theorem in arithmetic progressions. We leave the details to the reader.

Combining (4.14) and (4.15), we deduce

$$B(g,t) \gg \frac{L}{\log^6 L}, \tag{4.17}$$

where the implied constant depends only on N and T. We therefore get

$$\frac{L^2}{(\log L)^{12}} \int_{|t-t_0|\leqslant\alpha_p} |\mathfrak{S}(E_{\chi,g}(t),K;p)|^2 dt \ll \int_{|t-t_0|\leqslant\alpha_p} |B(g,t)|^2 |\mathfrak{S}(E_{\chi,g}(t),K;p)|^2 dt,$$

and the same argument used in the previous section leads to

$$\int_{|t-t_0|\leqslant\alpha_p} |\mathfrak{S}(E_{\chi,g}(t),K;p)| dt \ll M^{3/2}p^{1-\delta}(PQ)^{1/2}(P+Q)^{1/2},$$

for any $\delta < 1/8$, the implied constant depending on (T,M,δ). Finally we get

$$\begin{aligned}\int_{-T}^{T} |\mathfrak{S}_V(E_{\chi,g}(t),K;p)| dt &\ll M^{3/2}\alpha_p^{-1}p^{1-\delta}(PQ)^{1/2}(P+Q)^{1/2})\\ &\ll M^{3/2}p^{1-\delta'}(PQ)^{1/2}(P+Q)^{1/2}\end{aligned}$$

for any $\delta' < \delta < 1/8$, the implied constant depending on (δ,T), by partitioning the interval $[-T,T]$ into roughly $\alpha_p^{-1} = \exp(\sqrt{\log p})$ intervals of length α_p. □

Remark 4.4. The bounds (4.9) and (4.17) exhibit a polynomial dependency in the parameters of f or $E_{\chi,g,\varphi}$. This is due to the direct use of the prime number theorem for various L-functions. However, with more sophisticated Hoheisel-type estimates (see [Mot] for instance), this dependency can be made polynomial. This is important for instance to obtain polynomial decay rates in p in Theorem 2.3.

Remark 4.5. Using the non-obvious amplifier of [DFI94]

$$b_\ell = \begin{cases} \overline{\lambda_f(\ell)} & \text{if } \ell \sim L \text{ is prime and coprime to } pN, \\ -1 & \text{if } \ell = (\ell')^2 \text{ for } \ell' \sim L \text{ a prime coprime to } pN, \\ 0 & \text{otherwise,} \end{cases}$$

and the identity $|\lambda_f(\ell)|^2 - \lambda_f(\ell^2) = 1$ for ℓ prime it is possible to obtain a non trivial bound for the sum $\mathcal{S}_V(f, K; p)$ when f is of level Np (rather than N); however due to the lacunarity of the amplifier the resulting bounds are weaker: the exponent $1/8$ in Theorem 1.2 and its corollaries has to be replaced by $1/16$. The proof is a little bit more involved as one has to consider more than 3 cases in §5.5 and we will not give it here.

5 Estimation of the Amplified Second Moment

We begin here the proof of Proposition 4.1. Obviously, we can assume that $P \leqslant p$, $Q \leqslant p$.

We start by expanding the squares in $B(g)$ and $|\mathcal{S}(g, K; p)|^2$, getting

$$M(L;k) = \frac{(k-2)!}{\pi(4\pi)^{k-1}} \sum_{\ell_1,\ell_2} b_{\ell_1}\overline{b_{\ell_2}} \sum_{n_1,n_2} K(n_1)\overline{K(n_2)} V\left(\frac{n_1}{p}\right) V\left(\frac{n_2}{p}\right) \times \sum_{g \in \mathcal{B}_k(q)} \lambda_g(\ell_1)\lambda_g(\ell_2)\varrho_g(n_1)\overline{\varrho_g(n_2)}$$

and similarly

$$\begin{aligned} M(L) = \sum_{\ell_1,\ell_2} b_{\ell_1}\overline{b_{\ell_2}} \sum_{n_1,n_2} K(n_1)\overline{K(n_2)} V\left(\frac{n_1}{p}\right) V\left(\frac{n_2}{p}\right) \\ \times \Bigg\{ \sum_{k \equiv 0 \,(\mathrm{mod}\, 2),\ k>0} \sum_{g \in \mathcal{B}_k(q)} \dot{\phi}(k) \frac{(k-1)!}{\pi(4\pi)^{k-1}} \lambda_g(\ell_1)\lambda_g(\ell_2)\varrho_g(n_1)\overline{\varrho_g(n_2)} \\ + \sum_{g \in \mathcal{B}(q)} \tilde{\phi}(t_g) \frac{4\pi}{\cosh(\pi t_g)} \lambda_g(\ell_1)\lambda_g(\ell_2)\varrho_g(n_1)\overline{\varrho_g(n_2)} \\ + \sum_{\chi} \sum_{g \in \mathcal{B}(\chi)} \int_{-\infty}^{\infty} \tilde{\phi}(t) \frac{1}{\cosh(\pi t)} \lambda_\chi(\ell_1, t)\lambda_\chi(\ell_2, t)\varrho_g(n_1, t)\overline{\varrho_g(n_2, t)}\, dt \Bigg\} \end{aligned}$$

where we used the fact that the Hecke eigenvalues $\lambda_g(\ell_2)$ and $\lambda_\chi(\ell_2, t)$ which are involved are real for ℓ_2 coprime to pN, because of the absence of Nebentypus.

5.1 First decomposition. We decompose these two moments as

$$M(L) = M_d(L) + M_{nd}(L), \quad M(L;k) = M_d(L;k) + M_{nd}(L;k)$$

depending on whether $\ell_1 = \ell_2$ or $\ell_1 \neq \ell_2$.

We begin with the "diagonal" terms $M_d(L)$, $M_d(L;k)$ where $\ell_1 = \ell_2$, which are the only cases where ℓ_1 and ℓ_2 are not coprime.

LEMMA 5.1. *Assume that $|K| \leqslant M$. For any $\varepsilon > 0$, we have*

$$M_d(L;k),\ M_d(L) \ll M^2 p^{1+\varepsilon} LP(P+1),$$

where the implied constants depend only on ε.

Proof. Consider $M_d(L)$: it decomposes as a sum of the holomorphic, Maass and Eisenstein contributions

$$M_d(L) = M_{d,Hol}(L) + M_{d,Maa}(L) + M_{d,Eis}(L)$$

where, for instance, we have

$$M_{d,Maa}(L) = \sum_{g\in\mathcal{B}(q)} \tilde{\phi}(t_g) \frac{4\pi}{\cosh(\pi t_g)} \sum_{\ell\leqslant L} |b_\ell|^2 |\lambda_g(\ell)|^2 \left| \sum_n K(n)\varrho_g(n) V\left(\frac{n}{p}\right)\right|^2.$$

By (3.6) and the bound $|b_\ell| \leqslant 2$, we get

$$\sum_{\ell\sim L} |b_\ell|^2 |\lambda_g(\ell)|^2 \leqslant 4 \sum_{\ell\sim L} |\lambda_g(\ell)|^2 \ll_\varepsilon (p(1+|t_g|))^\varepsilon L,$$

where the implied constant is independent of f. We can then apply the rapid decay (3.18) of $\tilde{\phi}(t)$ at infinity and the large sieve inequality of Deshouillers–Iwaniec [DI82, Theorem 2, (1.29)] to obtain

$$\begin{aligned} M_{d,Maa}(L) &\ll_\varepsilon p^\varepsilon L \sum_{g\in\mathcal{B}(q)} \tilde{\phi}(t_g) \frac{(1+|t_g|)^\varepsilon}{\cosh(\pi t_g)} \left| \sum_n K(n)\varrho_g(n) V\left(\frac{n}{p}\right)\right|^2 \\ &\ll p^\varepsilon L \left(1 + \frac{P}{N}\right) M^2(pP) \ll p^{1+\varepsilon} LPM^2(P+1) \end{aligned}$$

where the implied constant depends only on ε.

The bounds for the holomorphic and Eisenstein portion are similar and in fact slightly simpler as we can use Deligne's bound on Hecke eigenvalues of holomorphic cusp form (or unitary Eisenstein series) instead of (3.6) (still using [DI82, Th. 2, (1.28), (1.30)]). And the treatment of $M_d(L;k)$ is essentially included in that of the holomorphic contribution. □

5.2 The contribution of $\ell_1 \neq \ell_2$. The modular forms appearing in $M_{nd}(L)$ or $M_{nd}(L;k)$ are Hecke-eigenforms for the Hecke operators $T(n)$ for $(n,q) = (n,pN) = 1$, hence we can combine the eigenvalues at the primes $\ell_1 \neq \ell_2$ using the Hecke relation (3.10) and

$$\lambda_g(\ell_1)\lambda_g(\ell_2) = \lambda_g(\ell_1\ell_2),$$

obtaining

$$\lambda_g(\ell_1\ell_2)\varrho_g(n_1) = \sum_{d|(\ell_1\ell_2,n_1)} \varrho_g\left(\frac{\ell_1\ell_2 n_1}{d^2}\right).$$

By the Petersson formula (3.12), we write

$$\pi M_{nd}(L;k) = M_1(L;k) + M_2(L;k)$$

where $M_1(L;k)$ corresponds to the diagonal terms $\delta(\ell_1\ell_2 n_1 d^{-2}, n_2)$ while

$$M_2(L;k) = \sum_{\ell_1\neq\ell_2} b_{\ell_1}\overline{b_{\ell_2}} \sum_{d|\ell_1\ell_2} \sum_{\substack{n_1,n_2\\ d|n_1}} K(n_1)\overline{K(n_2)} V\left(\frac{n_1}{p}\right) V\left(\frac{n_2}{p}\right) \Delta_{q,k}\left(\frac{\ell_1\ell_2 n_1}{d^2}, n_2\right)$$

where $\Delta_{q,k}$ is given in (3.13).

On the other hand, by (3.15), there is no diagonal contribution for $M_{nd}(L)$, and we write

$$M_2(L) = M_{nd}(L) = \sum_{\ell_1\neq\ell_2} b_{\ell_1}\overline{b_{\ell_2}} \sum_{d|\ell_1\ell_2} \sum_{\substack{n_1,n_2\\ d|n_1}} K(n_1)\overline{K(n_2)} V\left(\frac{n_1}{p}\right)$$
$$\times V\left(\frac{n_2}{p}\right) \Delta_{q,\phi}\left(\frac{\ell_1\ell_2 n_1}{d^2}, n_2\right),$$

where $\Delta_{q,\phi}(m,n)$ is defined in (3.16).

Remark 5.2. One can obtain a "trivial" bound for $M_2(L)$ and $M_2(L;k)$ by applying the Cauchy-Schwarz inequality and again the large sieve inequalities of Deshouillers–Iwaniec [DI82, Theorem 2], namely

$$\begin{aligned} M_2(L), k^{-1}M_2(L;k) &\ll_\varepsilon p^{1+\varepsilon}((P+1)L)^\varepsilon LP(P+1)^{1/2}(L^2P+1)^{1/2} \\ &\ll pL^2(P+1)M^2 \end{aligned} \tag{5.1}$$

where the implied constant depends on (C,ε,a,b).

5.3 Diagonal terms. We begin with $M_1(L;k)$: we have

$$M_1(L;k) = \sum_{\ell_1\neq\ell_2} b_{\ell_1}\overline{b_{\ell_2}} \sum_{d|\ell_1\ell_2} \sum_{\substack{n_1,n_2\geqslant 1\\ d|n_1}} K(n_1)\overline{K(n_2)} V\left(\frac{n_1}{p}\right) V\left(\frac{n_2}{p}\right) \delta\left(\frac{\ell_1\ell_2 n_1}{d^2}, n_2\right)$$

$$= \sum_{\ell_1\neq\ell_2} b_{\ell_1}\overline{b_{\ell_2}} \sum_{de=\ell_1\ell_2} \sum_{\substack{n_1\geqslant 1\\ d|n_1}} K(n_1)\overline{K(en_1d^{-1})} V\left(\frac{n_1}{p}\right) V\left(\frac{en_1/d}{p}\right)$$

$$= \sum_{\ell_1\neq\ell_2} b_{\ell_1}\overline{b_{\ell_2}} \sum_{de=\ell_1\ell_2} \sum_{m\geqslant 1} K(dm)\overline{K(em)} V\left(\frac{dm}{p}\right) V\left(\frac{em}{p}\right).$$

Since V has compact support in $[P,2P]$ the sum over m is in fact of length $\ll \min(pP/d, pP/e)$. But since $de=\ell_1\ell_2$ with $\ell_i\sim L$, we have

$$\max(d,e) > L.$$

Thus, simply using the bound $|K(n)|\leqslant M$ and the boundedness of b_ℓ, we get:

LEMMA 5.3. *Let $K(n)$ be such that $|K|\leqslant M$ for some $M\geqslant 1$.*

Then we have

$$M_1(L;k) \ll pLPM^2.$$

5.4 Arranging the off-diagonal terms. Now comes the most important case of $M_2(L)$ and $M_2(L;k)$. Their shape is very similar, so we define

$$M_2[\phi] = \frac{1}{pN} \sum_{\ell_1\neq\ell_2} b_{\ell_1}\overline{b_{\ell_2}} \sum_{d|\ell_1\ell_2} \sum_{\substack{n_1,n_2\\ d|n_1}} K(n_1)\overline{K(n_2)} V\left(\frac{n_1}{p}\right) V\left(\frac{n_2}{p}\right)$$

$$\sum_{c\geqslant 1} c^{-1} S(\ell_1\ell_2 n_1 d^{-2}, n_2; cpN)\phi\left(\frac{4\pi}{cpN}\sqrt{\frac{\ell_1\ell_2 n_1 n_2}{d^2}}\right), \quad (5.2)$$

for an arbitrary function ϕ. We then have

$$M_2(L) = M_2[\phi_{a,b}] \text{ and } M_2(L;k) = M_2[\phi_k]$$

for $\phi_k = 2\pi i^{-k} J_{k-1}$.

We first transform these sums by writing

$$M_2[\phi] = \sum_{\ell_1\neq\ell_2} b_{\ell_1}\overline{b_{\ell_2}} \sum_{de=\ell_1\ell_2} M_2[\phi;d,e],$$

where

$$M_2[\phi;d,e] = \frac{1}{pN} \sum_{c\geqslant 1} c^{-1}\tilde{\mathcal{E}}_\phi(c,d,e)$$

and

$$\tilde{\mathcal{E}}_\phi(c,d,e) = \sum_{n_1}\sum_{n_2} S(en_1,n_2;cpN)K(dn_1)\overline{K(n_2)}\phi\left(\frac{4\pi\sqrt{en_1n_2}}{cpN}\right)V\left(\frac{dn_1}{p}\right)V\left(\frac{n_2}{p}\right)$$
$$= \sum_{n_1\geqslant 1}\sum_{n_2\geqslant 1} S(en_1,n_2;cpN)K(dn_1)\overline{K(n_2)}H_\phi(n_1,n_2),$$

with

$$H_\phi(x,y) = \phi\left(\frac{4\pi\sqrt{exy}}{cpN}\right)V\left(\frac{dx}{p}\right)V\left(\frac{y}{p}\right). \tag{5.3}$$

Having fixed d, e as above, let $C = C(d,e) \geqslant 1/2$ be a parameter. We decompose further

$$M_2[\phi;d,e] = M_{2,C}[\phi;d,e] + M_3[\phi;d,e] \tag{5.4}$$

where $M_{2,C}[\phi;d,e]$ denotes the contribution of the terms with $c > C$, and correspondingly

$$M_2[\phi] = M_{2,tail}[\phi] + M_3[\phi]. \tag{5.5}$$

We begin by estimating those, assuming that

$$|\phi(x)| \leqslant Bx^\kappa \tag{5.6}$$

for some $\kappa \geqslant 1$, $B \geqslant 0$ and all $x > 0$. Using the trivial bound for Kloosterman sums and the bound $|K(n)| \leqslant M$, we get

$$\tilde{\mathcal{E}}_\phi(c,d,e) \ll M^2 \sum_{n_1\ll pP/d,\ n_2\ll pP}\sum cp(en_1n_2)^{\kappa/2}(cp)^{-\kappa}$$
$$\ll M^2 c^{-\kappa+1}\left(\frac{e}{d}\right)^{\kappa/2} p^3P^{2+\kappa}$$

for all $c \geqslant 1$, the implied constant depending on B.

For our specific choices of ϕ, we note that we have the upper-bound

$$|J_{k-1}(x)| \leqslant \min(1, x^{k-1}) \tag{5.7}$$

where the constant implied is absolute. Recalling the definition (3.17), we obtain (5.6) with $\kappa = a-b$ for $\phi = \phi_{a,b}$ and with $\kappa = k-1$ for $\phi = 2\pi i^{-k}J_{k-1}$, and we note that in the latter case, the constant B is independent of k. Then, summing over $c > C(d,e)$, we obtain:

PROPOSITION 5.4. *With notation as above, assuming that $|K| \leqslant M$, we have*

$$M_{2,C}[\phi_{a,b};d,e] \ll M^2p^2CP^2\left(\frac{P}{C}\sqrt{\frac{e}{d}}\right)^{a-b},$$

$$M_{2,C}[\phi_k;d,e] \ll M^2p^2CP^2\left(\frac{P}{C}\sqrt{\frac{e}{d}}\right)^{k-1}$$

where the implied constant is absolute.

In view of this proposition, we choose

$$C = \max\left(1/2, p^{\delta}P\sqrt{\frac{e}{d}}\right) \ll p^{\delta}LP, \tag{5.8}$$

for some small parameter $\delta > 0$ which is at our disposal. Then taking $k = k(\delta)$ and $a = a(\delta)$, $b = b(\delta)$ so that k and $a - b$ are large enough, and summing over ℓ_1, ℓ_2 we see that the total contribution, $M_{2,tail}$, to $M(L)$ and $M(L;k)$, of the terms $M_{2,C}[\phi_{a,b}; d, e]$ and $M_{2,C}[\phi_k; d, e]$ is bounded by

$$M_{2,tail} \ll p^{-10}L^2P^2M^2, \tag{5.9}$$

so it is negligible.

5.5 Estimating the off-diagonal terms. It remains to handle the complementary sum [see (5.4)] which is

$$M_3[\phi; d, e] = \frac{1}{pN}\sum_{1\leqslant c\leqslant C} c^{-1}\tilde{\mathcal{E}}_{\phi}(c, d, e), \tag{5.10}$$

where C is defined by (5.8). In particular, we can assume $C \geqslant 1$ otherwise the above sum is zero.

Recall that we factored the product of distinct primes $\ell_1\ell_2$ (with $\ell_i \sim L$) as $\ell_1\ell_2 = de$. Hence we have three types of factorizations of completely different nature, which we denote as follows:

- Type $(L^2, 1)$: this is when $d = \ell_1\ell_2$ and $e = 1$, so that $L^2 < d \leqslant 4L^2$;
- Type $(1, L^2)$: this is when $d = 1$ and $e = \ell_1\ell_2$, so that $L^2 < e \leqslant 4L^2$;
- Type (L, L): this is when d and e are both $\neq 1$ (so $d = \ell_1$ and $e = \ell_2$ or conversely), so that $L < d \neq e \leqslant 2L$.

