ANNALES

DE

L'INSTITUT FOURIER

Étienne FOUVRY, Emmanuel KOWALSKI, Philippe MICHEL,
Chandra Sekhar RAJU, Joël RIVAT & Kannan SOUNDARARAJAN

On short sums of trace functions

Tome 67, nº 1 (2017), p. 423-449.

<http://aif.cedram.org/item?id=AIF_2017__67_1_423_0>

Ann. Inst. Fourier, Grenoble
67, 1 (2017) 423-449

ON SHORT SUMS OF TRACE FUNCTIONS

**by Étienne FOUVRY, Emmanuel KOWALSKI,
Philippe MICHEL, Chandra Sekhar RAJU,
Joël RIVAT & Kannan SOUNDARARAJAN (*)**

ABSTRACT. — We consider sums of oscillating functions on intervals in cyclic groups of size close to the square root of the size of the group. We first prove non-trivial estimates for intervals of length slightly larger than this square root (bridging the "Polyá-Vinogradov gap" in some sense) for bounded functions with bounded Fourier transforms. We then prove that the existence of non-trivial estimates for ranges slightly below the square-root bound is stable under the discrete Fourier transform. We then give applications related to trace functions over finite fields.

RÉSUMÉ. — Nous considérons des sommes de fonctions oscillantes sur des intervalles contenus dans un groupe fini cyclique, de taille proche de la racine carrée du cardinal du groupe. Nous démontrons tout d'abord des bornes non-triviales pour tout intervalle de longueur à peine plus grande que cette racine carrée (améliorant l'inégalité de Polyá-Vinogradov) pour les fonctions bornées dont la transformée de Fourier est bornée. Nous démontrons ensuite que l'existence d'une borne non-triviale pour un intervalle de taille un peu plus petite que la racine carrée est une propriété stable par transformation de Fourier. Nous donnons des applications liées aux fonctions trace sur les corps finis.

1. Introduction and statement of results

Consider a positive integer $m \geqslant 1$. Let $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ be a complex-valued function defined modulo m, which we also view as a function $\mathbb{Z} \longrightarrow$

Keywords: Short exponential sums, trace functions, van der Corput lemma, completion method, Riemann Hypothesis over finite fields.
Math. classification: 11L07, 11L05, 11T23.
(*) Ph. M. was partially supported by the SNF (grant 200021-137488); Ph. M. and E. K. were also partially supported by a DFG-SNF lead agency program grant (grant 200021L_153647); É. F. thanks ETH Zürich, EPF Lausanne and the Institut Universitaire de France for financial support. Ph. M. thanks Stanford University, ETH Zürich and Caltech for providing excellent working conditions. K. S. was partially supported by NSF grant DMS 1001068, and a Simons Investigator grant from the Simons Foundation. CS. R. was supported by B. C. and E. J. Eaves Stanford Graduate Fellowship. J. R. was supported by the ANR (grant ANR-10-BLAN 0103).

$\mathbb{C}$ by composing with the reduction modulo m. Let $I \subset \mathbb{Z}$ be an interval of cardinality $|I|$ at most equal to m. One of the most important general problems in analytic number theory is to estimate the partial sum

$$S(\varphi, I) := \sum_{n \in I} \varphi(n).$$

Of course, one has the obvious upper bound

$$|S(\varphi, I)| \leqslant \|\varphi\|_\infty |I|, \tag{1.1}$$

where

$$\|\varphi\|_\infty = \max_{n \in \mathbb{Z}/m\mathbb{Z}} |\varphi(n)|$$

but the goal is usually to improve significantly this bound when φ is an oscillating function. Both the *quality* of the improvement (i.e., the saving compared with the trivial bound for given I) and the *range* of possibilities for I that give rise to non-trivial bounds are important. We will mostly focus on this second aspect in this paper.

1.1. The Pólya–Vinogradov range

There exists a very general method to estimate incomplete sums, based on Fourier theory on $\mathbb{Z}/m\mathbb{Z}$. This is called the *Pólya–Vinogradov* or *completion* method.

For any function $\varphi : \mathbb{Z} \to \mathbb{C}$ which is m-periodic, we define its normalized Fourier transform $\widehat{\varphi} : \mathbb{Z} \to \mathbb{C}$ by

$$\widehat{\varphi}(h) = \frac{1}{\sqrt{m}} \sum_{x \,(\mathrm{mod}\, m)} \varphi(x) e\Big(\frac{hx}{m}\Big), \tag{1.2}$$

for all $h \in \mathbb{Z}$, where $e(t) := \exp(2\pi i t)$. We shall also find it convenient to use the notation $e_m(t)$ to denote $e(t/m) = e^{2\pi i t/m}$.

Given an interval $I \subset \mathbb{Z}$ with cardinality at most m, let $\tilde{I}$ be its image in $\mathbb{Z}/m\mathbb{Z}$, with characteristic function denoted by $\mathbf{1}_{\tilde{I}}$. The discrete Plancherel formula gives the identity

$$S(\varphi, I) = \sum_{h \,(\mathrm{mod}\, m)} \widehat{\varphi}(h) \overline{\widehat{\mathbf{1}}_{\tilde{I}}(h)},$$

so that

$$|S(\varphi, I)| \leqslant \|\widehat{\varphi}\|_\infty \sum_{h \,(\mathrm{mod}\, m)} \Big|\widehat{\mathbf{1}}_{\tilde{I}}(h)\Big| \leqslant \|\widehat{\varphi}\|_\infty m^{1/2} \log(3m) \tag{1.3}$$

since it is well known that

$$\sum_{h\,(\mathrm{mod}\,m)} \left|\widehat{\mathbf{1}}_{\tilde{I}}(h)\right| \leqslant m^{1/2}\log(3m)$$

for any $m \geqslant 1$ and any interval I.

Therefore if we assume that $\|\widehat{\varphi}\|_\infty \leqslant c$ for some constant c, the bound (1.3) will be non-trivial as long as

$$|I| \geqslant cm^{1/2}\log(3m) \tag{1.4}$$

which we call the *Pólya–Vinogradov range*.