We will also work under the following (harmless) restriction

$$p^{\delta}P < L. \tag{5.11}$$

By the definitions (5.8) and (5.10), we infer that $C < 1$ hence

PROPOSITION 5.5. *Suppose that (d, e) is of* Type $(L^2, 1)$ *and that (5.11) is satisfied. Then we have the equality*

$$M_3[\phi; d, e] = 0.$$

It remains to deal with the two types (L, L) and $(1, L^2)$. We will transform each of the sums $\tilde{\mathcal{E}}_{\phi}(c, d, e)$ to connect them with the correlation sums $\mathcal{C}(K; \gamma)$ for suitable matrices γ. First, observing that $(c, p) = 1$ because $C < p$ [by combining (4.6, 5.8) and (5.11)], the twisted multiplicativity of Kloosterman sums leads to

$$\tilde{\mathcal{E}}_{\phi}(c, d, e) = \sum_{0\leqslant x_1<cN}\sum_{0\leqslant x_2<cN} S(ex_1\bar{p}, x_2\bar{p}; cN)D(c, d, e, x_1, x_2), \tag{5.12}$$

where

$$D(c,d,e,x_1,x_2)=\sum_{n_1\geqslant 0}\sum_{n_2\geqslant 0}K(df_1(n_1))\overline{K(f_2(n_2))}S(ef_1(n_1)\overline{cN},f_2(n_2)\overline{cN};p)\\ \times H_\phi(f_1(n_1),f_2(n_2)),$$

with

$$f_i(x)=x_i+cNx.$$

We split the double sum over n_1, n_2 into congruence classes modulo p, and apply the Poisson summation formula and the identity

$$\frac{\overline{h}_1}{h_2}+\frac{\overline{h}_2}{h_1}\equiv\frac{1}{h_1h_2}\pmod 1$$

for non-zero coprime integers h_1 and h_2. This shows that[4]

$$\begin{aligned}D(c,d,e,x_1,x_2)&=\sum_{n_1,n_2\in\mathbf{Z}}\frac{1}{(cpN)^2}\widehat{H}_\phi\left(\frac{n_1}{cpN},\frac{n_2}{cpN}\right)e\left(\frac{x_1n_1+x_2n_2}{cpN}\right)\\ &\quad\times e\left(-\frac{\overline{cN}}{p}(x_1n_1+x_2n_2)\right)E(c,d,e,x_1,x_2,n_1,n_2)\\ &=\sum_{n_1,n_2\in\mathbf{Z}}\frac{1}{(cpN)^2}\widehat{H}_\phi\left(\frac{n_1}{cpN},\frac{n_2}{cpN}\right)e\left(\frac{\bar{p}x_1n_1+\bar{p}x_2n_2}{cN}\right)\\ &\quad\times E(c,d,e,x_1,x_2,n_1,n_2)\end{aligned}$$

with $\widehat{H}_\phi(x,y)$ the Fourier transform over $\mathbf{R}^2$ of H_ϕ and

$$\begin{aligned}E(c,d,e,x_1,x_2,n_1,n_2)&:=e\left(\frac{\overline{cN}}{p}(x_1n_1+x_2n_2)\right)\\ &\quad\times\sum_{u_1,u_2(p)}K(df_1(u_1))\overline{K(f_2(u_2))}S(ef_1(u_1)\overline{cN},f_2(u_2)\overline{cN};p)e\left(\frac{u_1n_1+u_2n_2}{p}\right)\\ &=\sum_{u_1,u_2(p)}K(u_1)\overline{K(u_2)}S(e\overline{cdN}u_1,\overline{cN}u_2;p)e\left(\frac{\overline{cdN}u_1n_1+\overline{cN}u_2n_2}{p}\right).\end{aligned}\tag{5.13}$$

Note that the last expression is now independent of (x_1,x_2), so that we will be justified to denote this simply by $E(c,d,e,n_1,n_2)$. Opening the Kloosterman sums in (5.13) and changing the order of summation, we see that

$$E(c,d,e,n_1,n_2)=p\sum_{z\in\mathbf{F}_p^\times}\hat{K}(\overline{cN}(\bar{d}ez+\bar{d}n_1))\overline{\hat{K}(-\overline{cN}(z^{-1}+n_2))},\tag{5.14}$$

[4] We use the same notation n_1, n_2 for the dual variables, but note that they now range over $\mathbf{Z}$.

and by a further change of variable this becomes

$$E(c,d,e,n_1,n_2) = p\mathcal{C}\left(K; \begin{pmatrix} n_1 & (n_1n_2-e)/(cN) \\ cdN & dn_2 \end{pmatrix}\right). \tag{5.15}$$

Our next step is to implement the summation over x_1 and x_2 modulo cN in (5.12): we have

$$\sum_{x_1,x_2 \,(\mathrm{mod}\, cN)}\sum S(ex_1\bar{p}, x_2\bar{p}; cN)e\left(\frac{\bar{p}x_1n_1 + \bar{p}x_2n_2}{cN}\right)$$
$$= \begin{cases} (cN)^2 & \text{if } e \equiv n_1n_2 \,(\mathrm{mod}\, cN),\ (n_2, cN) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

by orthogonality of characters modulo cN. Observe also that, since $N \geqslant 2$, the congruence condition $e \equiv n_1n_2 \,(\mathrm{mod}\, N)$ and the fact that $(e, N) = 1$ implies that $n_1n_2 \neq 0$ and is coprime with N.

The outcome of the above computations is, for any $c \geqslant 1$, the identity

$$\tilde{\mathcal{E}}_\phi(c,d,e) = \frac{1}{p}\sum_{\substack{n_1n_2\neq 0,\ (n_2,cN)=1 \\ n_1n_2\equiv e \,(\mathrm{mod}\, cN)}}\sum \widehat{H}_\phi\left(\frac{n_1}{cpN}, \frac{n_2}{cpN}\right)\mathcal{C}\left(K; \gamma(c,d,e,n_1,n_2)\right) \tag{5.16}$$

where

$$\gamma(c,d,e,n_1,n_2) := \begin{pmatrix} n_1 & (n_1n_2-e)/(cN) \\ cdN & dn_2 \end{pmatrix} \in \mathrm{M}_2(\mathbf{Z}) \cap \mathrm{GL}_2(\mathbf{Q}). \tag{5.17}$$

We make the following definition:

Definition 5.6 (Resonating matrix). *For $n_1n_2 \equiv e \,(\mathrm{mod}\, cN)$, the integral matrix $\gamma(c,d,e,n_1,n_2)$ defined by (5.17) is called a resonating matrix.*

Observe that

$$\det(\gamma(c,d,e,n_1,n_2)) = de$$

and since de is coprime with p, the reduction of $\gamma(c,d,e,n_1,n_2)$ modulo p provides a well-defined element in $\mathrm{PGL}_2(\mathbf{F}_p)$.

5.6 Estimating the Fourier transform. Our next purpose is to truncate the sum over n_1, n_2 in (5.16). To do this, we introduce a new parameter:

$$Z = \frac{P}{cN}\sqrt{\frac{e}{d}} \asymp \begin{cases} \frac{P}{cN} & \text{if } (d,e) \text{ is of Type } (L,L), \\ \\ \frac{LP}{cN} & \text{if } (d,e) \text{ is of Type } (1,L^2). \end{cases} \tag{5.18}$$

Note that, since $1 \leqslant c \leqslant C = p^\delta P(e/d)^{1/2}$, we have

$$Z \gg_N p^{-\delta}. \tag{5.19}$$

We will use Z to estimate the Fourier transform $\widehat{H}_\phi(\frac{n_1}{cpN}, \frac{n_2}{cpN})$. The first bound is given by the following lemma:

LEMMA 5.7. *Let (d, e) be of* Type (L, L) *or of* Type $(1, L^2)$. *Let H_ϕ and Z be defined by* (5.3) *and* (5.18). *Assume that V satisfies $(V(C, P, Q))$ and that $n_1 n_2 \neq 0$.*

(1) *For $\phi = \phi_{a,b}$, we have*

$$\frac{1}{(pN)^2}\widehat{H}_{\phi_{a,b}}\left(\frac{n_1}{cpN}, \frac{n_2}{cpN}\right) \ll \frac{P^2}{d}\frac{Z^{a-b}}{(1+Z)^{a+1/2}}\left(\frac{cdP^{-1}(Q+Z)}{|n_1|}\right)^\mu\left(\frac{cP^{-1}(Q+Z)}{|n_2|}\right)^\nu$$

for all μ, $\nu \geqslant 0$, where the implied constant depends on (N, μ, ν, a, b).

(2) *For $\phi = 2\pi i^{-k} J_{k-1}$, we have*

$$\frac{1}{(pN)^2}\widehat{H}_{\phi}\left(\frac{n_1}{cpN}, \frac{n_2}{cpN}\right) \ll \frac{P^2}{d}\left(\frac{cdP^{-1}(Q+Z)}{|n_1|}\right)^\mu\left(\frac{cP^{-1}(Q+Z)}{|n_2|}\right)^\nu$$

for all μ, $\nu \geqslant 0$, where the implied constant depends on (N, μ, ν), but not on k.

Proof. (1) Recalling (5.3) and (3.17), we have

$$\frac{1}{p^2}\widehat{H}_{\phi_{a,b}}\left(\frac{n_1}{cpN}, \frac{n_2}{cpN}\right) = \frac{1}{d}\iint_{\mathbf{R}^2} V(x)V(y)i^{b-a}\left(4\pi\frac{(e/d)^{1/2}}{cN}\sqrt{xy}\right)^{-b}$$
$$\times J_a\left(4\pi\frac{(e/d)^{1/2}}{cN}\sqrt{xy}\right)e\left(-\frac{(n_1/d)x + n_2 y}{cN}\right)dxdy. \tag{5.20}$$

We use the uniform estimates

$$\left(\frac{z}{1+z}\right)^\nu J_a^{(\nu)}(2\pi z) \ll \frac{z^a}{(1+z)^{a+1/2}}$$

for the Bessel function, valid for $z > 0$ and $\nu \geqslant 0$, where the implied constant depends on a and ν (see [EMOT55, Chap. VII]). We also remark that Z is the order of magnitude of the variable inside $J_a(\cdots)$ in the above formula, then integrating by parts μ times with respect to x and ν times with respect to y, we get the result indicated.

(2) This is very similar: since we want uniformity with respect to k, we use the integral representation

$$J_{k-1}(2\pi x) = \int_0^1 e(-(k-1)t + x\sin(2\pi t))dt$$

for the Bessel function ([GR94, 8.411]). After inserting it in the integral defining the Fourier transform, we find the desired estimates by repeated integrations by parts as before. □

Applying this Lemma with μ, ν very large, remarking that in both cases we have $dZ \leqslant LP$, and appealing to the bound (1.11), namely

$$|\mathcal{C}(K; \gamma(c,d,e,n_1,n_2))| \leqslant M^2 p,$$

we see that, for any fixed $\varepsilon > 0$, the contributions to $\tilde{\mathcal{E}}_\phi(c,d,e)$ of the integers n_1, n_2 with

$$|n_1| \geqslant N_1 = p^\varepsilon \frac{cd(Q+Z)}{P}, \quad \text{or} \quad |n_2| \geqslant N_2 = \frac{N_1}{d} = p^\varepsilon \frac{c(Q+Z)}{P} \tag{5.21}$$

are negligible (see (5.16)).

Thus we get:

Proposition 5.8 (Off-diagonal terms). *Let (d,e) be of* Type (L,L) *or of* Type $(1,L^2)$. *Let $\delta > 0$ and $\varepsilon > 0$ be fixed. Let C, N_1 and N_2 be defined by (5.8) and (5.21). Then for $\phi = \phi_{a,b}$ or $2\pi i^{-k} J_{k-1}$, we have*

$$M_3[\phi; d, e] = \frac{1}{pN} \sum_{c \leqslant C} c^{-1} \mathcal{E}_\phi(c,d,e) + O(M^2 p^{-2})$$

where $\mathcal{E}_\phi$ is the subsum of $\tilde{\mathcal{E}}_\phi$ given by

$$\mathcal{E}_\phi(c,d,e) = \frac{1}{p} \sum_{\substack{1 \leqslant |n_1| \leqslant N_1,\ 1 \leqslant |n_2| \leqslant N_2 \\ (n_2, cN) = 1 \\ n_1 n_2 \equiv e \,(\mathrm{mod}\, cN)}} \widehat{H}_\phi\left(\frac{n_1}{cpN}, \frac{n_2}{cpN}\right) \mathcal{C}\left(K; \begin{pmatrix} n_1 & (n_1 n_2 - e)/(cN) \\ cdN & dn_2 \end{pmatrix}\right).$$

The implied constant depends on $(\delta, \varepsilon, N, a, b)$, but is independent of k for $\phi = 2\pi i^{-k} J_{k-1}$.

5.7 A more precise evaluation. In the range $|n_i| \leqslant N_i$, $i = 1, 2$ we will need a more precise evaluation. We will take some time to prove the following result:

Lemma 5.9. *Let (d,e) be of* Type (L,L) *or of* Type $(1,L^2)$. *Let H_ϕ and Z be defined by (5.3) and (5.18). Assume that V satisfies $(V(C,P,Q))$ and that $n_1 n_2 \neq 0$.*

(1) *For $\phi = \phi_{a,b}$, we have*

$$\frac{1}{p^2} \widehat{H}_{\phi_{a,b}}\left(\frac{n_1}{cpN}, \frac{n_2}{cpN}\right) \ll p^\delta \frac{P^2}{d} \min\left(\frac{1}{Z^{1/2}}, \frac{Q}{Z}\right),$$

where the implied constant depends on (C, a, b, N).

(2) *For $\phi = \phi_k$, we have*

$$\frac{1}{p^2} \widehat{H}_{\phi_k}\left(\frac{n_1}{cpN}, \frac{n_2}{cpN}\right) \ll k^3 p^\delta \frac{P^2}{d} \min\left(\frac{1}{Z^{1/2}}, \frac{Q}{Z}\right),$$

where the implied constant depends on C and N.

Proof. We consider the case $\phi = \phi_k$, the other one being similar. We shall exploit the asymptotic oscillation and decay of the Bessel function $J_{k-1}(z)$ for large z. More precisely, we use the formula

$$J_{k-1}(2\pi z) = \frac{1}{\pi z^{1/2}}\left(\cos\left(2\pi z - \frac{\pi}{2}(k-1) - \frac{\pi}{4}\right) + O\left(\frac{k^3}{z}\right)\right)$$

which is valid uniformly for $z > 0$ and $k \geqslant 1$ with an absolute implied constant (to see this, use the formula

$$J_{k-1}(2\pi z) = \frac{1}{\pi z^{1/2}}\left(\cos\left(2\pi z - \frac{\pi}{2}(k-1) - \frac{\pi}{4}\right) + O\left(\frac{1+(k-1)^2}{z}\right)\right)$$

from, e.g., [Iwa95, p.227, (B 35)], which holds with an absolute implied constant for $z \geqslant 1 + (k-1)^2$, and combine it with the bound $|J_{k-1}(x)| \leqslant 1$.)

The contribution of the second term in this expansion to

$$\frac{1}{p^2}\widehat{H}_{\phi_k}\left(\frac{n_1}{cpN}, \frac{n_2}{cpN}\right)$$

is bounded by

$$\ll \frac{P^2}{d}\frac{k^3}{Z^{3/2}}. \tag{5.22}$$

The contribution arising from the first term can be written as a linear combination (with bounded coefficients) of two expression of the shape

$$\begin{aligned}&\frac{1}{dZ^{1/2}}\int_{\mathbf{R}_+^2}\left(\frac{P}{\sqrt{xy}}\right)^{1/2} V(x)V(y)e\left(\frac{\pm 2\sqrt{(e/d)xy} - (n_1/d)x - n_2 y}{cN}\right)dxdy\\ &= \frac{8P^2}{dZ^{1/2}}\int_{\mathbf{R}_+^2}(2xy)^{1/2}\,V(2Px^2)V(2Py^2)\\ &\quad\times e\left(-2P\frac{(n_1/d)x^2 \mp 2\sqrt{e/d}xy + n_2 y^2}{cN}\right)dxdy.\end{aligned}$$

We write these in the form

$$\frac{8P^2}{dZ^{1/2}}\int_{\mathbf{R}_+^2} G(x,y)e(F_\pm(x,y))dx\,dy, \tag{5.23}$$

where we note that the function

$$G(x,y) = (2xy)^{1/2}V(2Px^2)V(2Py^2)$$

is smooth and compactly supported in $[0,1]^2$, and – crucially – the phase

$$F_{\pm}(x,y) = -2P\frac{(n_1/d)x^2 \mp 2\sqrt{e/d}xy + n_2y^2}{cN}$$

is a quadratic form.

In particular, since $Z \gg p^{-\delta}$ [see (5.19)], we obtain a first easy bound

$$\frac{1}{p^2}\widehat{H}_{\phi_k}\left(\frac{n_1}{cpN}, \frac{n_2}{cpN}\right) \ll k^3p^{\delta}\frac{P^2}{dZ^{1/2}}. \tag{5.24}$$

We now prove two lemmas in order to deal with the oscillatory integrals (5.23) above, from which we will gain an extra factor $Z^{1/2}$. We use the notation

$$\varphi^{(i,j)} = \frac{\partial^{i+j}\varphi}{\partial x^i \partial y^j}$$

for a function φ on $\mathbf{R}^2$.

LEMMA 5.10. *Let $F(x,y)$ be a quadratic form and $G(x,y)$ a smooth function, compactly supported on $[0,1]$, satisfying the inequality*

$$\|G\|_{\infty} + \|G^{(0,1)}\|_{\infty} \leqslant G_0,$$

where G_0 is some positive constant. Let λ_2 denote the Lebesgue measure on $\mathbf{R}^2$.

Then, for every $B > 0$, we have

$$\int_0^1\int_0^1 G(x,y)e\left(F(x,y)\right)dx\,dy \ll G_0\left(\lambda_2(G(B)) + B^{-1}\right),$$

where

$$G(B) = \left\{(x,y) \in [0,1]^2 \;\mid\; |F^{(0,1)}(x,y)| \leqslant B\right\}$$

and the implied constant is absolute.

Proof. For $0 \leqslant x \leqslant 1$, let

$$\mathcal{A}(x) = \left\{y \in [0,1] \;\mid\; |F^{(0,1)}(x,y)| \leqslant B\right\},$$

and $\overline{\mathcal{A}}(x)$ its complement in $[0,1]$. Note that $\mathcal{A}(x)$ is a segment (possibly empty), with length $\lambda_1(\mathcal{A}(x))$. Using Fubini's formula, we write

$$\begin{aligned}\int_0^1\int_0^1 G(x,y)e\left(F(x,y)\right)dx\,dy &= \int_0^1\left(\int_0^1 G(x,y)e\left(F(x,y)\right)d\,y\right)dx\\ &= \int_0^1 I(x)dx,\end{aligned} \tag{5.25}$$

say. To study $I(x)$, we use the partition $[0,1] = \mathcal{A}(x) \cup \overline{\mathcal{A}(x)}$, leading to the inequality

$$|I(x)| \leqslant G_0\, \lambda_1(\mathcal{A}(x)) + \left| \int_{\overline{\mathcal{A}}(x)} G(x,y) e\left(F(x,y)\right) dy \right|.$$

To simplify the exposition, we suppose that $\overline{\mathcal{A}}(x)$ is a segment of the form $]a(x), 1]$ with $0 \leqslant a(x) \leqslant 1$ (when it consists in two segments, the proof is similar). Integrating by part, we get

$$\begin{aligned} \int_{\overline{\mathcal{A}}(x)} G(x,y) e\left(F(x,y)\right) dy &= \int_{a(x)}^1 \frac{G}{F^{(0,1)}}(x,y) \cdot F^{(0,1)}(x,y) \cdot e\left(F(x,y)\right) dy \\ &= \left[\frac{G}{F^{(0,1)}}(x,y) \cdot e\left(F(x,y)\right) \right]_{y=a(x)}^{y=1} \\ &\quad - \int_{a(x)}^1 \left(\frac{G}{F^{(0,1)}}(x,y) \right)^{(0,1)} \cdot e\left(F(x,y)\right)\, dy. \quad (5.26) \end{aligned}$$

The first term in the right hand side of (5.26) is $\ll G_0 B^{-1}$. The modulus of the second one is

$$\leqslant G_0 \int_{a(x)}^1 \left\{ \frac{1}{|F^{(0,1)}|} + \frac{|F^{(0,2)}|}{|F^{(0,1)}|^2} \right\}(x,y)\, dy \ll G_0 B^{-1}$$

since, on the interval of integration, $F^{(0,1)}$ has a constant sign and $F^{(0,2)}$ is constant. Inserting these estimations in (5.25) and using the equality

$$\int_0^1 \lambda_1(\mathcal{A}(x))\, dx = \lambda_2(G(B)),$$

we complete the proof. □

The following lemma gives an upper bound for the constant $\lambda_2(G(B))$ that appears in the previous one.

LEMMA 5.11. *Let $F(x,y) = c_0 x^2 + 2c_1 xy + c_2 y^2$ be a quadratic form with real coefficients c_i. Let $B > 0$ and let $G(B)$ be the corresponding subset of $[0,1]^2$ as defined in Lemma 5.10. We then have the inequality*

$$\lambda_2(G(B)) \leqslant B/|c_1|.$$

Proof. By integrating with respect to x first, we can write

$$\lambda_2(G(B)) = \int_0^1 \lambda_1(\mathcal{B}(y))\, dy,$$

where

$$\mathcal{B}(y) = \{x \in [0,1] \mid |2c_1 x + 2c_2 y| = |F^{(0,1)}(x,y)| \leqslant B\}.$$

This set is again a segment, of length at most $B/|c_1|$. Integrating over y, we get the desired result. □

We return to the study of the integral appearing in (5.23). Here we see easily that Lemma 5.11 applies with

$$|c_1| = \frac{2P}{cN}\sqrt{\frac{e}{d}} = 2Z, \qquad G_0 \ll Q.$$

Hence, by Lemma 5.10, we deduce

$$\int_{\mathbf{R}^2_{\geqslant 0}} G(x,y)e(F_\pm(x,y))dx\,dy \ll Q\left(B/Z + B^{-1}\right),$$

for any $B > 0$. Choosing $B = \sqrt{Z}$, we see that the above integral is $\ll QZ^{-1/2}$.

It only remains to gather (5.22, 5.23, 5.24) with the bound $Z^{-3/2} \ll p^{\delta/2}Q/Z$ to complete the proof of Lemma 5.9. □

5.8 Contribution of the non-correlating matrices. From now on, we simply choose $\delta = \varepsilon > 0$ in order to finalize the estimates.

We start by separating the terms according as to whether

$$|\mathcal{C}(K;\gamma(c,d,e,n_1,n_2))| \leqslant Mp^{1/2}$$

or not, *i.e.*, as to whether the reduction modulo p of the resonating matrix $\gamma(c,d,e,n_1,n_2)$ is in the set $\mathbf{G}_{K,M}$ of M-correlation matrices or not [see (1.12)]. Thus we write

$$\mathcal{E}_\phi(c,d,e) = \mathcal{E}^c_\phi(c,d,e) + \mathcal{E}^n_\phi(c,d,e),$$

where

$$\mathcal{E}^c_\phi(c,d,e) = \frac{1}{p}\sum_{\substack{1\leqslant|n_1|\leqslant N_1,\ 1\leqslant|n_2|\leqslant N_2\\(n_2,cN)=1\\ n_1n_2\equiv e\,(\mathrm{mod}\,cN)}}^{*} \widehat{H}_\phi\left(\frac{n_1}{cpN},\frac{n_2}{cpN}\right)\mathcal{C}\left(K;\gamma(c,d,e,n_1,n_2)\right),$$

where $\sum\sum^*$ restricts to those (n_1,n_2) such that

$$\gamma(c,d,e,n_1,n_2)\,(\mathrm{mod}\,p) \in \mathbf{G}_{K,M},$$

and $\mathcal{E}^n_\phi$ is the contribution of the remaining terms. Similarly, we write

$$\begin{aligned} M_3[\phi;d,e] &= \frac{1}{pN}\sum_{c\leqslant C} c^{-1}\left(\mathcal{E}^n_\phi(c,d,e) + \mathcal{E}^c_\phi(c,d,e)\right) + O(M^2p^{-2})\\ &= M_3^n[\phi;d,e] + M_3^c[\phi;d,e] + O(M^2p^{-2}), \end{aligned}$$

say.

We will treat $M_3^n[\phi; d, e]$ slightly differently, depending on whether (d, e) is of Type (L, L) or of Type $(1, L^2)$. For $\mathsf{T} = (L, L)$ or $(1, L^2)$, we write

$$M_3^{n,\mathsf{T}}[\phi] = \sum_{\ell_1 \neq \ell_2} b_{\ell_1} \overline{b_{\ell_2}} \sum_{de = \ell_1 \ell_2, \text{ type } \mathsf{T}} M_3^n[\phi; d, e].$$

Notice that in both cases we have

$$\frac{N_1 N_2}{c} = p^{2\varepsilon} \left(\frac{cdQ}{P} + \frac{(de)^{1/2}}{N} \right) \left(\frac{Q}{P} + \frac{(e/d)^{1/2}}{cN} \right) \gg \frac{L}{P} \gg 1,$$

by (5.11, 5.18) and (5.21); here the implied constant depends on N. This shows that the total number of terms in the sum $\mathcal{E}_\phi(c, d, e)$ (or its subsums $\mathcal{E}_\phi^n(c, d, e)$) is $\ll N_1 N_2 c^{-1}$.

– When (d, e) is of Type (L, L), we appeal simply to Lemma 5.7 with $\mu = \nu = 0$, and obtain

$$c^{-1} \mathcal{E}_\phi^n(c, d, e) \ll c^{-1} M p^{3/2} \sideset{}{^*}\sum\sum_{\substack{1 \leqslant |n_1| \leqslant N_1,\ 1 \leqslant |n_2| \leqslant N_2 \\ (n_2, cN) = 1 \\ n_1 n_2 \equiv e \,(\mathrm{mod}\, cN)}} \frac{1}{p^2} \left| \widehat{H}_\phi \left(\frac{n_1}{cpN}, \frac{n_2}{cpN} \right) \right|$$

$$\ll M p^{3/2+2\varepsilon} \frac{P^2}{d} \frac{N_1 N_2}{c^2} \ll M p^{3/2+2\varepsilon} (Q + Z)^2 \ll M p^{3/2+2\varepsilon} \left(Q + \frac{P}{c} \right)^2,$$

for $\phi = \phi_{a,b}$ or $\phi = \phi_k$.

Summing the above over $c \leqslant C \ll p^\varepsilon P$ and then over (ℓ_1, ℓ_2), and over the pairs (d, e) of Type (L, L), we conclude that

$$M_3^{n,(L,L)}[\phi] \ll M p^{1/2+3\varepsilon} L^2 (Q^2 P + PQ + P^2) \ll M p^{1/2+3\varepsilon} L^2 PQ(P + Q). \quad (5.27)$$

– When (d, e) is of Type $(1, L^2)$, we have $d = 1$ and

$$c \leqslant C \ll p^\varepsilon LP, \quad Z \asymp \frac{LP}{cN}, \quad N_1 = N_2 \asymp p^\varepsilon \frac{c(Q + LP/(cN))}{P}.$$

We now apply Lemma 5.9. Considering the case of $\phi = \phi_k$, we get

$$c^{-1} \mathcal{E}_\phi^n(c, d, e) \ll c^{-1} M p^{3/2} \sideset{}{^*}\sum\sum_{\substack{1 \leqslant |n_1| \leqslant N_1,\ 1 \leqslant |n_2| \leqslant N_2 \\ (n_2, cN) = 1 \\ n_1 n_2 \equiv e \,(\mathrm{mod}\, cN)}} \frac{1}{p^2} \left| \widehat{H}_\phi \left(\frac{n_1}{cpN}, \frac{n_2}{cpN} \right) \right|$$

$$\ll M k^3 p^{3/2+2\varepsilon} \frac{P^2 Q}{Z} \frac{N_1 N_2}{c^2} \ll M k^3 p^{3/2+2\varepsilon} \frac{cQ}{LP} \left(Q + \frac{LP}{c} \right)^2.$$

If $\phi = \phi_{a,b}$, we obtain the same bound without the factor k^3, but the implied constant then depends also on (a, b).

We then sum over $c \leqslant C$, over (ℓ_1, ℓ_2) and over the pairs (d, e) of Type $(1, L^2)$, and deduce that

$$M_3^{n,(1,L^2)}[\phi_k] \ll Mk^3p^{1/2+5\varepsilon}L^3PQ^3, \qquad M_3^{n,(1,L^2)}[\phi_{a,b}] \ll Mp^{1/2+5\varepsilon}L^3PQ^3. \tag{5.28}$$

Finally, in view of Proposition 5.5, the combination of (5.27) and (5.28), and a renaming of ε, show that

$$M_3^{n}[\phi_{a,b}] \ll Mp^{1/2+\varepsilon}L^3PQ^2(P+Q), \qquad M_3^{n}[\phi_k] \ll Mk^3p^{1/2+\varepsilon}L^3PQ^2(P+Q) \tag{5.29}$$

for any $\varepsilon > 0$ where the implied constant depends on (ε, N, a, b) for $\phi = \phi_{a,b}$ and on (ε, N) for $\phi = \phi_k$.

6 Contribution of the Correlating Matrices

To conclude the proof of Proposition 4.1 we evaluate the contribution $M_3^c[\phi, d, e]$, corresponding to the resonating matrices whose reduction modulo p is a correlating matrix, *i.e.*, such that

$$\gamma(c, d, e, n_1, n_2) = \begin{pmatrix} n_1 & (n_1n_2 - e)/(cN) \\ cdN & dn_2 \end{pmatrix} (\mathrm{mod}\, p) \in \mathbf{G}_{K,M}. \tag{6.1}$$

In that case, we will use the estimate

$$|\mathcal{C}(K; \gamma(c, d, e, n_1, n_2))| \leqslant M^2p \tag{6.2}$$

from (1.11).

The basic idea is that correlating matrices are *sparse*, which compensates the loss involved in this bound.

Corresponding to Definition 1.8, we write

$$\mathcal{E}_\phi^c(c, d, e) = \mathcal{E}_\phi^b(c, d, e) + \mathcal{E}_\phi^p(c, d, e) + \mathcal{E}_\phi^t(c, d, e) + \mathcal{E}_\phi^w(c, d, e)$$

where the superscripts b, p, t, and w denote the subsums of $\mathcal{E}_\phi^c(c, d, e)$ where (c, n_1, n_2) are such that the resonating matrix $\gamma = \gamma(c, d, e, n_1, n_2)$ is of the corresponding type in Definition 1.8 (in case a matrix belongs to two different types, it is considered to belong to the first in which it belongs in the order b, p, t, w).

We write correspondingly

$$M_3^{cor}[\phi, d, e] = M_3^b[\phi, d, e] + M_3^p[\phi, d, e] + M_3^t[\phi, d, e] + M_3^w[\phi, d, e],$$

and

$$M_3^c[\phi] = M_3^b[\phi] + M_3^p[\phi] + M_3^t[\phi] + M_3^w[\phi].$$

Most of the subsequent analysis works when d and e are fixed, and we will therefore often write

$$\gamma(c, d, e, n_1, n_2) = \gamma(c, n_1, n_2)$$

to simplify notation.

The main tool we use is the fact that, when the coefficients of $\gamma(c,d,e,n_1,n_2)$ are small enough compared with p, various properties which hold modulo p can be lifted to $\mathbf{Z}$.

6.1 Triangular and related matrices. Note that

$$B(\mathbf{F}_p)\cup B(\mathbf{F}_p)w\cup wB(\mathbf{F}_p)=\left\{\begin{pmatrix}a_1 & b_1\\ c_1 & d_1\end{pmatrix}\in \mathrm{PGL}_2(\mathbf{F}_p)\mid a_1c_1d_1=0\right\},$$

so that a matrix $\gamma(c,n_1,n_2)$ can only contribute to $\mathcal{E}_\phi^b(c,d,e)$ if $p|cNn_1n_2$.

If we impose the condition

$$p^{3\varepsilon}LQ<p \tag{6.3}$$

(which will be strengthened later on), noting the bounds

$$cd\leqslant dC\leqslant p^\varepsilon P\sqrt{de}\ll p^\varepsilon LP,$$

and

$$N_1=dN_2=p^\varepsilon\frac{cd(Q+Z)}{P}=p^\varepsilon\left(\frac{cdQ}{P}+\frac{cd}{P}\frac{P}{cN}\sqrt{\frac{e}{d}}\right)\ll p^{2\varepsilon}LQ,$$

we see that

$$cdn_1n_2N\equiv 0\,(\mathrm{mod}\,p)$$

is impossible, hence the sum $\mathcal{E}_\phi^b(c,d,e)$ is empty and

$$M_3^b[\phi;d,e]=0. \tag{6.4}$$

6.2 Parabolic matrices. We now consider $\mathcal{E}_\phi^p(c,d,e)$, which is also easily handled. Indeed, a parabolic $\gamma\in\mathrm{PGL}_2(\bar{\mathbf{F}}_p)$ has a unique fixed point in $\mathbf{P}^1$, and hence any representative $\tilde{\gamma}$ of γ in $\mathrm{GL}_2(\bar{\mathbf{F}}_p)$ satisfies $\mathrm{tr}(\tilde{\gamma})^2-4\det(\tilde{\gamma})=0$.

Now if there existed some matrix $\gamma(c,n_1,n_2)$ which is parabolic modulo p, we would get

$$(n_1+dn_2)^2=4de=4\ell_1\ell_2\,(\mathrm{mod}\,p).$$

Under the assumption

$$p^{3\varepsilon}LQ<p^{1/2} \tag{6.5}$$

[which is stronger than (6.3)], this becomes an equality in $\mathbf{Z}$, and we obtain a contradiction since the right-hand side $4\ell_1\ell_2$ is not a square. Therefore, assuming (6.5), we have also

$$M_3^p[\phi;d,e]=0. \tag{6.6}$$

6.3 Toric matrices. We now examine the more delicate case of $\mathcal{E}_\phi^t(c,d,e)$. Recall that this is the contribution of matrices whose image in $\mathrm{PGL}_2(\mathbf{F}_p)$ belong to a set of $\leqslant M$ tori T^{x_i,y_i}. We will deal with each torus individually, so we may concentrate on those $\gamma(c,n_1,n_2)$ which (modulo p) fix $x\neq y$ in $\mathbf{P}^1(\mathbf{F}_p)$. In fact, we can assume that x and y are finite, since otherwise γ would be treated by Section 6.1.

We make the stronger assumption

$$p^{3\varepsilon}LQ<p^{1/3} \tag{6.7}$$

to deal with this case.

We therefore assume that there exists a resonating matrix $\gamma(c,n_1,n_2)$ whose image in $\mathrm{PGL}_2(\mathbf{F}_p)$ is contained in $\mathrm{T}^{x,y}(\mathbf{F}_p)$. From (6.3), we saw already that $\gamma\,(\mathrm{mod}\,p)$ is not a scalar matrix. Now consider the integral matrix

$$2\gamma-\mathrm{tr}(\gamma)\mathrm{Id}=\begin{pmatrix} n_1-dn_2 & 2(n_1n_2-e)/(cN)\\ 2cdN & dn_2-n_1\end{pmatrix}=\begin{pmatrix} u & v\\ w & -u\end{pmatrix}$$

(which has trace 0). The crucial (elementary!) fact is that, since γ is not scalar, an element γ_1 in $\mathrm{GL}_2(\mathbf{F}_p)$ has image in $\mathrm{T}^{x,y}$ if and only $2\gamma_1-\mathrm{tr}(\gamma_1)\mathrm{Id}$ is proportional to $2\gamma-\mathrm{tr}(\gamma)\mathrm{Id}$ (indeed, this is easily checked if $x=0$, $y=\infty$, and the general case follows by conjugation).

Hence, if a resonating matrix $\gamma_1=\gamma(c_1,m_1,m_2)$ has reduction modulo p in $\mathrm{T}^{x,y}$, the matrix

$$2\gamma_1-\mathrm{tr}(\gamma_1)\mathrm{Id}=\begin{pmatrix} m_1-dm_2 & 2(m_1m_2-e)/(c_1N)\\ 2c_1dN & dm_2-m_1\end{pmatrix}=\begin{pmatrix} u_1 & v_1\\ w_1 & -u_1\end{pmatrix}$$

is proportional modulo p to $\begin{pmatrix} u & v\\ w & -u\end{pmatrix}$, which gives equations

$$uv_1-u_1v=uw_1-u_1w=vw_1-v_1w=0\,(\mathrm{mod}\,p). \tag{6.8}$$

Because of (6.7), one sees that these equalities modulo p hold in fact over $\mathbf{Z}$. We then get

$$2u^2m_1m_2=u^2(c_1v_1N+2e)=(uc_1N)(uv_1)+2u^2e,$$

where the first term is also given by

$$(uc_1N)(uv_1)=\frac{(uw_1)(uv_1)}{2d}=\frac{(u_1w)(u_1v)}{2d}=cNv(m_1-dm_2)^2,$$

so that

$$2u^2m_1m_2-cNv(m_1-dm_2)^2=2eu^2. \tag{6.9}$$

We interpret this relation as $F(m_1,m_2)=2eu^2$, where

$$F(X,Y)=-cNvX^2+(2u^2+2cNdv)XY-cNd^2vY^2$$

is an integral binary quadratic form. For $u \neq 0$, it is non-singular, since its discriminant is given by

$$(2u^2+2Ncdv)^2-4(cNv)(cNd^2v) = 4u^2(u^2+2Ncdv) = 4u^2((n_1+dn_2)^2-4de) \neq 0.$$

Note also that all the coefficients of $F(X,Y)$ are $\ll p^A$ for some $A \geqslant 0$ and that similarly

$$|m_1|, |m_2| \leqslant p^A.$$

By a classical result going back to Estermann (see, e.g., [Hea97, Theorem 3]), the number of integral solutions (x,y) to the equation

$$F(x,y) = 2eu^2$$

such that $|x|$, $|y| \leqslant p^A$ is bounded by $\ll p^\varepsilon$ for any $\varepsilon > 0$. But when m_1 and m_2 are given, the value of c_1 is uniquely determined from the second equation in (6.8). Hence the number of possible triples (c_1, m_1, m_2) is bounded by $\ll_\varepsilon p^\varepsilon$.