The problem of estimating non-trivially sums over shorter intervals is crucial for many applications, for instance to study averages or subconvexity estimates of L-functions [5, 2] (see also [21] for a recent very different situation where this range determines the solution of a natural problem). Here we study this problem, starting with a general result which gives a modest improvement over the Pólya–Vinogradov range (1.4).

Theorem 1.1. — *For any interval I in $\mathbb{Z}$ with $\sqrt{m} < |I| \leqslant m$, we have*

$$\Big|\sum_{n\in I}\varphi(n)\Big| \leqslant c\sqrt{m}\log\Big(\frac{4e^8|I|}{m^{1/2}}\Big) \tag{1.5}$$

where $c = \max(\|\varphi\|_\infty, \|\widehat{\varphi}\|_\infty)$.

The estimate (1.5) is non-trivial as soon as I is of length $\gg \sqrt{m}$, and we may view this result as "bridging the Pólya–Vinogradov gap". As we will see in Section 2, the proof is very simple, but such results do not seem to have been noticed before. While we have given an explicit bound in Theorem 1.1, we have not made any attempt to optimize constants, and a more careful smoothing argument (for example, using the Beurling–Selberg trigonometric polynomials as in [14]) would provide better explicit constants.

Before continuing, we note that Theorem 1.1 is essentially best possible, since for $\varphi(n) = e(n^2/m)$ the sum over $1 \leqslant n \leqslant m^{1/2}$ is $\gg m^{1/2}$. Hence any improvement beyond Theorem 1.1 requires some input on the function φ.

1.2. Beyond the Pólya–Vinogradov range

Our next result is concerned with the problem of going significantly below the range $|I| \geqslant \sqrt{m}$ for suitable functions φ. There are only few results of this type already known, the most famous being the Burgess bound, when $\varphi(n) = \chi(n)$ is a primitive Dirichlet character modulo m.

We are currently unable to obtain results in great generality, but we will obtain a number of new cases by proving a general principle that, roughly speaking, states that if the partial sums of a function φ has substantial cancellation near the Pólya–Vinogradov range, then so does its discrete Fourier transform. We now formulate this principle precisely, giving in the next section several applications.

Suppose throughout that $\varphi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{C}$ is a periodic function with

$$c = \max(\|\varphi\|_\infty, \|\widehat{\varphi}\|_\infty).$$

For any $N \geqslant 1$, we define the sum $S(\varphi, N)$ by the formula

$$S(\varphi, N) = \sum_{1 \leqslant n \leqslant N} \varphi(n),$$

and if $N \leqslant -1$, then we put

$$S(\varphi, N) = \sum_{N \leqslant n \leqslant -1} \varphi(n).$$

Next define, for any $1 \leqslant N \leqslant m/2$,

$$\Delta(\varphi, N) = \frac{1}{\sqrt{m}} + \max_{m/2 \geqslant t \geqslant 1} \Big\{ \min\Big(\frac{1}{ct}, \frac{1}{cN}\Big) \Big(|S(\varphi, t)| + |S(\varphi, -t)|\Big) \Big\}. \tag{1.6}$$

From the definition, it is clear that $\Delta(\varphi, N)$ is a non-increasing function of N, and also that $N\Delta(\varphi, N)$ is a non-decreasing function of N. Further, the definition immediately gives

$$\max_{t \leqslant N} \Big(|S(\varphi, t)| + |S(\varphi, -t)|\Big) \leqslant cN\Delta(\varphi, N), \tag{1.7}$$

and

$$\max_{m/2 \geqslant t \geqslant N} \frac{1}{t} \Big(|S(\varphi, t)| + |S(\varphi, -t)|\Big) \leqslant c\Delta(\varphi, N). \tag{1.8}$$

With this notation, our main theorem transfers bounds for $\Delta(\varphi, m/N)$ into bounds for $\Delta(\widehat{\varphi}, N)$.

Theorem 1.2. — *Let m, φ, c and Δ be as above. For $2 \leqslant N \leqslant m/2$ we have*

$$|S(\widehat{\varphi}, N)| + |S(\widehat{\varphi}, -N)| \ll c\sqrt{N} m^{\frac{1}{4}} \Delta\Big(\varphi, \frac{m}{N}\Big)^{\frac{1}{2}}, \tag{1.9}$$

and

$$\Delta(\widehat{\varphi}, N) \ll \frac{m^{\frac{1}{4}}}{\sqrt{N}} \Delta\Big(\varphi, \frac{m}{N}\Big)^{\frac{1}{2}}.$$

In particular

$$\Delta(\widehat{\varphi}, \sqrt{m}) \ll \Delta(\varphi, \sqrt{m})^{\frac{1}{2}}. \tag{1.10}$$

If we apply the bound of (1.10) twice, we see that we obtain $\Delta(\widehat{\varphi}, \sqrt{m}) \ll \Delta(\varphi, \sqrt{m})^{\frac{1}{2}} \ll \Delta(\widehat{\varphi}, \sqrt{m})^{\frac{1}{4}}$, so that some loss in precision has occurred. One may wonder if this loss in precision could be removed, perhaps by defining some other quantity rather than Δ.

1.3. Applications

Our methods apply best to functions modulo m that are pointwise small and whose Fourier transform is also small, in a precise quantitative sense. In analytic number theory, there is a plentiful supply of such functions which arise naturally in applications: they are given by *Frobenius trace functions* modulo m.

These functions originate in algebraic geometry, and their analytic properties have been investigated systematically in recent years by Fouvry, Kowalski and Michel especially (see [8, 9, 10, 11, 12] for instance). We will recall briefly the definition in Section 2.2, referring to [13] for a longer survey.

Basic examples of trace functions lead to the following application of Theorem 1.1, where we denote as usual by $\bar{x}$ the inverse of x modulo p for $x \in \mathbb{F}_p^\times$.