Similarly, if $u = 0$, we have $m_1 - dm_2 = n_1 - dn_2 = 0$, and the third equation $vw_1 - v_1 w - 0$ becomes

$$c_1^2(dn_2^2 - e) = c^2(dm_2^2 - e).$$

We view this as $G(c_1, m_2) = -ec^2$ where

$$G(X,Y) = (dn_2^2 - e)X^2 - (dc^2)Y^2.$$

This is again a non-degenerate integral quadratic form (note that $dn_2^2 - e \neq 0$ since d and e are coprime) with coefficients $\ll p^A$, and the pairs $(x,y) = (c_1, m_2)$ also satisfy $|x|$, $|y| \ll p^A$, for some $A \geqslant 0$. Thus the number of solutions (c_1, m_2) to $G(c_1, m_2) = -ec^2$ is $\ll p^\varepsilon$ for any $\varepsilon > 0$. Since (c_1, m_2) determine $(c_1, m_1, m_2) = (c_1, dm_2, m_2)$, we get the same bound $\ll p^\varepsilon$ for the number of possible triples (c_1, m_1, m_2).

Using Lemma 5.9 and (6.2), we then deduce (for a single torus)

$$\begin{aligned}\frac{1}{p}\sum_{c\leqslant C} c^{-1}\mathcal{E}^t_{\phi_k}(c,d,e) &\ll M^2p^{1+\varepsilon} \max_{\substack{c\leqslant C\\ 1\leqslant|n_i|\leqslant N_i}} \frac{1}{cp^2}\left|\widehat{H}_{\phi_k}\left(\frac{n_1}{cpN}, \frac{n_2}{cpN}\right)\right| \\ &\ll M^2k^3p^{1+\varepsilon}\max_{c\leqslant C}\frac{P^2}{d}\frac{Q}{cZ} \ll M^2k^3p^{1+\varepsilon}\frac{PQ}{L}\end{aligned}$$

and similarly, without the factor k^3, for $\phi_{a,b}$. Hence, multiplying by the number $\leqslant M$ of tori and summing up over ℓ_1, ℓ_2, d, e, we have

$$M_3^t[\phi_{a,b}] \ll M^3p^{1+\varepsilon}LPQ, \qquad M_3^t[\phi_k] \ll M^3k^3p^{1+\varepsilon}LPQ, \tag{6.10}$$

for any $\varepsilon > 0$, where the implied constant depends on (ε, N, a, b).

6.4 Normalizers of tori. We now finally examine the contribution of $\mathbf{G}_{K,M}^{w}$, *i.e.*, of resonating matrices $\gamma(c, n_1, n_2)$ whose image in $\mathrm{PGL}_2(\mathbf{F}_p)$ are contained in the non-trivial coset of the normalizer of one of the tori T^{x_i,y_i}. Again, we may work with a fixed normalizer $\mathrm{N}^{x,y}$, and we can assume that x and y are finite. Denote by R the set of resonating matrices with image in $\mathrm{N}^{x,y} - \mathrm{T}^{x,y}$.

Suppose that $\gamma = \gamma(c, n_1, n_2)$ is in R. We then have

$$\gamma^2 \equiv \det(\gamma)\mathrm{Id} = de\ \mathrm{Id}\,(\mathrm{mod}\, p),$$

and

$$\mathrm{tr}(\gamma) = n_1 + dn_2 = 0\,(\mathrm{mod}\, p).$$

Assuming, as we do, that (6.7) holds, then we deduce

$$n_1 = -dn_2,\ \gamma^2 = de\mathrm{Id}$$

over $\mathbf{Z}$. In particular, $\gamma(c, n_1, n_2)$ only depends on the two parameters (c, n_2) and we will denote

$$\gamma(c, n_2) := \gamma(c, -dn_2, n_2).$$

Fix some dyadic parameter D with $1 \leqslant D \leqslant C$. We restrict our attention first to matrices $\gamma(c, n_2) \in R$ with $D/2 \leqslant c \leqslant D$; denote by R_D the set of these matrices. Our aim is to show that the total number of resonating matrices in R_D is $\ll_\varepsilon p^\varepsilon$ for any $\varepsilon > 0$.

We distinguish two cases. If R_D has at most one element up to multiplication by ± 1 we are obviously done. Otherwise, let $\gamma_1 = \gamma(c_1, n_1)$ and $\gamma_2 = \gamma(c_2, n_2)$ be two elements of R_D with $\gamma_2 \neq \pm\gamma_1$. We denote

$$\gamma = \gamma_1\gamma_2.$$

Because of (6.7) we see that the reduction modulo p of γ_1 and γ_2 are not scalar multiples of each other, and similarly $\gamma\,(\mathrm{mod}\, p)$ is not a scalar matrix. On the other hand, $\gamma\,(\mathrm{mod}\, p) \in \mathrm{T}^{x,y}$ which implies that the matrix $2\gamma - \mathrm{tr}(\gamma)\mathrm{Id}\,(\mathrm{mod}\, p)$ anti-commutes with the elements of $\mathrm{N}^{x,y} - \mathrm{T}^{x,y}$:

$$\text{for all } \sigma \in \mathrm{N}^{x,y} - \mathrm{T}^{x,y},\ \text{we have } \sigma(2\gamma - \mathrm{tr}(\gamma)\mathrm{Id}) = -(2\gamma - \mathrm{tr}(\gamma))\sigma\,(\mathrm{mod}\, p). \quad (6.11)$$

Finally, let $\gamma_3 = \gamma(c_3, n_3) \in R_D$. Writing

$$2\gamma - \mathrm{tr}(\gamma)\mathrm{Id} = \begin{pmatrix} u & v \\ w & -u \end{pmatrix}$$

the anti-commutation relation leads to the relation

$$-2udn_3 + vNdc_3 - w\frac{dn_3^2 + e}{c_3 N} = 0\,(\mathrm{mod}\, p).$$

Looking at the sizes of u, v, w, and using the fact that $1/2 \leqslant c_i/c_j \leqslant 2$, we see that if we make the stronger assumption

$$p^{3\varepsilon} LQ < p^{1/4}, \tag{6.12}$$

this equation is valid over $\mathbf{Z}$ (for instance,

$$udn_3 = \frac{c_1}{c_2}((dn_2)^2 + de)dn_3 - \frac{c_2}{c_1}((dn_1)^2 + de)dn_3,$$

and the other two are similar). This means that

$$F(c_3, n_3) = ew$$

where

$$F(X, Y) = dvN^2X^2 - 2duNXY - dwY^2$$

is again an integral binary quadratic form. Since its discriminant is

$$(2du)^2 - 4(dv)(-dw) = 4d^2(u^2 + vw) \neq 0,$$

it is non-degenerate.

Hence we can argue as in the previous case, and conclude that, under the assumption (6.12), the total number of resonating matrices in R_D is $\ll p^{\varepsilon}$ for any $\varepsilon > 0$. Summing over the dyadic ranges, the total number of resonating matrices $\gamma(c, n_1, n_2)$ for $c \leqslant C$, $|n_i| \leqslant N_i$, $i = 1, 2$ associated to $\mathrm{N}^{x,y} - \mathrm{T}^{x,y}$ is also $\ll p^{\varepsilon}$.

We deduce then as before the bounds

$$\begin{aligned}\frac{1}{p}\sum_{c\leqslant C} c^{-1}\mathcal{E}^w_{\phi_k}(c, d, e) &\ll M^2 p^{1+\varepsilon} \max_{\substack{c\leqslant C\\ 1\leqslant|n_i|\leqslant N_i,\ i=1,2}} \frac{1}{cp^2}\left|\widehat{H}_{\phi_k}\left(\frac{-dn_2}{cpN}, \frac{n_2}{cpN}\right)\right| \\ &\ll M^2 p^{1+\varepsilon} k^3 \max_{c\leqslant C} \frac{P^2}{d}\frac{Q}{cZ} \ll M^2 k^3 p^{1+\varepsilon}\frac{PQ}{L},\end{aligned}$$

for one normalizer (and similarly with $\phi_{a,b}$ without the k^3 factor), and therefore

$$M_3^w[\phi_{a,b}] \ll M^3 p^{1+\varepsilon} LPQ, \qquad M_3^w[\phi_k] \ll M^3 k^3 p^{1+\varepsilon} LPQ, \tag{6.13}$$

for any $\varepsilon > 0$, where the implied constants depend on (a, b, N, ε).

6.5 Conclusion. We can now gather Lemmas 5.1, 5.3 and Proposition 5.4 [choosing $a - b$ and k large enough depending on ε so that (5.9) holds], together with (5.29, 6.4, 6.6, 6.10) and (6.13). We derive, under the assumptions that (5.11) and (6.12) hold, the bound

$$\begin{aligned}&M(L),\ k^{-3}M(L; k)\\ &\quad\ll M^3\{pLP + p^{1+\varepsilon}LP(P+1) + p^{1+\varepsilon}LPQ + p^{1/2+\varepsilon}L^3PQ(P+Q)^2\}\\ &\quad\ll M^3\{p^{1+\varepsilon}LP(P+Q) + p^{1/2+\varepsilon}L^3PQ^2(P+Q)\}\end{aligned}$$

for any $\varepsilon > 0$, where the implied constant depends on f and ε.

Finally, we observe that if (5.11) does not hold, the above bound remains valid by Lemma 5.1 and (5.1), and this concludes the proof of Proposition 4.1.

7 Distribution of Twisted Hecke Orbits and Horocycles

We prove in this section, the results of Section 2.3, using the main estimate of Theorem 1.9 as basic tool.

Proof of Theorem 2.3. Let $K = K_p$ be an isotypic trace function with conductor at most M and $I = I_p \subset [1, p]$ an interval. We have to show that if $|I| \geqslant p^{7/8+\kappa}$ for some fixed $\kappa > 0$, we have the limit

$$\mu_{K,I,\tau}(\varphi) = \frac{1}{|I|} \sum_{t \in I} K(t) \varphi\left(\frac{\tau + t}{p}\right) \longrightarrow 0$$

as $p \to +\infty$, for all φ continuous and compactly supported on $Y_0(N)$ and all $\tau \in Y_0(N)$. By the spectral decomposition theorem for $Y_0(N)$, it is sufficient to prove the result for φ either the constant function 1, or a Maass Hecke-eigenform or a packet of Eisenstein series.

Let $\varphi = f$ be a Maass cusp form with Fourier expansion

$$f(z) = \sum_{n \in \mathbf{Z} - \{0\}} \varrho_f(n) |n|^{-1/2} W_{it_f}(4\pi |n| y) e(nx).$$

We can assume, by linearity, that f is an eigenfunction of the involution $z \mapsto -\bar{z}$, so that there exists $\varepsilon_f = \pm 1$ with

$$\varrho_f(n) = \varepsilon_f \varrho_f(-n) \tag{7.1}$$

for all $n \in \mathbf{Z}$. We now derive the basic identity relating Hecke orbits with the twisted sums of Fourier coefficients: we have (for $p \geqslant 3$)

$$\mu_{K,I,\tau}(f) = \frac{1}{|I|} \sum_n \varrho_f(n) |n/p|^{-1/2} W_{it_f}\left(\frac{4\pi \Im\mathfrak{m}(\tau)|n|}{p}\right) e\left(\frac{n \Re\mathfrak{e}(\tau)}{p}\right) K_I'(n)$$

with

$$\begin{aligned} K_I'(n) &= \frac{1}{p^{1/2}} \sum_{t \in I} K(t) e\left(\frac{nt}{p}\right) = \frac{1}{p} \sum_{x \in [-p/2, p/2]} \hat{K}(n - x) \sum_{t \in I} e\left(\frac{tx}{p}\right) \\ &= \frac{|I|}{p} \hat{K}(n) + \frac{1}{p} \sum_{\substack{|x| \leqslant p/2 \\ x \neq 0}} \hat{K}(n - x) \sum_{t \in I} e\left(\frac{tx}{p}\right), \end{aligned}$$

where $\hat{K}$ is the unitarily-normalized Fourier transform modulo p, as before. Hence, by (7.1), we get

$$\begin{aligned} \mu_{K,I,\tau}(f) &= \frac{1}{p} \left\{ \mathcal{S}_V(f, \hat{K}; p) + \varepsilon_f \mathcal{S}_W(f, [\times(-1)]^* \hat{K}; p) \right\} \\ &+ \frac{1}{|I|} \frac{1}{p} \sum_{\substack{|x| \leqslant p/2 \\ x \neq 0}} \left\{ \mathcal{S}_V(f, [-x]^* \hat{K}; p) + \varepsilon_f \mathcal{S}_W(f, [-x]^* [\times(-1)]^* \hat{K}; p) \right\} \sum_{t \in I} e\left(\frac{tx}{p}\right) \end{aligned} \tag{7.2}$$

where, for any function $L : \mathbf{F}_p \longrightarrow \mathbf{C}$, we denote

$$[-x]^*L(n) = L(n-x) = L\left(\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} n\right), \quad [\times(-1)]^*L(n) = L(-n),$$

and V and W are the functions (depending on t_f and on τ) defined on $]0, +\infty[$ by

$$V(x) = x^{-1/2}W_{it_f}(4\pi\Im\mathfrak{m}(\tau)x)e(x\Re\mathfrak{e}(\tau)),$$
$$W(x) = x^{-1/2}W_{it_f}(4\pi\Im\mathfrak{m}(\tau)x)e(-x\Re\mathfrak{e}(\tau)).$$

Let $L : \mathbf{F}_p \longrightarrow \mathbf{C}$ be one of the functions $[\times(-1)]^*\hat{K}$ or $[-x]^*\hat{K}$ or $[-x]^*[\times(-1)]^*\hat{K}$ for some $x \in \mathbf{F}_p$. By Lemma 8.1, Propositions 8.2 and 8.4, each such L is an isotypic trace function whose conductor is bounded solely in terms of $\mathrm{cond}(K)$. Therefore we would like to apply Theorem 1.9.

Remark 7.1. For the rest of this section we will not necessarily display the dependency in M or f or τ of the various constants implicit in the Vinogradov symbols $\ll$.

The functions V and W above do not a priori satisfy a condition of type $(V(C, P, Q))$, but it is standard to reduce to this situation. First, we truncate the large values of n, observing that since

$$W_{it}(x) \ll e^{-x/2},$$

where the implied constant depends on t [see (3.9)], the contribution of the terms with $n \geqslant p^{1+\varepsilon}$ to any of the sums appearing in (7.2) is

$$\ll \exp(-p^{\varepsilon/2}),$$

for any $\varepsilon > 0$.

Then, by means of a smooth dyadic partition of the remaining interval, the various sums $\mathcal{S}_V(f, L; p)$ and $\mathcal{S}_W(f, L; p)$ occuring in (7.2), are decomposed into a sum of $O(\log p)$ sums of the shape

$$P^{-1/2}\mathcal{S}_{\tilde{V}}(f, L; p)$$

where L has conductor bounded in terms of M only, for functions $\tilde{V}$, depending on τ and t_f, which satisfy Condition $(V(C, P, Q))$ for some sequence $C = (C_\nu)$, and

$$P \in \left[\frac{1}{2}p^{-1}, p^{\varepsilon}\right], \qquad Q \ll_{t_f,\varepsilon} 1$$

(the normalizing factor $P^{-1/2}$ comes from the factorization $(x/p)^{-1/2} = P^{-1/2}(x/pP)^{-1/2}$, and is introduced to ensure that $\tilde{V}(x) \ll_{t_f,\varepsilon} 1$).

The trivial bound for these sums is $O(P^{-1/2}Pp^{1+\varepsilon})$ and using

$$\frac{1}{p}\sum_{\substack{|x|\leqslant p/2\\ x\neq 0}}\left|\sum_{t\in I} e\left(\frac{tx}{p}\right)\right| \ll \log p, \tag{7.3}$$

we see that the contribution to $\mu_{K,I,\tau}(f)$ of the sums with $P \leqslant p^{-1/2}$ is

$$\ll p^{3/4+\varepsilon}\left(\frac{1}{p}+\frac{1}{|I|}\right) = o(1)$$

provided $|I| \geqslant p^{3/4+2\varepsilon}$.

For the remaining sums, we use Theorems 1.9 and 1.14: we have

$$P^{-1/2}\mathfrak{S}_{\tilde{V}}(f, L; p) \ll p^{1-\delta+\varepsilon}$$

for any $\delta < 1/8$, where the implicit constants depend on $(M, C, f, \tau, \delta, \varepsilon)$. We obtain that

$$\mu_{K,I,\tau}(f) \ll p^{-\delta+\varepsilon} + \frac{1}{|I|}p^{1-\delta+\varepsilon}. \tag{7.4}$$

As long as $|I| \geqslant p^{7/8+\kappa}$ for some fixed $\kappa > 0$, we can take $\varepsilon > 0$ small enough and $\delta > 0$ small enough so that we above shows that $\mu_{K,I,\tau}(f) \to 0$ as $p \to +\infty$, as desired.