Corollary 1.3 (Equidistribution over short intervals). — *Let β be any function defined on positive integers such that $1 \leqslant \beta(p) \to +\infty$ as $p \to +\infty$, and for all p prime, let I_p be an interval in $\mathbb{F}_p$ of cardinality $|I_p| \geqslant p^{1/2}\beta(p)$.*

(1) *Let f_1, $f_2 \in \mathbb{Z}[X]$ be monic polynomials such that $f = f_1/f_2 \in \mathbb{Q}(X)$ is not a polynomial of degree $\leqslant 1$. Then for p prime, the set of fractional parts*

$$\left\{ \frac{f(n)}{p} \right\}, \quad n \in I_p,$$

becomes equidistributed in $[0,1]$ with respect to Lebesgue measure as $p \to +\infty$, where $f(n) = f_1(n)\overline{f_2(n)}$ is computed in $\mathbb{F}_p$ and defined to be 0 if $n \pmod p$ is a pole of f.

(2) *For p prime and $n \in \mathbb{F}_p$ (resp. $n \in \mathbb{F}_p^\times$), define the Birch (resp. Kloosterman) angles $\theta_{3,p}(n)$ (resp. $\theta_{-1,p}(n)$) in $[0,\pi]$ by the relations*

$$\mathrm{B}_3(n) = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} e_p(x^3 + nx) = 2\cos\theta_{3,p}(n),$$

$$\frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p^\times} e_p(\bar{x} + nx) = 2\cos\theta_{-1,p}(n).$$

Then the angles $\{\theta_{3,p}(n),\ n \in I_p\}$, $\{\theta_{-1,p}(n),\ n \in I_p - \{0\}\}$ become equidistributed in $[0,\pi]$ with respect to the Sato–Tate measure $2\pi^{-1}\sin^2\theta d\theta$ as $p \to +\infty$.

Remark 1.4. — We use the terminology "Birch angles" as analogous to Kloosterman angles. Historically, Birch [1, §3] mentioned the problem of the distribution of these angles as a problem similar to the Sato–Tate distribution of the number of points on elliptic curves over finite fields. This Sato–Tate equidistribution was subsequently first proved by Livné [22].

See Section 2.2 for the proofs, which are direct applications of the Weyl criterion and the estimate (1.5). These statements can be generalized considerably to other summands, as will be clear from the proof in Section 2.2; there are also variants for geometric progressions instead of intervals, which are discussed in Section 2.3.

Below the Pólya–Vinogradov range, we obtain:

Corollary 1.5. — *Let p be a prime number, let $P(X) \in \mathbb{F}_p[X]$ be a non-zero polynomial and let $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ be a multiplicative character. Assume that either χ is non-trivial or that $\deg P \geqslant 3$. Let*

$$\varphi(x) = \chi(x) e_p(P(x)) \tag{1.11}$$

and

$$\widehat{\varphi}(n) = \frac{1}{\sqrt{p}} \sum_{x \pmod p} \chi(x) e_p(P(x) + nx).$$

There exists $\delta > 0$, depending only on $\deg P$, such that for any interval $I \subset \mathbb{R}$ with $|I| \geqslant p^{\frac{1}{2}-\delta}$ we have

$$\Big|\sum_{n \in I} \widehat{\varphi}(n)\Big| \ll |I|^{1-\delta}$$

where the implied constant depends only on $\deg(P)$.

The basic input here is the work of Weyl, Burgess, Enflo, Heath-Brown, Chang and Heath-Brown–Pierce on short sums with summands of the type $\chi(x)e(P(x)/p)$.

Corollary 1.5 has partial consequences to the distribution properties of the cubic Birch sums in shorter intervals than is allowed in Corollary 1.3:

Corollary 1.6. — *Let p be a prime number and let $\mathrm{B}_3(n)$, the cubic Birch sum, be as in Corollary 1.3.*

There exists $\delta > 0$, such that for any interval $I \subset \mathbb{R}$ with $|I| \geqslant p^{\frac{1}{2}-\delta}$ we have

$$\sum_{n\in I} \mathrm{B}_3(n) \ll |I|^{1-\delta} \tag{1.12}$$

and

$$\sum_{n\in I} |\mathrm{B}_3(n)|^2 = |I| + O(|I|^{1-\delta}) \tag{1.13}$$

where the implied constants are absolute. Further, for such intervals I, and any $0 \leqslant t < \frac{1}{2}$ we have

$$\min\Big(\sum_{\substack{n\in I\\ \mathrm{B}_3(n)>t}} 1, \sum_{\substack{n\in I\\ \mathrm{B}_3(n)<-t}} 1\Big) \geqslant \Big(\frac{1-2t}{4(2-t)} + o(1)\Big)|I|,$$

and for any $0 \leqslant t < 1$ we have

$$\sum_{\substack{n\in I\\ |\mathrm{B}_3(n)|>t}} 1 \geqslant \Big(\frac{1-t^2}{4-t^2} + o(1)\Big)|I|.$$

Using delicate work of Bourgain and Garaev on Kloosterman fractions [4], [3], we obtain corresponding, but weaker, results for short sums of Kloosterman sums:

Corollary 1.7. — *Let p be a prime number. For $k \geqslant 1$ an integer and $(a,p) = 1$ some parameter, let*

$$\varphi(x) = e_p(ax^{-k})$$

for $x \in \mathbb{F}_p^\times$ and $\varphi(0) = 0$. Let

$$\widehat{\varphi}(n) = \frac{1}{\sqrt{p}} \sum_{x\in\mathbb{F}_p^\times} e_p(ax^{-k} + nx)$$

be its Fourier transform.

For $k=1$ and $k=2$, there exists $\delta>0$ such that for all $x\geqslant\sqrt{p}(\log p)^{-\delta}$ we have

$$\Big|\sum_{1\leqslant n\leqslant x}\widehat{\varphi}(n)\Big|\ll x(\log x)^{-\delta},$$

where the implied constant is absolute.

All these applications of Theorem 1.2 are found in Section 3.2.

Acknowledgments.

We thank the referee for carefully reading of the text, and especially for pointing out a slip in the proof of Theorem 3.2 in the first version of this paper.

2. Bridging the Pólya–Vinogradov gap

2.1. The basic inequality: Proof of Theorem 1.1

We may assume that $m\geqslant 64$ since otherwise the trivial bound cm is better than the claim. In that case we have $\lceil\sqrt{m}\rceil\leqslant m/4$.

For any $r\geqslant 0$, we denote by $I_r=r+I$ the interval I shifted by r, and by $\widehat{I_r}$ the Fourier transform of its characteristic function:

$$\widehat{I_r}(t)=\frac{1}{\sqrt{m}}\sum_{x\in I_r}e_m(tx).$$

By the discrete Plancherel formula, we have

$$S(\varphi,I_r)=\sum_{t\in\mathbb{Z}/m\mathbb{Z}}\widehat{\varphi}(t)\overline{\widehat{I_r}(t)}=\sum_{t\in\mathbb{Z}/m\mathbb{Z}}\widehat{\varphi}(t)\overline{\widehat{I}(t)}e_m(-rt)$$

for any r, where $\widehat{I}=\widehat{I_0}$. Moreover, we have

$$|S(\varphi,I_r)-S(\varphi,I)|\leqslant 2cr$$

since $|\varphi(x)|\leqslant c$ for all x.

Let $R=\lceil\sqrt{m}\rceil$. Since $\sqrt{m}<|I|$, we see that R is an integer with $\sqrt{m}\leqslant R\leqslant|I|$. Thus,

$$|I|\geqslant R\geqslant\sqrt{m}\geqslant m/|I|\geqslant 1,\qquad m\geqslant 4R$$

(the last inequality because $m \geqslant 64$, as assumed at the beginning of the proof). Summing our identity for $S(\varphi, I_r)$ for $1 \leqslant r \leqslant R$, we obtain

$$RS(\varphi, I) = \sum_{-m/2<t\leqslant m/2} \widehat{\varphi}(t)\overline{\widehat{I}(t)} \sum_{1\leqslant r\leqslant R} e_m(-rt) + E, \tag{2.1}$$

where $|E| \leqslant 2cR^2$.

Now, the Fourier transform $\widehat{I}$ satisfies

$$|\widehat{I}(t)| \leqslant \frac{1}{\sqrt{m}} \min\Big(|I|, \frac{m}{2|t|}\Big)$$

for $-m/2 \leqslant t \leqslant m/2$, and similarly, we have

$$\Big|\sum_{1\leqslant r\leqslant R} e_m(-rt)\Big| \leqslant \min\Big(R, \frac{m}{2|t|}\Big).$$

Using these bounds in (2.1), together with $R \leqslant |I|$ and $|\widehat{\varphi}(t)| \leqslant c$, we get

$$\begin{aligned} R|S(\varphi, I)| \leqslant c\Big\{ \sum_{|t|\leqslant m/(2|I|)} R\frac{|I|}{m^{1/2}} &+ \sum_{m/(2|I|)<|t|\leqslant m/(2R)} R\frac{m^{1/2}}{2|t|} \\ &+ \sum_{m/(2R)<|t|\leqslant m/2} \frac{m^{3/2}}{4t^2}\Big\} + 2cR^2. \end{aligned}$$

The first sum above is at most

$$\frac{R|I|}{\sqrt{m}}\Big(\frac{m}{|I|} + 1\Big) \leqslant 2R\sqrt{m}.$$

Since $m \geqslant 4R$, the third term is at most

$$\frac{m^{3/2}}{2} \sum_{t>m/(2R)} \frac{1}{t^2} \leqslant \frac{m^{3/2}}{2} \frac{1}{m/(2R) - 1} = \frac{m^{3/2}R}{m - 2R} \leqslant 2R\sqrt{m}.$$

We claim that the middle term is

$$R\sqrt{m} \sum_{m/(2|I|)<t\leqslant m/(2R)} \frac{1}{t} \leqslant R\sqrt{m} \log\Big(\frac{4|I|}{\sqrt{m}}\Big), \tag{2.2}$$

from which it follows that

$$|S(\varphi, I)| \leqslant 4c\sqrt{m} + 2cR + c\sqrt{m}\log\Big(\frac{4|I|}{\sqrt{m}}\Big) \leqslant c\sqrt{m}\log\Big(\frac{4|I|}{\sqrt{m}}\Big) + 8c\sqrt{m},$$

as desired.

To verify the claim (2.2), note that if $|I| < m/4$ then the quantity in question is

$$\leqslant R\sqrt{m}\log\Big(\frac{m/(2R)}{m/(2|I|) - 1}\Big) \leqslant R\sqrt{m}\log\Big(\frac{m/(2R)}{m/(4|I|)}\Big),$$

which verifies (2.2) in this range. If $m/4 \leqslant |I| < m/2$, then we may use the bound

$$R\sqrt{m}\sum_{1<t\leqslant m/(2R)}\frac{1}{t}\leqslant R\sqrt{m}\log\Big(\frac{m}{2R}\Big)\leqslant R\sqrt{m}\log\Big(\frac{4|I|}{\sqrt{m}}\Big),$$

which again verifies (2.2). Finally, if $|I| \geqslant m/2$, then

$$R\sqrt{m}\sum_{t\leqslant m/(2R)}\frac{1}{t}\leqslant R\sqrt{m}\Big(1+\log\Big(\frac{m}{2R}\Big)\Big)\leqslant R\sqrt{m}\log\Big(\frac{4|I|}{\sqrt{m}}\Big),$$

which completes our verification of (2.2).

2.2. Applications to trace functions, I: the additive case

We now recall the definition and give some basic examples of trace functions before proving Corollary 1.3. As is usual, we will restrict our attention to prime moduli; the extension of the results to squarefree moduli at least is a matter of applying the Chinese Remainder Theorem.

Thus let p be a prime number. Given a prime $\ell \neq p$, we fix an isomorphism $\iota : \bar{\mathbb{Q}}_\ell \simeq \mathbb{C}$, and we use it implicitly to identify any ℓ-adic number with a complex number. A *Fourier sheaf* modulo p is defined to be a middle-extension $\bar{\mathbb{Q}}_\ell$-adic sheaf $\mathcal{F}$ on $\mathbf{A}^1_{\mathbb{F}_p}$, that is pointwise pure of weight 0 and of Fourier type, i.e., none of its geometric Jordan–Hölder components is isomorphic to an Artin–Schreier sheaf $\mathcal{L}_\psi$ for some additive character ψ.