The case where φ is a packet of Eisenstein series $E_{\chi,g}(\varphi)$ is similar, using Proposition 4.3. Indeed, the contribution of the non-zero Fourier coefficients are handled in this manner, and the only notable difference is that we must handle the constant term of this packet. This is given by

$$\varrho_{\chi,g}(\varphi, 0)(z) = \int_{\mathbf{R}} \varphi(t)\{c_{1,g}(t)y^{1/2+it} + c_{2,g}(t)y^{1/2-it}\}dt, \tag{7.5}$$

and contributes to $\mu_{K,I,\tau}(E_{\chi,g}(\varphi))$ by

$$\begin{aligned}\frac{1}{|I|}\sum_{t\in I} K(t)\varrho_{\chi,g}(\varphi, 0)\left(\frac{\tau+t}{p}\right) &= \varrho_{\chi,g}(\varphi, 0)\left(\frac{\tau}{p}\right)\frac{1}{|I|}\sum_{t\in I} K(t)\\ &= \varrho_{\chi,g}(\varphi, 0)\left(\frac{\tau}{p}\right)\frac{p^{1/2}}{|I|}K_I'(0)\end{aligned}$$

since $\varrho_{\chi,g}(\varphi, 0)(z)$ does not depend on the real part of z. We have

$$\varrho_{\chi,g}(\varphi, 0)\left(\frac{\tau}{p}\right) \ll p^{-1/2}$$

(since $\Im\mathfrak{m}\tau/p \ll 1/p$) and by (7.3), and the fact that $\hat{K}$ is bounded by a constant depending only on M [a consequence of Proposition 8.2 (1)], we have

$$K_I'(0) \ll \log p$$

and therefore the contribution of the constant terms of Eisenstein series is bounded by

$$\ll \frac{\log p}{|I|} = o(1).$$

For $\varphi = 1$ the exact same argument yields

$$\mu_{K,I,\tau}(1) = \frac{p^{1/2}}{|I|} K_I'(0) \ll \frac{p^{1/2}\log p}{|I|}$$

which is $o(1)$ as long as $|I| \geqslant p^\eta$ with $\eta > 1/2$. This concludes the proof of Theorem 2.3. □

Proof of Corollary 2.4. We now consider a non-constant polynomial ϕ of degree $\deg\phi \geqslant 1$. The probability measure (2.4) satisfies

$$\frac{1}{|I|} \sum_{\substack{x\in\mathbf{F}_p \\ \phi(x)\in I}} \delta_{\Gamma_0(N)\phi(x)\cdot\tau} = \mu + \mu_{K,I,\tau}$$

where

$$K(t) = |\{x \in \mathbf{F}_p \mid \phi(x) = t\}| - 1$$

for $t \in \mathbf{F}_p$. By §10.2, K is a Fourier trace function (not necessarily isotypic), whose Fourier transform is therefore also a Fourier trace function, given by

$$\hat{K}(n) = \frac{1}{p^{1/2}} \sum_{x\in\mathbf{F}_p} e\left(\frac{n\phi(x)}{p}\right), \ (n,p) = 1$$
$$\hat{K}(0) = 0.$$

By Proposition 8.3, we can express $\hat{K}$ as a sum of at most $\deg(\phi)$ functions $\hat{K}_i$ which are irreducible trace functions with conductors bounded by M. The contribution from the terms $\hat{K}_i$ is then treated by the previous proof. □

8 Trace Functions

We now come to the setting of Section 1.3. For an isotypic trace function $K(n)$, we will see that the cohomological theory of algebraic exponential sums and the Riemann Hypothesis over finite fields provide interpretations of the sums $\mathcal{C}(K;\gamma)$, from which it can be shown that trace functions are good.

In this section, we present some preliminary results. In the next one, we give many different examples of trace functions (isotypic or not), and compute upper

bounds for the conductor of the associated sheaves. We then use the cohomological theory to prove Theorem 1.14.

First we recall the following notation for trace functions: for a finite field k, an algebraic variety X/k, a constructible ℓ-adic sheaf $\mathcal{F}$ on X, a finite extension k'/k, and a point $x \in X(k')$, we define

$$(\mathrm{tr}\,\mathcal{F})(k', x) = \mathrm{tr}(\mathrm{Fr}_{k'} \mid \mathcal{F}_{\bar{x}}),$$

the trace of the geometric Frobenius automorphism of k' acting on the stalk of $\mathcal{F}$ at a geometric point $\bar{x}$ over x (seen as a finite-dimensional representation of the Galois group of k'; see [Kat90, 7.3.7]).

Now let p be a prime number, and let $\ell \neq p$ be another auxiliary prime. Let

$$\iota : \bar{\mathbf{Q}}_\ell \longrightarrow \mathbf{C}$$

be a fixed isomorphism, and let $\mathcal{F}$ be an ℓ-adic constructible Fourier sheaf on $\mathbf{A}^1_{\mathbf{F}_p}$ (in the sense of Katz [Kat90, Def. 8.2.1.2]). Recall that we consider the functions

$$K(x) = \iota((\mathrm{tr}\,\mathcal{F})(\mathbf{F}_p, x))$$

for $x \in \mathbf{F}_p = \mathbf{A}^1(\mathbf{F}_p)$. We also consider the (Tate-twisted) Fourier transform $\mathcal{G} = \mathrm{FT}_\psi(\mathcal{F})(1/2)$ with respect to an additive ℓ-adic character ψ of $\mathbf{F}_p$. It satisfies

$$(\mathrm{tr}\,\mathcal{G})(k, v) = -\frac{1}{|k|^{1/2}} \sum_{x \in k} (\mathrm{tr}\,\mathcal{F})(k, x)\psi(\mathrm{tr}_{k/\mathbf{F}_p}(vx)) \tag{8.1}$$

for any finite extension $k/\mathbf{F}_p$ and $v \in k = \mathbf{A}^1(k)$ (see [Kat90, Th. 7.3.8, (4)]).

We collect here the basic properties of Fourier sheaves and of the Fourier transform, consequences of works of Deligne, Laumon, Brylinski and Katz (see [Kat90, §7.3.5], [Kat88, Th. 8.2.5 (3)] and [Kat88, Th. 8.4.1]).

Lemma 8.1 (Fourier sheaves). *Let p and $\ell \neq p$ be primes, and let $\mathcal{F}$ be an ℓ-adic Fourier sheaf on $\mathbf{A}^1_{\mathbf{F}_p}$.*

(1) *The sheaf $\mathcal{F}$ is a middle-extension sheaf: if $j : U \hookrightarrow \mathbf{A}^1$ is the open immersion of a non-empty open set on which $\mathcal{F}$ is lisse, we have*

$$\mathcal{F} \simeq j_*(j^*\mathcal{F}).$$

(2) *Suppose that $\mathcal{F}$ is pointwise ι-pure*[5] *of weight 0, i.e., that it is a trace sheaf. Then*

- *$\mathcal{G} = \mathrm{FT}_\psi(\mathcal{F})(1/2)$ is pointwise ι-pure*[6] *of weight 0;*
- *At the points $v \in \mathbf{A}^1$ where $\mathcal{G}$ is not lisse, it is pointwise mixed of weights $\leqslant 0$, i.e., for any finite field k with $v \in k$, the eigenvalues of the Frobenius of k acting on the stalk of $\mathcal{G}$ at a geometric point $\bar{v}$ over v are $|k|$-Weil numbers of weight at most 0.*

[5] On the maximal open set on which it is lisse.
[6] Idem.

(3) *If $\mathcal{F}$ is geometrically isotypic (resp. geometrically irreducible) then the Fourier transform $\mathcal{G}$ is also geometrically isotypic (resp. geometrically irreducible).*

We defined the conductor of a sheaf in Definition 1.13. An important fact is that this invariant also controls the conductor of the Fourier transform, and that it controls the dimension of cohomology groups which enter into the Grothendieck-Lefschetz trace formula. We state suitable versions of these results:

PROPOSITION 8.2. *Let p be a prime number and $\ell \neq p$ an auxiliary prime.*

(1) *Let $\mathcal{F}$ be an ℓ-adic Fourier sheaf on $\mathbf{A}^1_{\mathbf{F}_p}$, and let $\mathcal{G} = \mathrm{FT}_\psi(\mathcal{F})(1/2)$ be its Fourier transform. Then, for any $\gamma \in \mathrm{GL}_2(\mathbf{F}_p)$, the analytic conductor of $\gamma^*\mathcal{G}$ satisfies*

$$\mathrm{cond}(\gamma^*\mathcal{G}) \leqslant 10\,\mathrm{cond}(\mathcal{F})^2. \tag{8.2}$$

(2) *For $\mathcal{F}_1$ and $\mathcal{F}_2$ lisse ℓ-adic sheaves on an open subset $U \subset \mathbf{A}^1$, we have*

$$\dim H^1_c(U \times \bar{\mathbf{F}}_p, \mathcal{F}_1 \otimes \mathcal{F}_2) \leqslant r_1 r_2(1 + m + \mathrm{cond}(\mathcal{F}_1) + \mathrm{cond}(\mathcal{F}_2)),$$

where

$$m = |(\mathbf{P}^1 - U)(\bar{\mathbf{F}}_p)|, \qquad r_i = \mathrm{rank}(\mathcal{F}_i).$$

(3) *Let $\mathcal{F}_1$ and $\mathcal{F}_2$ be middle-extension ℓ-adic sheaves on $\mathbf{A}^1_{\mathbf{F}_p}$. Then*

$$\mathrm{cond}(\mathcal{F}_1 \otimes \mathcal{F}_2) \leqslant 5\,\mathrm{cond}(\mathcal{F}_1)^2\,\mathrm{cond}(\mathcal{F}_2)^2. \tag{8.3}$$

Note that (8.2) and (8.3) can certainly be improved, but these bounds will be enough for us.

Proof. (1) Since γ is an automorphism of $\mathbf{P}^1$, we have $\mathrm{cond}(\gamma^*\mathcal{G}) = \mathrm{cond}(\mathcal{G})$ and we can assume $\gamma = 1$.

We first bound the number of singularities

$$n(\mathcal{G}) = |\mathbf{P}^1 - U|$$

of $\mathcal{G}$. By [Kat88, Cor. 8.5.8] (and the remark in its proof), on $\mathbf{G}_m$, the Fourier transform is lisse except at points corresponding to Jordan-Hölder components of the local representation $\mathcal{F}(\infty)$ at ∞ which have unique break equal to 1. The number of these singularities outside of 0, ∞ is therefore bounded by the rank of $\mathcal{F}$, hence by the conductor of $\mathcal{F}$, and

$$n(\mathcal{G}) \leqslant 2 + \mathrm{rank}(\mathcal{F}) \leqslant 3\,\mathrm{cond}(\mathcal{F}). \tag{8.4}$$

Now we bound the rank of $\mathcal{G}$. This is given by [Kat90, Lemma 7.3.9 (2)], from which we get immediately

$$\mathrm{rank}(\mathcal{G}) \leqslant \sum_\lambda \max(0, \lambda - 1) + \sum_x (\mathrm{Swan}_x(\mathcal{F}) + \mathrm{rank}(\mathcal{F}))$$

where λ runs over the breaks of $\mathcal{F}(\infty)$, and x over the singularities of $\mathcal{F}$ in $\mathbf{A}^1$. The first term is $\leqslant \mathrm{Swan}_\infty(\mathcal{F})$, so that the rank of $\mathcal{G}$ is bounded by

$$\mathrm{rank}(\mathcal{G}) \leqslant \mathrm{Swan}(\mathcal{F}) + \mathrm{rank}(\mathcal{F})n(\mathcal{F}) \leqslant \mathrm{cond}(\mathcal{F})^2. \tag{8.5}$$

Thus it only remains to estimate the Swan conductors $\mathrm{Swan}_x(\mathcal{G})$ at each singularity. We do this using the local description of the Fourier transform, due to Laumon [Lau87], separately for 0, ∞ and points in $\mathbf{G}_m$.

First case. Let $x = \infty$. By [Kat90, Cor. 7.4.2] we can write

$$\mathcal{G}(\infty) = N_0 \oplus N_\infty \oplus N_m$$

as representations of the inertia group at ∞, where N_0, N_∞ are the local Fourier transform functors denoted

$$\mathrm{FT}_\psi \,\mathrm{loc}(\infty,\infty)\mathcal{F}(\infty), \quad \mathrm{FT}_\psi \,\mathrm{loc}(0,\infty)(\mathcal{F}(0)/\mathcal{F}_0)$$

in loc. cit., and N_m is the sum of the similar contributions of the local Fourier transforms at all $s \in \mathbf{G}_m$. Let s_0, s_∞ and s_m denote the corresponding Swan conductors, which add up to $\mathrm{Swan}_\infty(\mathcal{G})$. By [Kat90, Cor. 7.4.1.1], all breaks of N_0 and N_m are $\leqslant 1$, hence by (8.5)

$$s_0 + s_m \leqslant \dim(N_0) + \dim(N_m) \leqslant \mathrm{rank}(\mathcal{G}) \leqslant \mathrm{Swan}(\mathcal{F}) + \mathrm{rank}(\mathcal{F})n(\mathcal{F}).$$

As for s_∞, by a further result of Laumon [Kat90, Th. 7.5.4 (1)], the contribution s_∞ is equal to the similar contribution of breaks > 1 to the Swan conductor $\mathrm{Swan}_\infty(\mathcal{F})$. Hence by (8.5)

$$\mathrm{Swan}_\infty(\mathcal{G}) \leqslant 2\,\mathrm{Swan}(\mathcal{F}) + \mathrm{rank}(\mathcal{F})n(\mathcal{F}) \leqslant 2\,\mathrm{cond}(\mathcal{F})^2. \tag{8.6}$$

Second case. Let $x = 0$. Then, by [Kat90, Th. 7.5.4 (5)], the Swan conductor $\mathrm{Swan}_0(\mathcal{G})$ is equal to the contribution to $\mathrm{Swan}_\infty(\mathcal{F})$ of the breaks in $]0,1[$, so that

$$\mathrm{Swan}_0(\mathcal{G}) \leqslant \mathrm{Swan}_\infty(\mathcal{F}) \leqslant \mathrm{cond}(\mathcal{F}). \tag{8.7}$$

Third case. Let $x \in \mathbf{G}_m$. By translation, we have

$$\mathrm{Swan}_x(\mathcal{G}) = \mathrm{Swan}_0(\mathrm{FT}_\psi(\mathcal{F} \otimes \mathcal{L}_{\psi(xX)})),$$

so that the previous case gives

$$\mathrm{Swan}_x(\mathcal{G}) \leqslant \mathrm{Swan}_\infty(\mathcal{F} \otimes \mathcal{L}_{\psi(xX)}) \leqslant \mathrm{rank}(\mathcal{F}) + \mathrm{Swan}_\infty(\mathcal{F}) \leqslant \mathrm{cond}(\mathcal{F}).$$

By (8.4) and (8.5), this leads to

$$\sum_x \mathrm{Swan}_x(\mathcal{G}) \leqslant 2\,\mathrm{cond}(\mathcal{F})^2 + 3\,\mathrm{cond}(\mathcal{F})^2 = 5\,\mathrm{cond}(\mathcal{F})^2,$$

and

$$\mathrm{cond}(\mathcal{G}) \leqslant 10\,\mathrm{cond}(\mathcal{F})^2.$$

(2) We use the Euler-Poincaré formula: for a lisse ℓ-adic sheaf $\mathcal{M}$ on an affine curve $U \subset \mathbf{P}^1$ over $\mathbf{F}_p$, we have

$$\dim H_c^1(U\times\bar{\mathbf{F}}_p,\mathcal{M}) = \dim H_c^2(U\times\bar{\mathbf{F}}_p,\mathcal{M})+\operatorname{rank}(\mathcal{M})(-\chi_c(U\times\bar{\mathbf{F}}_p))+\operatorname{Swan}(\mathcal{M}) \quad (8.8)$$

(see [Kat88, 2.3.1]).

We apply this formula to $\mathcal{M} = \mathcal{F}_1 \otimes \mathcal{F}_2$. Since $H_c^2(U \times \bar{\mathbf{F}}_p, \mathcal{M})$ is the space of co-invariants of $\mathcal{M}$

$$\dim H_c^2(U \times \bar{\mathbf{F}}_p, \mathcal{M}) \leqslant r_1 r_2.$$

For the second term, we note simply that

$$\operatorname{rank}(\mathcal{M})(-\chi_c(U \times \bar{\mathbf{F}}_p)) \leqslant m r_1 r_2.$$

For the last term, we bound the Swan conductor at $x \in \mathbf{P}^1 - U$ of $\mathcal{F}_1 \otimes \mathcal{F}_2$ in terms of those of the factors. The existence of such a bound is a well-known result: if λ_1 (resp. λ_2) is the largest break of $\mathcal{F}_1$ (resp. $\mathcal{F}_2$) at x, then all breaks of $\mathcal{F}_1 \otimes \mathcal{F}_2$ at x are at most

$$\max(\lambda_1, \lambda_2) \leqslant \max(\operatorname{Swan}_x(\mathcal{F}_1), \operatorname{Swan}_x(\mathcal{F}_2)),$$

(see [Kat88, Lemma 1.3]) and hence

$$\operatorname{Swan}_x(\mathcal{F}_1 \otimes \mathcal{F}_2) \leqslant \operatorname{rank}(\mathcal{F}_1)\operatorname{rank}(\mathcal{F}_2)(\operatorname{Swan}_x(\mathcal{F}_1) + \operatorname{Swan}_x(\mathcal{F}_2))$$

and

$$\operatorname{Swan}(\mathcal{F}_1 \otimes \mathcal{F}_2) \leqslant r_1 r_2(\operatorname{Swan}(\mathcal{F}_1) + \operatorname{Swan}(\mathcal{F}_2)). \quad (8.9)$$

Adding this to the previous contribution, we get

$$\dim H_c^1(U \times \bar{\mathbf{F}}_p, \mathcal{M}) \leqslant r_1 r_2(1 + m + \operatorname{cond}(\mathcal{F}_1) + \operatorname{cond}(\mathcal{F}_2)),$$

as claimed.

(3) Let $c_i = \operatorname{cond}(\mathcal{F}_i)$, $r_i = \operatorname{rank}(\mathcal{F}_i)$ and n_i the number of singularities of $\mathcal{F}_i$. The rank of $\mathcal{F}_1 \otimes \mathcal{F}_2$ is $r_1 r_2$, and it has $\leqslant n_1 + n_2$ singularities. By (8.9), we have also

$$\operatorname{Swan}(\mathcal{F}_1 \otimes \mathcal{F}_2) \leqslant r_1 r_2(\operatorname{Swan}(\mathcal{F}_1) + \operatorname{Swan}(\mathcal{F}_2)).$$

The result follows by the roughest estimate:

$$\operatorname{cond}(\mathcal{F}_1 \otimes \mathcal{F}_2) \leqslant c_1 c_2 + c_1 + c_2 + c_1 c_2(c_1 + c_2) \leqslant 5c_1^2 c_2^2. \qquad \square$$

We can also explain here how to deal with Fourier trace functions which are not necessarily isotypic.

PROPOSITION 8.3. *Let p be a prime number, $\ell \neq p$ an auxiliary prime. Let $\mathcal{F}$ be a Fourier trace sheaf modulo p with conductor $\leqslant M$.*

There exist at most $\operatorname{rank}(\mathcal{F})$ *isotypic trace sheaves $\mathcal{F}_i$ modulo p, each with conductor $\leqslant M$, such that*

$$(\operatorname{tr}\mathcal{F})(\mathbf{F}_p, x) = \sum_i (\operatorname{tr}\mathcal{F}_i)(\mathbf{F}_p, x)$$

for all $x \in \mathbf{F}_p$. In particular, for any $s \geqslant 1$, the trace function

$$K(n) = \iota((\operatorname{tr}\mathcal{F})(\mathbf{F}_p, n))$$

satisfies $\|K\|_{\mathrm{tr},s} \leqslant M^{s+1}$.

Proof. We refer to [Kat80, §4.4–4.6] for basic facts concerning the correspondance between middle-extension sheaves on $\mathbf{A}^1_{\mathbf{F}_p}$ and representations of the étale fundamental group.

Let $j : U \hookrightarrow \mathbf{A}^1$ be an open dense subset, defined over $\mathbf{F}_p$, such that $\mathcal{F}$ is lisse on U, and let $G = \pi_1(U, \bar{\eta})$ and

$$\varrho \,:\, G \longrightarrow \mathrm{GL}(V)$$

the ℓ-adic representation corresponding to the restriction of $\mathcal{F}$ on U. Let

$$\varrho^{ss} = \bigoplus_{i\in I} \varrho_i$$

be the semisimplification of this representation, where ϱ_i is an irreducible representation of G. We denote by $\tilde{\mathcal{F}}_i$ the corresponding lisse sheaf on U, and let $\mathcal{F}_i = j_*\tilde{\mathcal{F}}_i$. Then each $\mathcal{F}_i$ is a Fourier sheaf modulo p, with conductor $\leqslant M$, and we have

$$(\operatorname{tr}\mathcal{F})(k, x) = \sum_{i\in I} (\operatorname{tr}\mathcal{F}_i)(k, x) \tag{8.10}$$

for any finite extension $k/\mathbf{F}_p$ and $x \in k$. Indeed, this holds by definition for $x \in U(k)$, and this extends to all x by properties of middle-extension sheaves (see Proposition 8.5).

Each ϱ_i is arithmetically irreducible, and there are two possibilities concerning its restriction ϱ_i^g to $G^g = \pi_1(U \times \bar{\mathbf{F}}_p, \bar{\eta})$: (1) either ϱ_i^g is isotypic, and hence $\mathcal{F}_i$ is an isotypic trace sheaf; or (2) there exists an integer $m \geqslant 2$, and a representation τ_i of the proper normal subgroup $H = \pi_1(U \times \mathbf{F}_{p^m}, \bar{\eta})$ of G such that

$$\varrho_i = \operatorname{Ind}_H^G \tau_i$$

(see, e.g., [Ser71, Prop. 8.1] or [Kow14, Prop. 2.8.20]). We claim that in this second case, the trace function of $\mathcal{F}_i$ is identically zero on $\mathbf{F}_p$, which finishes the proof since we can then drop $\mathcal{F}_i$ from the decomposition (8.10).

To check the claim, note that the formula for the character of an induced representation shows that

$$\operatorname{tr} \varrho_i(g) = 0$$

for any $g \notin H$ (see, e.g. [Kow14, Prop. 2.7.43]). Hence the trace function vanishes obviously on $U(\mathbf{F}_p)$ since the Frobenius elements associated to $x \in U(\mathbf{F}_p)$ relative to $\mathbf{F}_p$ are not in H.

This property extends to $x \in (\mathbf{A}^1 - U)(\mathbf{F}_p)$ by a similar argument (we thank N. Katz for explaining this last point; note that we could also treat separately the points in $\mathbf{A}^1 - U$, which would lead at most to slightly worse bounds for the trace norm of K).

Let $\tilde{G} = \pi_1(\mathbf{A}^1, \bar{\eta})$ be the fundamental group of the affine line. There is a surjective homomorphism

$$\tilde{G} \longrightarrow G.$$

The group $\tilde{G}$ contains as normal subgroups

$$\tilde{G}^g = \pi_1(\mathbf{A}^1 \times \bar{\mathbf{F}}_p, \bar{\eta}), \qquad \tilde{H} = \pi_1(\mathbf{A}^1 \times \mathbf{F}_{p^m}, \bar{\eta}),$$

with corresponding surjective morphisms $\tilde{G}^g \longrightarrow G^g$ and $\tilde{H} \longrightarrow H$.

Composing these with τ_i and ϱ_i gives representations $\tilde{\tau}_i$ and $\tilde{\varrho}_i$ of $\tilde{H}$ and $\tilde{G}$, respectively, with $\tilde{\varrho}_i = \operatorname{Ind}_{\tilde{H}}^{\tilde{G}} \tilde{\tau}_i$.

The stalk of $\mathcal{F}_i$ at a geometric point above $x \in (\mathbf{A}^1 - U)(\mathbf{F}_p)$ is isomorphic, as a vector space with the action of the Galois group of $\mathbf{F}_p$, to the invariant space $\varrho_i^{I_x}$ under the inertia subgroup at x, which is a subgroup I_x of $\tilde{G}$.

The space of $\tilde{\varrho}_i$ can be written as a direct sum

$$\bigoplus_{\sigma \in \tilde{G}/\tilde{H}} W_\sigma$$

where the spaces W_σ are $\tilde{H}$-stable and permuted by $\tilde{G}$. Moreover, any $g \in \tilde{G} - \tilde{H}$ permutes the W_σ without fixed points, because $\tilde{H}$ is normal in $\tilde{G}$.

The point is that since $I_x \subset \tilde{G}^g \subset \tilde{H}$ (the inertia group is a subgroup of the geometric Galois group) and each W_σ is $\tilde{H}$-stable, we have

$$\tilde{\varrho}_i^{I_x} = \bigoplus_{\sigma \in G/H} W_\sigma^{I_x}.$$

(in other words, this shows that $\tilde{\varrho}_i^{I_x} \simeq \operatorname{Ind}_{\tilde{H}}^{\tilde{G}} \tilde{\tau}_i^{I_x}$).

The matrix representing the action on $\tilde{\varrho}_i^{I_x}$ of any element g in the decomposition group D_x mapping to the Frobenius conjugacy class at x in D_x/I_x is block-diagonal with respect to this decomposition. Since $g \notin \tilde{H}$, this block-diagonal matrix has zero diagonal blocks, hence its trace, which is the value of the trace function of $\mathcal{F}_i$ at x, also vanishes. □

The following is relevant to Theorem 2.3.

PROPOSITION 8.4. *Let p be a prime number, $\ell \neq p$ an auxiliary prime. Let $\mathcal{F}$ be an ℓ-adic Fourier trace sheaf modulo p with conductor $\leqslant N$. Let $K(n)$ be the corresponding Fourier trace function. Then, for any $x \in \mathbf{F}_p$, $[+x]^*K(n) = K(x+n)$ defines a Fourier trace function associated to the sheaf*

$$\mathcal{F}^{(x)} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^* \mathcal{F},$$

and we have $\mathrm{cond}(\mathcal{F}^{(x)}) = \mathrm{cond}(\mathcal{F}) \leqslant N$ for all $x \in \mathbf{F}_p$.

Proof. It is clear that $\mathcal{F}^{(x)}$ has the right trace function and that it is a Fourier trace sheaf, with the same conductor as $\mathcal{F}$. □

Finally, we state a well-known criterion for geometric isomorphism of sheaves, that says that two irreducible middle-extension sheaves are geometrically isomorphic if their trace functions are equal on $\mathbf{A}^1(\bar{\mathbf{F}}_p)$ "up to a constant depending on the definition field". Precisely:

PROPOSITION 8.5 (Geometric isomorphism criterion). *Let k be a finite field, and let $\mathcal{F}_1$ and $\mathcal{F}_2$ be geometrically irreducible ℓ-adic sheaves, lisse on a non-empty open set U/k and pointwise pure of weight 0. Then $\mathcal{F}_1$ is geometrically isomorphic to $\mathcal{F}_2$ if and only if there exists $\alpha \in \bar{\mathbf{Q}}_\ell^\times$ such that for all finite extensions k_1/k, we have*

$$(\mathrm{tr}\,\mathcal{F}_1)(k_1, x) = \alpha^{[k_1:k]}(\mathrm{tr}\,\mathcal{F}_2)(k_1, x) \tag{8.11}$$

for all $x \in U(k_1)$.

In particular, if $\mathcal{F}_1$ and $\mathcal{F}_2$ are irreducible Fourier sheaves, they are geometrically isomorphic if and only if there exists $\alpha \in \bar{\mathbf{Q}}_\ell^\times$ such that for all finite extensions k_1/k, we have

$$(\mathrm{tr}\,\mathcal{F}_1)(k_1, x) = \alpha^{[k_1:k]}(\mathrm{tr}\,\mathcal{F}_2)(k_1, x) \tag{8.12}$$

for all $x \in k_1$.

Proof (Sketch of proof). This is a well-known fact; it is basically an instance of what is called "Clifford theory" in representation theory. We sketch a proof for completeness. In the "if" direction, note that (8.11) shows that $\mathcal{F}_1$ and $\alpha^{\deg(\cdot)} \otimes \mathcal{F}_2$ are lisse sheaves on U with the same traces of Frobenius at all points of U; the Chebotarev Density Theorem shows that the Frobenius conjugacy classes are dense in $\pi_1(U, \bar{\eta})$, so we conclude that $\mathcal{F}_1 \simeq \alpha^{\deg(\cdot)} \otimes \mathcal{F}_2)$ as lisse sheaves on U. But then restriction to the geometric fundamental group (the kernel of the degree) gives $\mathcal{F}_1 \simeq \mathcal{F}_2$ geometrically on U.

Conversely, if $\mathcal{F}_1$ is geometrically isomorphic to $\mathcal{F}_2$, and ϱ_i is the representation of $\pi_1(U, \bar{\eta})$ associated to $\mathcal{F}_i$, then representation theory (see, e.g., [Kow14, 2.8.2])

shows that there exists a character χ of the abelian group $\pi_1(U,\bar\eta)/\pi_1(U\times\bar{\mathbf{F}}_p,\bar\eta)$ such that

$$\varrho_1 \simeq \chi\otimes\varrho_2.$$

But such characters are of the type $\alpha^{\deg(\cdot)}$ since the quotient is isomorphic to the Galois group $\mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$.

For the second part, apply the first with the fact that middle-extension sheaves on $\mathbf{A}^1$ are geometrically isomorphic if and only if their restrictions to a common dense open set where they are lisse are geometrically isomorphic. □

Here is a last definition. If $\mathcal{F}$ is a Fourier sheaf on $\mathbf{A}^1/k$, we write $\mathrm{D}(\mathcal{F})$ for the middle-extension dual of $\mathcal{F}$, i.e., given a dense open set $j : U\hookrightarrow\mathbf{A}^1$ where $\mathcal{F}$ is lisse, we have

$$\mathrm{D}(\mathcal{F}) = j_*((j^*\mathcal{F})'),$$

where the prime denotes the lisse sheaf on U associated to the contragredient of the representation of the fundamental group of U which corresponds to $j^*\mathcal{F}$ (see [Kat90, 7.3.1]). If $\mathcal{F}$ is pointwise pure of weight 0, it is known that

$$\iota((\mathrm{tr}\,\mathrm{D}(\mathcal{F}))(k',x)) = \overline{\iota((\mathrm{tr}\,\mathcal{F})(k',x))} \tag{8.13}$$

for all finite extensions k'/k and all $x\in k'$.

9 Application of the Riemann Hypothesis

We can now prove that correlation sums of trace functions are small, except for matrices in the Fourier–Möbius group. This is the crucial argument that relies on the Riemann Hypothesis over finite fields.

Theorem 9.1 (Cohomological bound for correlation sums). *Let p be a prime number, $\ell\neq p$ another prime. Let $\mathcal{F}$ be an isotypic trace sheaf on $\mathbf{A}^1_{\mathbf{F}_p}$ and let K denote its trace function. We have*

$$|\mathcal{C}(K;\gamma)| \leqslant M_1 + M_2 p^{1/2} \tag{9.1}$$

if $\gamma\notin\mathbf{G}_{\mathcal{F}}$ where

$$M_1 \leqslant 6\,\mathrm{cond}(\mathcal{F})^5, \qquad M_2 \leqslant 24\,\mathrm{cond}(\mathcal{F})^6. \tag{9.2}$$

The bounds (9.2) are certainly not sharp, but they show that the result is completely effective and explicit.

Proof. We denote by $\mathcal{G}$ the Fourier transform of $\mathcal{F}$ computed with respect to some non-trivial additive character ψ, and by U the largest open subset of $\mathbf{A}^1$ where $\mathcal{G}$ is lisse.

Let

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(\mathbf{F}_p).$$

We define the constructible ℓ-adic sheaf

$$\mathcal{H}_\gamma = \gamma^* \mathcal{G} \otimes \mathrm{D}(\mathcal{G})$$

on $\mathbf{P}^1_{\mathbf{F}_p}$. This sheaf is lisse and pointwise ι-pure of weight 0 on any open subset of $\mathbf{P}^1$ where it is lisse, in particular on the non-empty open set

$$U_\gamma = \gamma^{-1} U \cap U \subset \mathbf{A}^1 - \{-d/c\},$$

and for $z \in U_\gamma(\mathbf{F}_p)$, we have

$$\iota((\mathrm{tr}\, \mathcal{H}_\gamma)(\mathbf{F}_p, z)) = \hat{K}(\gamma \cdot z)\overline{\hat{K}(z)}$$

by the definition (1.16) of the Fourier transform and by (8.13). Thus we have

$$\mathcal{C}(K; \gamma) = \iota\left(\sum_{z \in U_\gamma(\mathbf{F}_p)} (\mathrm{tr}\, \mathcal{H}_\gamma)(\mathbf{F}_p, z) \right) + \sum_{\substack{z \in \mathbf{F}_p - U_\gamma(\mathbf{F}_p) \\ z \neq -d/c}} \hat{K}(\gamma \cdot z)\overline{\hat{K}(z)}. \tag{9.3}$$

According to the Grothendieck–Lefschetz trace formula (see, e.g., [Del77, Rapport, Th. 3.2]), we have

$$\begin{aligned} \sum_{z \in U_\gamma(\mathbf{F}_p)} (\mathrm{tr}\, \mathcal{H}_\gamma)(k, z) &= \mathrm{tr}(\mathrm{Fr} \mid H^0_c(U_\gamma \times \bar{\mathbf{F}}_p, \mathcal{H}_\gamma)) \\ &\quad - \mathrm{tr}(\mathrm{Fr} \mid H^1_c(U_\gamma \times \bar{\mathbf{F}}_p, \mathcal{H}_\gamma)) + \mathrm{tr}(\mathrm{Fr} \mid H^2_c(U_\gamma \times \bar{\mathbf{F}}_p, \mathcal{H}_\gamma)) \end{aligned} \tag{9.4}$$

where Fr denotes the geometric Frobenius of $\mathbf{F}_p$ acting on the cohomology groups of $\mathcal{H}_\gamma$.

Since U_γ is an affine curve, we have $H^0_c(U_\gamma \times \bar{\mathbf{F}}_p, \mathcal{H}_\gamma) = 0$ (see, e.g., [Del80, (1.4.1)b]). Next, the coinvariant formula for H^2_c on a curve (see [Del80, (1.4.1)b]) states that $H^2_c(U_\gamma \times \bar{\mathbf{F}}_p, \mathcal{H}_\gamma)$ is isomorphic to the space of coinvariants of $\pi_1(U_\gamma \times \bar{\mathbf{F}}_p, \bar{\eta})$ acting on $\mathcal{H}_{\gamma, \bar{\eta}}$. In particular, we have

$$H^2_c(U_\gamma \times \bar{\mathbf{F}}_p, \mathcal{H}_\gamma) = 0$$

if this coinvariant space is zero. We next show that this is the case if $\gamma \notin \mathbf{G}_{\mathcal{F}}$.

The sheaf $\mathcal{F}$ is geometrically isotypic when restricted to an open set V where it is lisse. Let $j : V \hookrightarrow \mathbf{A}^1$ be the open immersion of V in the affine line. There exists a (geometrically) irreducible lisse sheaf $\mathcal{F}_1$ on $V \times \bar{\mathbf{F}}_p$ such that

$$\mathcal{F} \simeq (j_* \mathcal{F}_1)^{\oplus d}$$

as sheaves on $\mathbf{A}^1 \times \bar{\mathbf{F}}_p$ (since both sides are middle-extension sheaves which are isomorphic on $V \times \bar{\mathbf{F}}_p$). This formula shows that $j_*\mathcal{F}_1$ is a Fourier sheaf on $\mathbf{A}^1 \times \bar{\mathbf{F}}_p$. Taking the Fourier transforms, it follows that we have a geometric isomorphism

$$\mathcal{G} \simeq \mathrm{FT}(j_*\mathcal{F}_1))(1/2)^{\oplus d},$$

and hence (since the Fourier transform of a geometrically irreducible sheaf is geometrically irreducible) that $\mathcal{G}$ is geometrically isotypic on U_γ, with irreducible component

$$\mathcal{G}_1 = \mathrm{FT}(j_*\mathcal{F}_1))(1/2).$$

Applying γ and taking dual, we see that $\gamma^*\mathcal{G}$ and $\mathrm{D}(\mathcal{G})$ are also lisse and geometrically isotypic on U_γ. Moreover, the geometrically irreducible components of $\gamma^*\mathcal{G}$ is $\gamma^*\mathcal{G}_1$, and that of $\mathrm{D}(\mathcal{G})$ is $\mathrm{D}(\mathcal{G}_1)$.

Finally, by Schur's Lemma, the coinvariant space of $\pi_1(U_\gamma \times \bar{\mathbf{F}}_p, \bar{\eta})$ acting on $\mathcal{H}_{\gamma,\bar{\eta}}$ is zero unless we have a geometric isomorphism

$$\gamma^*\mathcal{G}_1 \simeq \mathcal{G}_1,$$

which holds if and only if $\gamma^*\mathcal{G}$ is geometrically isomorphic to $\mathcal{G}$.

Thus, if $\gamma \notin \mathbf{G}_{\mathcal{F}}$, the only contribution to the expression (9.4) comes from the cohomology group $H^1_c(U_\gamma \times \bar{\mathbf{F}}_p, \mathcal{H}_\gamma)$. But since $\mathcal{H}_\gamma$ is pointwise pure of weight 0 on U_γ, it follows from Deligne's fundamental proof of the Riemann Hypothesis over finite fields (see [Del80, Th. 3.3.1]) that all eigenvalues of Fr acting on $H^1_c(U_\gamma \times \bar{\mathbf{F}}_p, \mathcal{H}_\gamma)$ are algebraic numbers, all conjugates of which are of modulus at most $p^{1/2}$.

Thus, using (9.3), we obtain

$$|\mathcal{C}(K;\gamma)| \leqslant p^{1/2} \dim H^1_c(U_\gamma \times \bar{\mathbf{F}}_p, \mathcal{H}_\gamma) + \sum_{\substack{z \in \mathbf{F}_p - U_\gamma(\mathbf{F}_p) \\ z \neq -d/c}} \hat{K}(\gamma \cdot z)\overline{\hat{K}(z)}$$

for $\gamma \notin \mathbf{G}_{\mathcal{F}}$. By Lemma 8.1, at the points $z \in \mathbf{F}_p - U_\gamma(\mathbf{F}_p)$, we have

$$|\hat{K}(\gamma \cdot z)| \leqslant \mathrm{rank}(\gamma^*\mathcal{G}) = \mathrm{rank}(\mathcal{G}), \qquad |\hat{K}(z)| \leqslant \mathrm{rank}(\mathcal{G}),$$

since $\mathcal{G}$ and $\gamma^*\mathcal{G}$ have local weights $\leqslant 0$ at all points. There are at most $2n(\mathcal{G})$ points where we use this bound, and thus

$$\left| \sum_{\substack{z \in \mathbf{F}_p - U_\gamma(\mathbf{F}_p) \\ z \neq -d/c}} \hat{K}(\gamma \cdot z)\overline{\hat{K}(z)} \right| \leqslant 2n(\mathcal{G})\,\mathrm{rank}(\mathcal{G})^2.$$

Finally we have

$$\dim H^1_c(U_\gamma \times \bar{\mathbf{F}}_p, \mathcal{H}_\gamma) \leqslant \mathrm{rank}(\mathcal{G})^2(1 + n(\mathcal{G}) + 2\,\mathrm{cond}(\mathcal{G})) \leqslant 24\,\mathrm{cond}(\mathcal{F})^6$$

by Proposition 8.2 and (8.4, 8.5), and similarly

$$2n(\mathcal{G})\,\mathrm{rank}(\mathcal{G})^2 \leqslant 6\,\mathrm{cond}(\mathcal{F})^5. \qquad \square$$

Theorem 9.1 justifies the Definition 1.16 of the Fourier–Möbius group $\mathbf{G}_{\mathcal{F}}$ of an isotypic trace sheaf. Note that this group $\mathbf{G}_{\mathcal{F}}$ depends on ψ, although the notation does not reflect this ($\mathbf{G}_{\mathcal{F}}$ is well-defined up to $\mathbf{F}_p$-conjugacy, however).