Remark 2.1. — Note that in contrast with the definition of Katz [18], we impose the weight 0 condition instead of stating it separately.

The *(Frobenius) trace function* of $\mathcal{F}$ is the function $\mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{C}$ defined by

$$\varphi(x) = \iota(\mathrm{tr}(\mathrm{Fr}_{x,\mathbb{F}_p} \,|\mathcal{F})) \tag{2.3}$$

for any $x \in \mathbb{F}_p$. It is a deep property, due to Deligne, that the Fourier transform of the trace function of $\mathcal{F}$ is also a trace function, namely that of the sheaf-theoretic (normalized) Fourier transform of $\mathcal{F}$.

The complexity of the trace function is controlled by the (analytic) conductor of the sheaf $\mathcal{F}$, which is defined as

$$\mathbf{c}(\mathcal{F}) = \mathrm{rank}(\mathcal{F}) + n(\mathcal{F}) + \sum_{x\in S(\mathcal{F})}\mathrm{Swan}_x(\mathcal{F}),$$

where rank$(\mathcal{F})$ is the rank of $\mathcal{F}$, $S(\mathcal{F}) \subset \mathbf{P}^1(\bar{\mathbb{F}}_p)$ is the set of singularities of $\mathcal{F}$, the integer $n(\mathcal{F}) \geqslant 0$ is the cardinality of $S(\mathcal{F})$ and Swan_x denotes the Swan conductor at such a singularity. The conductor is a non-negative integer, and from its properties (see [11, Prop. 8.2] for (2.5)) we have the following inequalities

$$\|\varphi\|_\infty \leqslant \mathrm{rank}(\mathcal{F}) \leqslant \mathbf{c}(\mathcal{F}) \tag{2.4}$$

and

$$\mathbf{c}(\widehat{\mathcal{F}}) \leqslant 10\,\mathbf{c}(\mathcal{F})^2. \tag{2.5}$$

Thus we obtain

$$\max(\|\varphi\|_\infty, \|\widehat{\varphi}\|_\infty) \leqslant 10\,\mathbf{c}(\mathcal{F})^2. \tag{2.6}$$

This means that, for instance, Theorem 1.1 or Theorem 1.2 can be applied efficiently to a sequence of trace functions modulo primes $p \to +\infty$, provided the conductor of the underlying sheaves is bounded independently of p.

Example 2.2. — Let f_1, $f_2 \neq 0$, g_1, $g_2 \neq 0$ be monic polynomials with integer coefficients such that f_1 is coprime to f_2 and g_1 is coprime to g_2. Let p be a prime number and χ a multiplicative character modulo p. If χ is trivial, we adopt the convention that $f_1 = f_2 = 1$. If χ is non-trivial, we assume that none of the zeros or poles of f_1/f_2 has order divisible by the order of χ. Define the rational functions $f = f_1/f_2$ and $g = g_1/g_2$, and let

$$\varphi(n) = \chi\big(f(n)\big)e_p\big(g(n)\big)$$

for $n \in \mathbb{Z}$ such that

$$f_1(n)f_2(n)g_2(n) \neq 0 \pmod p,$$

where $f(n) = f_1(n)\overline{f_2(n)}$ and $g(n) = g_1(n)\overline{g_2(n)}$ are computed in $\mathbb{F}_p$, and let

$$\varphi(n) = 0$$

if $f_1(n)f_2(n)g_2(n) = 0 \pmod p$.

For all primes p large enough, the poles of g are of order $< p$. For any such prime, the function φ is the trace function of a middle-extension sheaf $\mathcal{F}$ with

$$\mathbf{c}(\mathcal{F}) \ll \deg(f_1) + \deg(f_2) + \deg(g_1) + \deg(g_2),$$

where the implied constant is absolute. If f is not constant modulo p or if g is not a polynomial of degree at most 1, this sheaf is a Fourier sheaf.

Proof of Corollary 1.3.

(1). — We can certainly assume that $\beta(p) < p^{1/2}$ for all p. By the Weyl criterion, we must show that, for any fixed integer $h \neq 0$, and for the interval I_p, the sums

$$\frac{1}{|I_p|}\sum_{n\in I_p} e_p\big(hf(n)\big)$$

tend to 0 as $p \to +\infty$. For a given p, and a suitable ℓ-adic non-trivial additive character ψ of $\mathbb{F}_p$, there exists a rank 1 sheaf $\mathcal{F} = \mathcal{L}_{\psi(hf(X))}$ with trace function given by

$$\varphi(x) = e_p(hf(x))$$

for all $x \in \mathbb{F}_p$. This is a middle-extension sheaf modulo p, which is pointwise pure of weight 0. For p large enough so that $hf(X)$ is not a polynomial of degree $\leqslant 1$, this sheaf is a Fourier sheaf. Its conductor satisfies

$$\mathbf{c}(\mathcal{F}) \leqslant 1 + (1+\deg(f_2)) + \sum_{x \text{ pole of } f_2} \mathrm{ord}_x(f_2) + \deg(f_1) \ll 1$$

for all p large enough (the first 1 is the rank, the singularities are at most at poles of f_2 and at ∞, the Swan conductor at a pole of f_2 is at most the order of the pole, and at infinity it is at most the order of the pole of f at infinity, which is at most the degree of f_1). Hence, there exists $c \geqslant 1$ such that the trace function φ satisfies

$$\max(\|\varphi\|_\infty, \|\widehat{\varphi}\|_\infty) \leqslant c$$

for all large p. By Theorem 1.1, we get

$$\frac{1}{|I_p|}\sum_{n\in I_p} e_p(hf(n)) = \frac{1}{|I_p|} S(\varphi, I_p) \ll \frac{\sqrt{p}}{|I_p|}\log\Big(\frac{|I_p|}{p^{1/2}}\Big) \ll \frac{\log\beta(p)}{\beta(p)} \to 0$$

by assumption.