Now from the definition of the Fourier–Möbius group and Theorem 9.1, we get our interpretation of $\mathbf{G}_{K,M}$ for irreducible trace functions:

Corollary 9.2. *Let p be a prime number, $\mathcal{F}$ an isotypic trace sheaf on $\mathbf{A}^1_{\mathbf{F}_p}$. Let K be the corresponding isotypic trace function. Then, for*

$$M \geqslant 6\operatorname{cond}(\mathcal{F})^5 + 24\operatorname{cond}(\mathcal{F})^6,$$

we have $\mathbf{G}_{K,M} \subset \mathbf{G}_{\mathcal{F}}(\mathbf{F}_p)$.

Our goal is now to prove Theorem 1.14: all isotypic trace functions are (p, M)-good, where M depends only on the conductor of the associated sheaf. This is done by distinguishing two cases, depending on whether the order of the finite subgroup $\mathbf{G}_{\mathcal{F}}(\mathbf{F}_p)$ is divisible by p or not.

For the first case, we have the following lemma, which is an immediate consequence of the classification of Artin-Schreier sheaves (or of Weil's theory, when spelled-out in terms of exponential sums).

Lemma 9.3. *Let p be a prime number, $\ell \neq p$ an auxiliary prime, ψ a non-trivial ℓ-adic additive character of $\mathbf{F}_p$. Let $\gamma_0 \in \mathrm{PGL}_2(\mathbf{F}_p)$, and let $\mathcal{F} = \mathcal{L}_{\psi(\gamma_0(X))}$. Then for $\gamma \in \mathrm{PGL}_2(\bar{\mathbf{F}}_p)$, we have a geometric isomorphism $\gamma^*\mathcal{F} \simeq \mathcal{F}$ if and only if γ is in the unipotent radical of the stabilizer of $\gamma_0^{-1} \cdot \infty$.*

Below we denote by $\mathrm{U}^x \subset \mathrm{PGL}_2$ the unipotent radical of the Borel subgroup of PGL_2 fixing $x \in \mathbf{P}^1$. Recall that, for $x \neq y$ in $\mathbf{P}^1$, we denote by $\mathrm{T}^{x,y} \subset \mathrm{PGL}_2$ the maximal torus of elements fixing x and y, and by $\mathrm{N}^{x,y}$ its normalizer.

Proof (Proof of Theorem 1.14). By Corollary 9.2, there exists $M \leqslant 30N^6$ such that

$$\mathbf{G}_{K,M} \subset G = \mathbf{G}_{\mathcal{F}}(\mathbf{F}_p),$$

which is a subgroup of $\mathrm{PGL}_2(\mathbf{F}_p)$. We distinguish two cases:

— If $p \nmid |G|$, then the classification of finite subgroups of $\mathrm{PGL}_2(\bar{\mathbf{F}}_p)$ of order coprime to the characteristic (see for instance [Bea10] and the references there) show that we have either $|G| \leqslant 60$, or G is cyclic or dihedral. In the former situation, the non-trivial elements of G are non-parabolic and belong to at most 59 different tori T^{x_i,y_i} and the function K is $(p, \max(59, M))$-good by Definition 1.8. In the cyclic or dihedral situation, one also knows that G is contained in the normalizer $\mathrm{N}^{x,y}$ of a certain fixed maximal torus $\mathrm{T}^{x,y}$ (indeed, if G is cyclic, all its elements are diagonalizable in a common basis, and it is a subgroup of a maximal torus; if G is dihedral of order $2r$, the cyclic subgroup of order r is contained in a maximal torus, and any element not contained in it is in the normalizer, see e.g., [Bea10, Prop. 4.1]). Hence K is (p, M)-good, with at most one pair (x, y) in (1.13).

— If $p \mid |G|$, we fix $\gamma_0 \in G$ of order p and denote by $x \in \mathbf{P}^1(\mathbf{F}_p)$ its unique fixed point. Let $\sigma \in \mathrm{PGL}_2(\mathbf{F}_p)$ be such that

$$\sigma \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \sigma^{-1} = \gamma_0$$

and let $\mathcal{G}_1 = \sigma^* \mathcal{G}$. We then have a geometric isomorphism

$$[+1]^* \mathcal{G}_1 \simeq \mathcal{G}_1.$$

Suppose first that $\mathcal{G}_1$ is ramified at some $x \in \mathbf{A}^1(\overline{\mathbf{F}_p})$. Then, by the above, it is ramified at x, $x+1, \dots, x+p-1$, and therefore we obtain

$$\mathrm{cond}(\mathcal{G}) = \mathrm{cond}(\mathcal{G}_1) \geqslant p + \mathrm{rank}(\mathcal{G}_1) = p + \mathrm{rank}(\mathcal{G}),$$

and in that case K is (p, N)-good for trivial reasons.

Now assume that $\mathcal{G}_1$ is lisse on $\mathbf{A}^1(\overline{\mathbf{F}_p})$. The geometrically irreducible component $\mathcal{G}_2$ of $\mathcal{G}_1$ satisfies also $[+1]^* \mathcal{G}_2 \simeq \mathcal{G}_2$. Hence, by [FKM13, Lemma 5.4, (2)] (applied with $G = \mathbf{F}_p$ and $P_h = 0$), either

$$\mathrm{cond}(\mathcal{G}_1) \geqslant \mathrm{Swan}_\infty(\mathcal{G}_2) \geqslant p + \mathrm{rank}(\mathcal{G})$$

(and we are done as above) or else $\mathcal{G}_2$ is geometrically isomorphic to some Artin-Schreier sheaf $\mathcal{L}_\psi$ for some non-trivial additive character ψ of $\mathbf{F}_p$.

In that case, we see that $\mathcal{G}_1$ is geometrically isomorphic to a sum of copies of $\mathcal{L}_\psi$. Hence there exists $a \in \mathbf{F}_p^\times$ and algebraic numbers $\alpha_1, \dots, \alpha_{\mathrm{rank}(\mathcal{G})}$, all of weight 0, such that

$$\iota((\mathrm{tr}\, \mathcal{G}_1)(\mathbf{F}_p, n)) = (\alpha_1 + \cdots + \alpha_{\mathrm{rank}(\mathcal{G})}) e\left(\frac{an}{p}\right) = \iota((\mathrm{tr}\, \mathcal{G}_1)(\mathbf{F}_p, 0)) e\left(\frac{an}{p}\right)$$

for all $n \in \mathbf{F}_p$.

Hence we get

$$\hat{K}(n) = e\left(\frac{a\sigma^{-1}(n)}{p}\right) \hat{K}(\sigma \cdot 0)$$

for all $n \neq x$ in $\mathbf{F}_p$. By Proposition 8.5, the trace function $K(n)$ is a multiple of the trace function of the (possibly) different Fourier trace sheaf $\tilde{\mathcal{F}}$, whose Fourier transform is geometrically isomorphic to the irreducible sheaf

$$\mathcal{L}_{\psi(a\sigma^{-1}(X))}.$$

But for this sheaf, we know by Lemma 9.3 that $\mathbf{G}_{\tilde{\mathcal{F}}} = \mathrm{U}^x$, and in particular all elements of $\mathbf{G}_{\tilde{\mathcal{F}}}$ are parabolic. Furthermore, the conductor of $\tilde{\mathcal{F}}$ is absolutely bounded (the conductor of its Fourier transform is 3, and we apply the Fourier inversion and Proposition 8.2, or we could do a direct computation). Since we have

$$|\hat{K}(\sigma \cdot 0)| = |\alpha_1 + \cdots + \alpha_{\mathrm{rank}(\mathcal{G})}| \leqslant \mathrm{rank}(\mathcal{G}) \leqslant 10N^2,$$

and

$$\mathcal{C}(K;\gamma) = |\hat{K}(\sigma\cdot 0)|^2\mathcal{C}(\tilde{K};\gamma)$$

where $\tilde{K}$ is the trace function of $\tilde{\mathcal{F}}$, it follows that $\mathbf{G}_{K,aN^4} \subset \mathbf{G}_{\tilde{\mathcal{F}}}(\mathbf{F}_p)$ for some absolute constant $a \geqslant 1$. It follows by Definition 1.8 that the function K is (p, aN^4)-good. □

10 Examples of Trace Functions

In this section, we will discuss four classes of functions $K(n)$ that arise as trace functions. In a first reading, only the definitions of these functions may be of interest, rather than the technical verification that they satisfy the necessary conditions.

We note that these examples are by no means an exhaustive list. One can find more examples, in particular, in [Kat90, §7.11].

10.1 Additive and multiplicative characters. We recall now how the characters (1.6) of Corollary 2.2 fit in the framework of trace functions. Let η be an ℓ-adic-valued multiplicative character

$$\eta : \mathbf{F}_p^\times \longrightarrow \bar{\mathbf{Q}}_\ell^\times$$

and let ψ be an ℓ-adic additive character

$$\psi : \mathbf{F}_p \longrightarrow \bar{\mathbf{Q}}_\ell^\times.$$

The classical constructions of Artin-Schreier and Kummer sheaves show that, for any $\ell \neq p$, one can construct ℓ-adic sheaves $\mathcal{L}_{\psi(\phi)}$ and $\mathcal{L}_{\eta(\phi)}$ on $\mathbf{A}^1_{\mathbf{F}_p}$ such that we have

$$(\operatorname{tr}\mathcal{L}_{\psi(\phi)})(\mathbf{F}_p, x) = \begin{cases} \psi(\phi(x)) & \text{if } \phi(x) \text{ is defined,} \\ 0 & \text{if } x \text{ is a pole of } \phi, \end{cases}$$

and

$$(\operatorname{tr}\mathcal{L}_{\eta(\phi)})(\mathbf{F}_p, x) = \begin{cases} \eta(\phi(x)) & \text{if } \phi(x) \text{ is defined and non-zero,} \\ 0 & \text{if } x\text{is a zero or pole of}\phi \end{cases}$$

(these are the extensions by zero to $\mathbf{A}^1$ of the pullback by ϕ of the lisse Artin-Schreier and Kummer sheaves defined on the corresponding open subsets of $\mathbf{A}^1$).

Fix an isomorphism $\iota : \bar{\mathbf{Q}}_\ell \to \mathbf{C}$. We assume that ψ is the standard character, so that

$$\iota(\psi(x)) = e\left(\frac{x}{p}\right),$$

for $x \in \mathbf{F}_p$. Similarly, if χ is a Dirichlet character modulo p, there is a multiplicative character η such that

$$\iota(\eta(x)) = \chi(x)$$

for $x \in \mathbf{F}_p$.

Let then ϕ_1, $\phi_2 \in \mathbf{Q}(X)$ be rational functions as in (1.6), with $\phi_2 = 1$ if χ is trivial. The ℓ-adic sheaf

$$\mathcal{F} = \mathcal{L}_{\eta(\phi_2)} \otimes \mathcal{L}_{\psi(\phi_1)}, \tag{10.1}$$

is such that

$$\iota((\operatorname{tr}\mathcal{F})(\mathbf{F}_p, x)) = \begin{cases} \chi(\phi_2(x))e\left(\dfrac{\phi_1(x)}{p}\right) & \text{if } \phi_1, \phi_2 \text{ are defined at } x, \\ 0 & \text{otherwise,} \end{cases}$$

which corresponds exactly to (1.6).

Proposition 10.1 (Mixed character functions are trace functions). *Assume that either ϕ_1 is not a polynomial of degree $\leqslant 1$, or if χ is non-trivial and ϕ_2 is not of the form $t\phi_3^h$, where $h \geqslant 2$ is the order of χ.*

(1) *The function above is an irreducible trace function.*

(2) *Let d_1 be the number of poles of ϕ_1, with multiplicity, and d_2 the number of zeros and poles of ϕ_2 (where both are viewed as functions from $\mathbf{P}^1$ to $\mathbf{P}^1$). The analytic conductor of the sheaf $\mathcal{F}$ satisfies*

$$\operatorname{cond}(\mathcal{F}) \leqslant 1 + 2d_1 + d_2.$$

Proof. (1) The sheaf $\mathcal{F}$ is pointwise pure of weight 0 on the open set U where ϕ_1 and ϕ_2 are both defined and ϕ_2 is non-zero, which is the maximal open set on which $\mathcal{F}$ is lisse. Moreover, it is of rank 1 on this open set, and therefore geometrically irreducible. By [Kat88, Proof of Lemma 8.3.1], $\mathcal{F}$ is a Fourier sheaf provided it is not geometrically isomorphic to the Artin-Schreier sheaf $\mathcal{L}_{\psi(sX)}$ for some $s \in \mathbf{A}^1$, which is the case under our assumption.

(2) The rank of $\mathcal{F}$ is one. The singular points are the poles of ϕ_1 and the zeros and poles of ϕ_2, so their number is bounded by $d_1 + d_2$. Furthermore, the Swan conductor at any singularity x is the same as that of $\mathcal{L}_{\psi(\phi_1)}$, since all Kummer sheaves are everywhere tame. Thus only poles of ϕ_1 contribute to the Swan conductor, and for such a pole x, the Swan conductor is at most the order of the pole at x, whose sum is d_1 (it is equal to the order of the pole when ϕ_1 is Artin-Schreier-reduced at x, which happens if p is larger than the order of the pole, see, e.g., [Del77, Sommes Trig., (3.5.4)]).

10.2 "Fiber counting" functions and their Fourier transforms. This example is discussed in greater detail in [Kat90, §7.10], where a number of variants also appear.

Let $C/\mathbf{Q}$ be a geometrically connected smooth algebraic curve and let $\phi : C \longrightarrow \mathbf{P}^1$ be a non-constant morphism of degree $\geqslant 2$. Let D be the divisor of poles of ϕ, $Z \subset C - D$ the divisor of zeros of $d\phi$ and $S = \phi(Z)$. For p large enough (in particular we assume $p > \deg(\phi)$), this situation has good reduction modulo p and we may consider the "fiber-counting function"

$$\begin{cases} \mathbf{F}_p \longrightarrow \mathbf{Z} \\ x \mapsto N(\phi; x) = |\{y \in C(\mathbf{F}_p) \mid \phi(y) = x\}|. \end{cases}$$

Defining $\mathcal{F} = \phi_* \bar{\mathbf{Q}}_\ell$, the direct image of the trivial ℓ-adic sheaf, we have

$$N(\phi; x) = \iota((\operatorname{tr} \mathcal{F})(\mathbf{F}_p, x)).$$

The sheaf $\mathcal{F}$ is a constructible ℓ-adic sheaf of rank $\deg(\phi)$ on $\mathbf{A}^1$, and it is lisse and pointwise pure of weight 0 outside S and tamely ramified there. It is not irreducible, but the kernel of the trace map

$$\tilde{\mathcal{F}} = \ker(\mathcal{F} \xrightarrow{\text{tr}} \bar{\mathbf{Q}}_\ell)$$

might be irreducible. This sheaf $\tilde{\mathcal{F}}$ is of rank $\deg(\phi) - 1$, of conductor $\operatorname{cond}(\tilde{\mathcal{F}}) \leqslant \deg(\phi) + |S|$ and its trace function is

$$(\operatorname{tr} \tilde{\mathcal{F}})(\mathbf{F}_p, x) = N(\phi; x) - 1 = \tilde{N}(\phi; x).$$

By [Kat90, Lemma 7.10.2.1], $\tilde{\mathcal{F}}$ is a Fourier trace sheaf for $p > \deg(\phi)$. The situation becomes even clearer if we assume that ϕ is *supermorse*, i.e.:

(1) The zeros of the derivative $d\phi$ are simple;
(2) ϕ separates the zeros of $d\phi$, i.e., the size of the set $S = \{\phi(x) \mid d\phi(x) = 0\}$ of critical values of ϕ is the same as the number of zeros of $d\phi$.

In this case, by [Kat90, Lemma 7.10.2.3], the sheaf $\tilde{\mathcal{F}}$ is geometrically irreducible for $p > \deg(\phi)$, and thus $\tilde{N}(\phi; x)$ is then an irreducible trace function.

For a given non-trivial ℓ-adic additive character ψ, the Fourier transform sheaf $\tilde{\mathcal{G}} = \mathrm{FT}_\psi(\tilde{\mathcal{F}})(1/2)$ has trace function given by

$$\begin{aligned} |k|^{1/2}(\operatorname{tr} \tilde{\mathcal{G}})(k, v) &= -\sum_{x \in k} \left(\sum_{\substack{y \in C(k) - D(k) \\ \phi(y) = x}} 1 - 1 \right) \psi(\operatorname{tr}_{k/\mathbf{F}_p}(xv)) \\ &= -\sum_{y \in C(k) - D(k)} \psi(\operatorname{tr}_{k/\mathbf{F}_p}(v\phi(y))) + \sum_{x \in k} \psi(\operatorname{tr}_{k/\mathbf{F}_p}(xv)) \end{aligned}$$

for any finite-extension $k/\mathbf{F}_p$ and $v \in k$, which gives

$$(\operatorname{tr} \tilde{\mathcal{G}})(k, v) = -|k|^{-1/2} \sum_{x \in C(k) - D(k)} \psi(\operatorname{tr}_{k/\mathbf{F}_p}(v\phi(x)))$$

for $v \in k^\times$ and

$$(\operatorname{tr} \tilde{\mathcal{G}})(k, 0) = |k|^{1/2} - |k|^{-1/2}|C(k) - D(k)|.$$

(note that since C is geometrically connected, we have $|C(k)| = |k| + O(g_C\sqrt{|k|})$, so this last quantity is bounded.)

Since $\tilde{\mathcal{F}}$ is an irreducible Fourier sheaf, so is $\tilde{\mathcal{G}}$. Thus, taking ψ the standard character with $\iota(\psi(x)) = e(x/p)$, we get a sheaf $\tilde{\mathcal{G}}$ with associated irreducible trace function given by

$$K'(n) = -\frac{1}{\sqrt{p}} \sum_{x \in C(\mathbf{F}_p) - D(\mathbf{F}_p)} e\left(\frac{n\phi(x)}{p}\right), \qquad \text{for } 1 \leqslant n \leqslant p-1, \tag{10.2}$$

and

$$K'(p) = \frac{p - |C(\mathbf{F}_p) - D(\mathbf{F}_p)|}{\sqrt{p}}$$

(as before, this holds under the assumption that ϕ is supermorse).

By the Fourier inversion formula (in this context, this is [Kat90, Th. 7.3.8 (1)]), the Fourier transform sheaf $\mathrm{FT}_\psi(\tilde{\mathcal{G}})$ (note that we must use the same ψ as was used to construct $\mathcal{G}$) is

$$[x \mapsto -x]^*\tilde{\mathcal{F}} = [\times(-1)]^*\tilde{\mathcal{F}}$$

with trace function

$$(\operatorname{tr} [\times(-1)]^*\tilde{\mathcal{F}})(k, y) = \tilde{N}(\phi; -y).$$

We summarize this and estimate the conductors in a proposition.