(2). — Let $\theta_p = \theta_{-1,p}$ or $\theta_{3,p}$, depending on whether one considers Kloosterman sums or Birch sums. Using the Weyl criterion, and keeping some notation from (1), it is enough to show that for any fixed $d \geqslant 1$, we have

$$\lim_{p\to+\infty} \frac{1}{|I_p|}\sum_{n\in I_p} U_d(2\cos\theta_p(n)) = 0$$

where $U_d \in \mathbb{Z}[X]$ is the Chebyshev polynomial defined by

$$U_d(2\cos\theta) = \sin((d+1)\theta)/\sin\theta.$$

By the theory of the Fourier transform of sheaves (see the exposition in [18, Ch. 8] and the survey in [11, §10.3]), the function

$$\varphi(x) = U_d(2\cos\theta_p(x))$$

is the trace function of an ℓ-adic irreducible middle-extension Fourier sheaf (the symmetric d-th power of the rank 2 Kloosterman sheaf or of the Fourier transform of the sheaf $\mathcal{L}_{\psi(x^3)}$, which is also of rank 2, both of which are irreducible); this sheaf has rank $d+1 \geqslant 2$ on the affine line over $\mathbb{F}_p$, and its conductor is bounded by a constant depending only on d, and not on p. It is therefore a Fourier sheaf with trace function satisfying

$$\max(\|\varphi\|_\infty, \|\widehat{\varphi}\|_\infty) \leqslant c$$

for some c depending only on d, and hence the desired limit holds again by a direct application of Theorem 1.1. □

Another interesting and somewhat similar application is the following:

Proposition 2.3 (Polynomial residues). — *Let β be a function defined on integers such that $1 \leqslant \beta(m) \to +\infty$ as $m \to +\infty$. Let $f \in \mathbb{Z}[X]$ be a non-constant monic polynomial. For all primes p large enough, depending on f and β, and for any interval I_p modulo p of size $|I_p| \geqslant p^{1/2}\beta(p)$, there exists $x \in I_p$ such that $x = f(y)$ for some $y \in \mathbb{F}_p$. In fact, denoting by P the set $f(\mathbb{F}_p)$ of values of f, the number of such x is $\sim \delta_f |I_p|$ as $p \to +\infty$, where $\delta_f = |P|/p$.*

Here again, the interest of the result is when $\beta(m)$ is smaller than $\log m$. However, it seems likely that this distribution property should also be true for much shorter intervals (as in the well-known conjecture for quadratic (non)-residues).

Proof. — Let φ be the characteristic function of the set P of values $f(y)$ for $y \in \mathbb{F}_p$. We must show that, for p large enough, we have

$$\sum_{x \in I_p} \varphi(x) \sim \delta_f |I_p|$$

(which in particular implies that the left-hand side is > 0 for p large enough.)

By [10, Prop. 6.7], if p is larger than $\deg(f)$, there exists a decomposition

$$\varphi(x) = \sum_i c_i \varphi_i(x)$$

where the number of terms in the sum and the c_i are bounded in terms of $\deg(f)$ only, and where φ_i is the trace function of a *tame* ℓ-adic middle-extension sheaf $\mathcal{F}_i$ with conductor bounded in terms of $\deg(f)$ only. Moreover, $\mathcal{F}_1$ is the trivial sheaf with trace function equal to 1, all others are geometrically non-trivial and geometrically isotypic, and

$$c_1 = \delta_f + O(p^{-1/2}),$$

where $\delta_f = |P|/p$ and the implied constant depends only on $\deg(f)$. In particular, $\mathcal{F}_i$, being tame and geometrically isotypic and non-trivial, is a Fourier sheaf for $i \neq 1$. We also note that $\delta_f \gg 1$ for primes $p > \deg(f)$.

This decomposition implies

$$\sum_{x\in I_p} \varphi(x) = c_1|I_p| + \sum_{i\neq 1} c_i S(\varphi_i, I_p) = \delta_f|I_p| + \sum_{i\neq 1} c_i S(\varphi_i, I_p) + O(p^{-1/2}|I_p|).$$

Since the $\mathcal{F}_i$, for $i \neq 1$, are Fourier sheaves, we get by Theorem 1.1

$$S(\varphi_i, I_p) \ll \sqrt{p}\log\Big(\frac{|I_p|}{p^{1/2}}\Big) \ll |I_p|\frac{\log\beta(p)}{\beta(p)},$$

for each $i \neq 1$, where the implied constant depends only on $\deg(f)$. Hence we obtain

$$\sum_{x\in I_p} \varphi(x) \sim \delta_f|I_p|$$

uniformly for $p > \deg(f)$, since $\beta(p) \to +\infty$, which gives the result. □

2.3. Applications to trace functions, II: the multiplicative case

We consider now a different application of the basic inequality: for a prime p, we look at the values of trace functions modulo p on the multiplicative group $A = \mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. Fixing a generator g of A, this means that we are now looking at sums over *geometric progressions* xg^n for n in some interval I in $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/(p-1)\mathbb{Z}$. Such sums have also been considered by Korobov, for instance (see, e.g. [20, Ch. 1, §7]).

We will use the notation and terminology of the previous section, but to avoid confusion we write $\tau_{\mathcal{F}}$ for the restriction of the trace function of a sheaf $\mathcal{F}$ to $\mathbb{F}_p^\times$. The discrete Fourier transform becomes the discrete Mellin transform

$$\widehat{\tau}_{\mathcal{F}}(\chi) = \frac{1}{\sqrt{p-1}} \sum_{x\in\mathbb{F}_p^\times} \tau_{\mathcal{F}}(x)\chi(x)$$

defined for χ in the group of multiplicative characters of $\mathbb{F}_p^\times$. (More precisely, this Mellin transform can be identified with the discrete Fourier transform on $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$; as we are interested in bounds for the maximum of the Fourier transform, we may as well use the multiplicative characters as arguments).

The analogue of Fourier sheaves in this case are the sheaves with "property $\mathcal{P}$" of Katz's work on the discrete Mellin transform [19, Ch. 1].

Proposition 2.4. — *Let p be a prime number, and let $\mathcal{F}$ be an ℓ-adic middle extension sheaf modulo p with conductor c, pointwise pure of weight 0. If no geometric Jordan–Hölder component of $\mathcal{F}$ is isomorphic to a Kummer sheaf $\mathcal{L}_\chi$ associated to a multiplicative character χ, then the Mellin transform of the trace function $\tau_{\mathcal{F}}$ is bounded by $2\sqrt{2}c^2$, i.e., for any character χ of $\mathbb{F}_p^\times$, we have*

$$\Big|\frac{1}{\sqrt{p-1}}\sum_{x\in\mathbb{F}_p^\times}\tau_{\mathcal{F}}(x)\chi(x)\Big| \leqslant 2\sqrt{2}c^2.$$

Proof. — This is again a form of the Riemann Hypothesis of Deligne. By the Grothendieck–Lefschetz trace formula, and the assumption on $\mathcal{F}$ which ensures the vanishing of H_c^2, we have

$$\sum_{x\in\mathbb{F}_p^\times}\tau_{\mathcal{F}}(x)\chi(x) = -\mathrm{Tr}(\mathrm{Frob}_{\mathbb{F}_p} \mid H_c^1(\mathbb{G}_m\times\bar{\mathbb{F}}_p,\mathcal{F}\otimes\mathcal{L}_\chi)).$$

Then, since the sheaf involved is pointwise mixed of weight 0 on $\mathbb{G}_m$, Deligne's Theorem implies that each eigenvalue of the Frobenius acting on $H_c^1(\mathbb{G}_m\times\bar{\mathbb{F}}_p,\mathcal{F}\otimes\mathcal{L}_\chi)$ has modulus at most $\sqrt{p}$. Thus

$$\Big|\sum_{x\in\mathbb{F}_p^\times}\tau_{\mathcal{F}}(x)\chi(x)\Big| \leqslant (\dim H_c^1(\mathbb{G}_m\times\bar{\mathbb{F}}_p,\mathcal{F}\otimes\mathcal{L}_\chi))\sqrt{p}.$$

Let $U\subset\mathbb{G}_m$ be the maximal dense open subset where $\mathcal{F}$ is lisse. By the Euler–Poincaré characteristic formula, we have

$$\begin{aligned}\dim H_c^1(\mathbb{G}_m\times\bar{\mathbb{F}}_p,\mathcal{F}\otimes\mathcal{L}_\chi) &= -\chi_c(\mathbb{G}_m\times\bar{\mathbb{F}}_p,\mathcal{F}\otimes\mathcal{L}_\chi)\\ &= \mathrm{Swan}_0(\mathcal{F}\otimes\mathcal{L}_\chi)+\mathrm{Swan}_\infty(\mathcal{F}\otimes\mathcal{L}_\chi)+\sum_{x\in(\mathbb{G}_m-U)}(\mathrm{drop}_x(\mathcal{F}\otimes\mathcal{L}_\chi)\\ &\qquad +\mathrm{Swan}_x(\mathcal{F}\otimes\mathcal{L}_\chi))\end{aligned}$$

(see, e.g. [19, p. 67]). Since $\mathcal{L}_\chi$ is tame of rank 1, we have $\mathrm{Swan}_x(\mathcal{F}\otimes\mathcal{L}_\chi) = \mathrm{Swan}_x(\mathcal{F})$ for all x, and therefore

$$\mathrm{Swan}_0(\mathcal{F}\otimes\mathcal{L}_\chi)+\mathrm{Swan}_\infty(\mathcal{F}\otimes\mathcal{L}_\chi)+\sum_{x\in(\mathbb{G}_m-U)}\mathrm{Swan}_x(\mathcal{F}\otimes\mathcal{L}_\chi)\leqslant\mathbf{c}(\mathcal{F}) = c.$$

Furthermore, we have $\mathrm{drop}_x(\mathcal{F}\otimes\mathcal{L}_\chi)\leqslant\mathrm{rank}(\mathcal{F})\leqslant c$ for all x, and at most c points occur where it is non-zero. Thus we derive

$$\dim H_c^1(\mathbb{G}_m\times\bar{\mathbb{F}}_p,\mathcal{F}\otimes\mathcal{L}_\chi)\leqslant c+c^2\leqslant 2c^2.$$

Finally, since $\sqrt{p}\leqslant\sqrt{2}\sqrt{p-1}$ for all primes p, we deduce the result. □

Corollary 2.5. — *Let $c \geqslant 1$, let p be a prime number, and let $\mathcal{F}$ be an ℓ-adic middle extension sheaf modulo p, pointwise pure of weight 0, with no Kummer sheaf as a geometric Jordan–Hölder component. Assume that the conductor of $\mathcal{F}$ is $\leqslant c$.*

Let $g \in \mathbb{F}_p^\times$ be a generator of $\mathbb{F}_p^\times$ and let $x \in \mathbb{F}_p^\times$ be given. For any interval I in $\mathbb{Z}/(p-1)\mathbb{Z}$, we have

$$\Big|\sum_{n\in I}\tau_{\mathcal{F}}(xg^n)\Big| \leqslant 2\sqrt{2}c^2\sqrt{p-1}\log\Big(4e^8\frac{|I|}{\sqrt{p-1}}\Big).$$

This follows immediately by combining Proposition 2.4 and Theorem 1.1 with $m = p-1$.

From this result, we can deduce equidistribution statements exactly similar to Corollary 1.3, with geometric progressions replacing intervals, since the sheaves used in the proof are in fact geometrically irreducible and are not Kummer sheaves.

Proposition 2.3 also extends with some restriction on the polynomial:

Proposition 2.6. — *Let β be a function defined on integers such that $1 \leqslant \beta(n) \to +\infty$ as $n \to +\infty$. Let $f \in \mathbb{Z}[X]$ be a non-constant* squarefree *monic polynomial. For all primes p large enough, depending on f and β, for any primitive root g modulo p, and for any interval I_p in $\mathbb{Z}/(p-1)\mathbb{Z}$ of size $|I_p| \geqslant (p-1)^{1/2}\beta(p)$, there exists $n \in I_p$ such that $g^n = f(y)$ for some $y \in \mathbb{F}_p^\times$.*

The only change in the proof of the previous case is that we must ensure that the sheaves $\mathcal{F}_i$ for $i \neq 1$ appearing there have no Kummer sheaf as Jordan–Hölder component, for p large enough. This is indeed the case because the assumption that f is squarefree implies first that f is squarefree modulo p for p large enough, and from this follows for each such prime that each $\mathcal{F}_i$ is lisse at 0 (see [10, Prop. 6.7]), which is not the case of $\mathcal{L}_\chi$.