Proposition 10.2 (Fiber counting functions and duals). *Let $C/\mathbf{Q}$ and ϕ be as above, with ϕ supermorse.*

(1) *For $p > \deg(\phi)$ such that there is "good reduction", the functions K and K' defined above are irreducible trace functions associated to the sheaves $\tilde{\mathcal{F}}$ and $\tilde{\mathcal{G}}$.*

Let $S \subset \bar{\mathbf{F}}_p$ be the set of critical values of ϕ modulo p.

(2) *The sheaf $\tilde{\mathcal{F}}$ is tame on $\mathbf{P}^1$, lisse on $\mathbf{A}^1 - S$, and has at most tame pseudo-reflection monodromy at all $s \in S$. It satisfies*

$$\operatorname{cond}(\tilde{\mathcal{F}}) \leqslant \deg(\phi) + |S|.$$

(3) *The sheaf* $\tilde{\mathcal{G}}$ *has rank* $|S|$*, it is lisse on* $\mathbf{G}_m$ *and tamely ramified at* 0*. At* ∞*, we have*

$$\mathrm{Swan}_\infty(\tilde{\mathcal{G}}) = \begin{cases} |S|-1 & \text{if } 0 \in S \\ |S| & \text{if } 0 \notin S, \end{cases}$$

and hence $\mathrm{cond}(\tilde{\mathcal{G}}) \leqslant 2|S|+2$*.*

Proof. We have already discussed (1). Then [Kat90, proof of Lemma 7.10.2.3] shows that $\tilde{\mathcal{F}}$ is tame everywhere, lisse on $\mathbf{A}^1 - S$, and has tame pseudo-reflection monodromy at all $s \in S$. This gives

$$\mathrm{cond}(\tilde{\mathcal{F}}) \leqslant \mathrm{rank}(\tilde{\mathcal{F}}) + |S| + 1 = \deg(\phi) + |S|.$$

For (3), since we know $\tilde{\mathcal{F}}$ is a tame pseudo-reflection sheaf, we can use [Kat90, Th. 7.9.4] to see that $\tilde{\mathcal{G}}$ has rank $|S|$ and is lisse on $\mathbf{G}_m$, and [Kat90, Cor. 7.4.5 (2)] to see that it is tamely ramified at 0. Still from [Kat90, Th. 7.9.4], we get the decomposition

$$\tilde{\mathcal{G}}(\infty) = \bigoplus_{s \in S} \mathcal{L}_{\psi(sY)}, \tag{10.3}$$

as a representation of the wild inertia group at ∞. Hence

$$\mathrm{Swan}_\infty(\tilde{\mathcal{G}}) = \begin{cases} |S|-1 & \text{if } 0 \in S \\ |S| & \text{if } 0 \notin S, \end{cases}$$

and then

$$\mathrm{cond}(\tilde{\mathcal{G}}) \leqslant |S| + 2 + \mathrm{Swan}_\infty(\tilde{\mathcal{G}}) \leqslant 2|S|+2. \qquad \square$$

To conclude this example, let us first recall that the condition of being supermorse is generic, in a fairly natural and obvious sense. For instance, if we consider $C = \mathbf{P}^1$ and look at the space L_{d_1,d_2} of all rational functions with coprime numerator and denominator of fixed degrees (d_1, d_2), the set of supermorse functions $\phi \in L_{d_1,d_2}$ will be Zariski-dense.

10.3 Hyper-Kloosterman sums. Let $m \geqslant 2$ and let p be a prime number. By results of Deligne (see [Kat88, 11.0]), for all $\ell \neq p$, and any non-trivial ℓ-adic additive character ψ, there exists a sheaf $\mathcal{K}\ell_m$ on $\mathbf{A}^1_{\mathbf{F}_p}$ such that

$$(\mathrm{tr}\,\mathcal{K}\ell_m)(k,a) = (-1)^{m-1}|k|^{-(m-1)/2} \sum_{\substack{x_1 \dots x_m = a \\ x_i \in k}} \cdots \sum \psi(x_1 + \cdots + x_m)$$

for all finite extensions $k/\mathbf{F}_p$ and all $a \in k^\times$. This sheaf is a Fourier sheaf, geometrically irreducible, of rank $m \geqslant 2$ and pointwise pure of weight 0, i.e., it is an irreducible trace sheaf.

Now fix a non-constant rational fraction, $\phi(T) = R(T)/S(T)$, $R(T), S(T) \in \mathbf{Z}[T]$. Assuming that p is large enough (greater that the degree of R, S and all their coefficients), the sheaf $\mathcal{K}\ell_{m,\phi} = \phi^*\mathcal{K}\ell_m$ satisfies

$$(\operatorname{tr} \mathcal{K}\ell_{m,\phi})(\mathbf{F}_p, a) = (-1)^{m-1} \operatorname{Kl}_m(\phi(a); p)$$

for $a \in \mathbf{F}_p - \phi^{-1}(\{0, \infty\})$. The following result is the main input to the proof of the second part of Corollary 2.2.

PROPOSITION 10.3. *If ϕ is non-constant, the sheaf $\mathcal{K}\ell_{m,\phi}$ above is geometrically irreducible and has conductor $\leqslant 2m + 1 + \deg(RS)$.*

Proof. Deligne has shown that $\mathcal{K}\ell_m$ has rank m, is lisse on $\mathbf{G}_m$, and is tame at 0 and totally wild at ∞ with Swan conductor 1, so that

$$\operatorname{cond}(\mathcal{K}\ell_m) = m + 3$$

(see, e.g., [Kat88, 11.0.2]).

It follows therefore that $\mathcal{K}\ell_{m,\phi}$ is of rank m, is lisse outside of the set $\phi^{-1}(\{0, \infty\})$, is tame at the zeros of ϕ and wild at its poles. At a pole $x \in \phi^{-1}(\infty)$ of order d_x, the map ϕ is generically étale, and hence we know that $\operatorname{Swan}_x(\phi^*\mathcal{K}\ell_m) = d_x \operatorname{Swan}_\infty(\mathcal{K}\ell_m) = d_x$ by [Kat88, 1.13.1]. Finally, Katz has shown that $\mathcal{K}\ell_m$ is geometrically Lie-irreducible (see [Kat88, Thm. 11.1]), i.e., that its restriction to any finite-index subgroup of the fundamental group of $\mathbf{G}_m$ is geometrically irreducible. Since ϕ is non-constant, this shows that $\mathcal{K}\ell_{m,\phi}$ is also irreducible.

11 Examples of Determination of $\mathbf{G}_{\mathcal{F}}$

Theorem 1.14 solves completely the question of showing that isotypic trace functions are good, reducing it to an estimation of the conductor of the associated sheaf. However we find it instructive to determine $\mathbf{G}_{\mathcal{F}}$ as precisely as possible for interesting families of functions, as was already done in Section 1.5 in simple cases. This gives illustrations of the various possibilities, and would be a first step in trying to improve the generic exponent 1/8. Since we won't need these results for this paper, we leave the proof to the reader as an exercise in the theory of the ℓ-adic Fourier transform (proximity with [Kat88, Kat90] is strongly advised).

11.1 Mixed characters.

Let

$$\mathcal{F} = \mathcal{L}_{\eta(\phi_2)} \otimes \mathcal{L}_{\psi(\phi_1)}$$

be a sheaf corresponding to mixed characters, where either ϕ_1 is not a polynomial of order $\leqslant 1$, or η is non-trivial of order $h \geqslant 2$ and ϕ_2 is not of the form $t\phi_3(X)^h$ for some $t \in \mathbf{F}_p^\times$, and $\phi_3 \in \mathbf{F}_p(X)$. Then one can show that $\mathbf{G}_{\mathcal{F}}$ is contained either in B (the stabilizer of ∞) or in $\mathrm{N}^{0,\infty}$ the normalizer of the diagonal torus. For $\mathcal{F} = \mathcal{L}_{\psi(X^{-1})}$, we have $\mathbf{G}_{\mathcal{F}} = 1$.

11.2 Symmetric powers of Kloosterman sums. Let $\mathcal{K}_2^{(1)} = \phi^*\mathcal{K}\ell_2$ be the pull-back of the Kloosterman sheaf $\mathcal{K}\ell_2$ of §10.3 (relative to some additive character ψ) by the map $x \mapsto x^2$, and for $d \geqslant 1$, let

$$\mathcal{K}_2^{(d)} = \mathrm{Sym}^d(\mathcal{K}^{(1)})$$

be the d-symmetric power of $\mathcal{K}^{(1)}$. The sheaf $\mathcal{K}^{(d)}$ is an irreducible trace sheaf of rank $d+1$ and one finds:

(1) If $d \geqslant 3$, then $\mathbf{G}_{\mathcal{K}^{(d)}} = 1$;
(2) If $d = 1$, then $\mathbf{G}_{\mathcal{K}^{(1)}}$ is the maximal torus in $\mathrm{PGL}_2(\bar{\mathbf{F}}_p)$ stabilizing the subset $\{-2, 2\}$;
(3) If $d = 2$, then $\mathbf{G}_{\mathcal{K}^{(2)}}$ is the subgroup of $\mathrm{PGL}_2(\bar{\mathbf{F}}_p)$ stabilizing the subset $\{0, \infty, -4, 4\}$, which is a dihedral group of order 8 (these four points have cross-ratios $\{-1, 1/2, 2\}$, and one sees that any element of PGL_2 stabilizing this set permutes the two pairs $\{0, \infty\}$ and $\{-4, 4\}$). In order to show that $\mathbf{G}_{\mathcal{K}^{(2)}}$ is not smaller than this dihedral group, one may use the results of Deligne and Flicker [DF13, Cor. 7.7] concerning tame local systems on $\mathbf{P}^1 - \{\text{four points}\}$.

11.3 Fiber-counting functions. Let C and ϕ be as in Example 10.2, with ϕ supermorse. Let $p > \deg(\phi)$ be a prime of good reduction, and let

$$\tilde{\mathcal{F}} = \ker(\phi_*\bar{\mathbf{Q}}_\ell \xrightarrow{\mathrm{tr}} \bar{\mathbf{Q}}_\ell)$$

be the irreducible trace sheaf corresponding to the trace function $K(x) = N_0(\phi; x) = N(\phi; x) - 1$.

If ϕ has degree $\geqslant 2$ and 0 is not the unique critical value of ϕ, then one finds that $\mathbf{G}_{\mathcal{F}}$ is a subgroup of diagonal matrices of order bounded by $\deg(\phi) - 1$.

Acknowledgments

This paper has benefited from the input of many people. We would like to thank V. Blomer, T. Browning, J. Ellenberg, C. Hall, H. Iwaniec, N. Katz, E. Lindenstrauss, P. Nelson, R. Pink, G. Ricotta, P. Sarnak, A. Venkatesh and D. Zywina for input and encouraging comments. We also thank B. Löffel and P. Nelson for their careful readings of the manuscript. We particularly thank G. Harcos, whose decisive comments on an earlier version of this paper have led to a significant improvement on the value of the exponents as well as the referee who read the paper with considerable attention, caught many slips and made many helpful comments on the penultimate version of this paper.

References

[Bea10] A. Beauville: Finite subgroups of $\mathrm{PGL}_2(K)$. *Contemporary Math. A.M.S* 522 (2010), 23–29

[BHM07] V. Blomer, G. Harcos and Ph. Michel. Bounds for modular L-functions in the level aspect. *Ann. Sci. École Norm. Sup. (4)* (5)40 (2007), 697–740.

[BH08] V. Blomer and G. Harcos. Hybrid bounds for twisted L- functions. *J. reine und angew. Mathematik* 621 (2008), 53–79.

[Byk98] V.A. Bykovski. A trace formula for the scalar product of Hecke series and its applications. *J. Math. Sciences* 89 (1998), 915–932.

[CI00] J.B. Conrey and H. Iwaniec. The cubic moment of central values of automorphic L-functions. *Ann. of Math. (2)* (3)151 (2000), 1175–1216.

[Del77] P. Deligne. *Cohomologie étale*, S.G.A $4\frac{1}{2}$, L.N.M 569, Springer, Verlag (1977).

[Del80] P. Deligne. La conjecture de Weil, II. *Publ. Math. IHÉS* 52 (1980), 137–252.

[DF13] P. Deligne and Y.Z. Flicker. Counting local systems with principal unipotent local monodromy. *Ann. of Math. (2)* (3)178 (2013), 921–982.

[DI82] J-M. Deshouillers and H. Iwaniec. Kloosterman sums and Fourier coefficients of cusp forms. *Invent. math.* (2)70 (1982/83), 219–288.

[DFI93] W.D. Duke, J. Friedlander and H. Iwaniec. Bounds for automorphic L-functions. *Invent. math.* 112 (1993), 1–8.

[DFI94] W.D. Duke, J. Friedlander and H. Iwaniec. Bounds for automorphic L-functions II. *Invent. math.* 115 (1994), 219–239.

[DFI02] W.D. Duke, J. Friedlander and H. Iwaniec. The subconvexity problem for Artin L-functions. *Invent. math.* (3)149 (2002), 489–577.

[EMS84] P.D.T.A Elliott, C.J. Moreno and F. Shahidi. On the absolute value of Ramanujan's τ-function. *Math. Ann.* 266 (1984), 507–511.

[EMOT55] A. Erdélyi, W. Magnus, F. Oberhettinger and F.G. Tricomi. *Higher transcendental functions*, Vol. II, McGraw Hill (1955).

[FKM13] É. Fouvry, E. Kowalski, Ph. Michel. An inverse theorem for Gowers norms of trace functions over $\mathbf{F}_p$. *Math. Proc. Cambridge Philos. Soc.* (2)155 (2013), 277–295.

[FKM14] É. Fouvry, E. Kowalski, Ph. Michel. Algebraic trace functions over the primes. *Duke Math. J.* (9)163 (2014), 1683–1736.

[FKM] É. Fouvry, E. Kowalski, Ph. Michel. *On the exponent of distribution of the ternary divisor function*, Mathematika (to appear). arXiv:1304.3199.

[FG14] É Fouvry and S. Ganguly. Orthogonality between the Möbius function, additive characters, and Fourier coefficients of cusp forms. *Compos. Math.* (5)150 (2014), 763–797.

[FI85] J. B. Friedlander and H. Iwaniec. Incomplete Kloosterman sums and a divisor problem, with an appendix by Bryan J. Birch and Enrico Bombieri. *Ann. of Math. (2)* (2)121 (1985), 319–350.

[GR94] I.S. Gradshteyn and I.M. Ryzhkik. *Tables of integrals, series and products.* 5th ed. (edited by A. Jeffrey). Academic Press (1994).

[Hea86] D. R. Heath-Brown. The divisor function $d_3(n)$ in arithmetic progressions. *Acta Arith.* (1)47 (1986), 29–56.

[Hea97] D. R. Heath-Brown. The density of rational points on cubic surfaces. *Acta Arith.* 79 (1997), 17–30.

[Iwa87] H. Iwaniec. Fourier coefficients of modular forms of half-integral weight. *Invent. math.* (2)87 (1987), 385–401.

[Iwa90] H. Iwaniec. Small eigenvalues of Laplacian for $\Gamma_0(N)$. *Acta Arith.* (1)56 (1990), 65–82.

[Iwa95] H. Iwaniec. *Introduction to the spectral theory of automorphic forms, Biblioteca de la Revista Matematica Iberoamericana*, Revista Matematica Iberoamericana, Madrid (1995).

[Iwa97] H. Iwaniec.Topics in classical automorphic forms. *Grad. Studies in Math. A.M.S* 17, (1997).

[IK04] H. Iwaniec and E. Kowalski. Analytic number theory. *A.M.S. Coll. Publ.* 53 (2004).

[Kat80] N.M. Katz. *Sommes exponentielles*, Astérisque 79, Soc. Math. France (1980).

[Kat88] N.M. Katz. *Gauss sums, Kloosterman sums and monodromy groups*, Annals of Math. Studies 116, Princeton Univ. Press (1988).

[Kat90] N.M. Katz. *Exponential sums and differential equations*, Annals of Math. Studies 124, Princeton Univ. Press (1990).

[KS03] H. Kim and P. Sarnak. Refined estimates towards the Ramanujan and Selberg conjectures. *J. American Math. Soc.* 16 (2003), 175–181.

[Kow14] E. Kowalski. An introduction to the representation theory of groups. *Grad. Studies in Math. A.M.S* 155 (2014).

[KRW07] E. Kowalski, O. Robert and J. Wu. Small gaps in coefficients of L-functions and $\mathfrak{B}$-free numbers in small intervals. *Rev. Mat. Iberoamericana* 23 (2007), 281–326.

[Lau87] G. Laumon. Transformation de Fourier, constantes d'équations fonctionnelles et conjecture de Weil. *Publ. Math. IHÉS* 65 (1987), 131–210.

[MV10] Ph. Michel and A. Venkatesh. The subconvexity problem for GL_2. *Publ. Math. I.H.É.S* 111 (2010), 171–271.

[Mot] Y. Motohashi. *On sums of Hecke-Maass eigenvalues squared over primes in short intervals*, preprint arXiv:1209.4140v1.

[Mun13] R. Munshi. Shifted convolution sums for $GL(3) \times GL(2)$. *Duke Math. J.* (13)162 (2013), 2345–2362.

[Pit95] N. Pitt. On shifted convolutions of $\zeta(s)^3$ with automorphic L-functions. *Duke Math. J.* (2)77 (1995), 383–406.

[RR05] D. Ramakrishnan and J. Rogawski. Average values of modular L-series via the relative trace formula, Special Issue: In memory of Armand Borel. Part 3. *Pure Appl. Math. Q.* (4)1 (2005), 701–735.

[Sar91] P. Sarnak. Diophantine problems and linear groups. In: *Proceedings of the I.C.M.* 1990, Kyoto, Springer (1991), 459–471.

[Ser71] J-P. Serre. *Représentations linéaires des groupes finis*, 2ème Édition, Hermann, (1971).

[Str04] A. Strömbergsson. On the uniform equidistribution of long closed horocycles. *Duke Math. J.* (3)123 (2004), 507–547.

[SU] P. Sarnak and A. Ubis. The horocycle flow at prime times. *Journal Math. Pures Appl.*, to appear.

[Ven10] A. Venkatesh. Sparse equidistribution problems, period bounds and subconvexity. *Ann. of Math. (2)* 172 (2010), 989–1094.

Étienne Fouvry, Laboratoire de Mathématique, Université Paris Sud, Campus d'Orsay, 91405 Orsay Cedex, France etienne.fouvry@math.u-psud.fr

Emmanuel Kowalski, ETH Zürich – D-MATH, Rämistrasse 101, CH-8092 Zürich, Switzerland kowalski@math.ethz.ch

Philippe Michel, EPFL Chaire TAN, Station 8, CH-1015 Lausanne, Switzerland philippe.michel@epfl.ch

Received: February 5, 2014
Revised: October 29, 2014
Accepted: November 16, 2014