3. The Fourier transfer principle

3.1. The basic principle

In this section we provide a quantitative version of the transfer principle discussed in Section 1.2. The idea is to estimate a sum

$$\sum_{t\in I}\widehat{\varphi}(t)$$

by beginning with an application of the completion method in a smooth form, followed however by a summation by parts that allows us to exploit bounds for short sums of the original function φ.

Proposition 3.1. — *Let $m \geqslant 2$ be an integer and let*

$$\varphi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{C}$$

be an arbitrary function. Let $c \geqslant 1$ be such that

$$\max(\|\varphi\|_\infty, \|\widehat{\varphi}\|_\infty) \leqslant c.$$

For any N with $|N| \leqslant m/2$, and for any $U \in [1/m, N/(2m)]$, we have

$$\begin{aligned}|S(\hat{\varphi}, N)| \ll cmU + c\frac{N}{\sqrt{m}} + \frac{cN}{m^3U^3}\\ + \frac{N}{\sqrt{m}} \int_1^{m/2} \Big(|S(\varphi, t)| + |S(\varphi, -t)|\Big) \min\Big(\frac{N}{m}, \frac{1}{t}, \frac{1}{t^4U^3}\Big) dt,\end{aligned}$$

where the implied constant is absolute.

Proof. — We will view φ as a function on $\mathbb{Z}$ which is periodic modulo m. We consider the case of positive N with $1 \leqslant N \leqslant m/2$, the negative case being entirely similar.

Let $U \in [1/m, N/(2m)] \subset (0, 1/4]$ be some parameter. We fix a smooth function $\Psi : [0, 1] \longrightarrow [0, 1]$ with compact support contained in $[U, N/m + U] \subset [0, 1]$, such that

- For $x \in [2U, N/m]$ we have $\Psi(x) = 1$.
- The function Ψ is increasing on the interval $[U, 2U]$ and decreasing on the interval $[N/m, N/m + U]$,
- For any integer $l \geqslant 0$, we have

$$\Psi^{(l)}(\alpha) \ll_l U^{-l}.$$

We extend Ψ to a 1-periodic function on $\mathbb{R}$ and consider its Fourier expansion

$$\Psi(\alpha) = \sum_{h \in \mathbb{Z}} \widehat{\Psi}(h) e(-h\alpha), \tag{3.1}$$

with

$$\widehat{\Psi}(h) = \int_{[0,1]} \Psi(\alpha) e(h\alpha) d\alpha. \tag{3.2}$$

The properties of the derivatives of Ψ immediately imply the following bounds for its Fourier coefficients

$$\widehat{\Psi}(0) = \frac{N-1}{m} + O(U) = O\Big(\frac{N}{m}\Big), \tag{3.3}$$

and

$$\widehat{\Psi}(h) \ll_A \min\Bigl(\frac{N}{m}, \frac{1}{|h|}(U|h|)^{-A}\Bigr) \tag{3.4}$$

for any $h \neq 0$ and any $A \geqslant 0$. Indeed, this follows from the definition of the Fourier coefficients using repeated integrations by parts and the fact that Ψ is supported in an interval of length $\ll N/m$, whereas the derivatives of Ψ are supported in the union of two intervals of length U.

Now, we observe furthermore that the expression (3.2) defines a *smooth* function of h on the whole real line (namely, the Fourier transform of Ψ seen as a function on $\mathbb{R}$). We have then

$$\widehat{\Psi}'(h) = 2\pi i \int_{[0,1]} \alpha\Psi(\alpha)e(h\alpha)\, d\alpha \ll \Bigl(\frac{N}{m}\Bigr)^2, \tag{3.5}$$

for all h and moreover, for $h \neq 0$, we have (after integrating by parts $A \geqslant 1$ times as in (3.4))

$$\widehat{\Psi}'(h) \ll_A \frac{N}{m|h|}(U|h|)^{-A+1}. \tag{3.6}$$

We now begin the estimation of the partial sums of $\widehat{\varphi}$. We have

$$\begin{aligned} \sum_{1\leqslant n\leqslant N} \widehat{\varphi}(n) &= \sum_{0\leqslant n<m} \widehat{\varphi}(n)\Psi\Bigl(\frac{n}{m}\Bigr) + O\bigl(\|\widehat{\varphi}\|_\infty\, m\,U\bigr) \\ &= m^{1/2}\sum_{h\in\mathbb{Z}} \widehat{\Psi}(h)\varphi(h) + O\bigl(c\,m\,U\bigr), \end{aligned} \tag{3.7}$$

where the implied constant is absolute, and where the second step (a version of the Plancherel formula) follows upon using the Fourier expansion (3.1).

By (3.3), the term $h = 0$ in (3.7) equals

$$\sqrt{m}\varphi(0)\Bigl(\frac{N-1}{m} + O(U)\Bigr) \ll \|\varphi\|_\infty \frac{N}{\sqrt{m}} \ll \frac{cN}{\sqrt{m}}.$$

Next consider the contribution of the positive values of h. By partial summation, these terms contribute

$$\begin{aligned} -\sqrt{m}\int_{1^-}^{\infty} S(\varphi,t)\widehat{\Psi}'(t)dt & \\ \ll \sqrt{m}\Bigl(\frac{N^2}{m^2}\int_1^{m/N} & |S(\varphi,t)|dt \\ &+ \frac{N}{m}\int_{m/N}^{1/U} \frac{|S(\varphi,t)|}{t}dt + \frac{N}{mU^3}\int_{1/U}^{\infty} \frac{|S(\varphi,t)|}{t^4}dt\Bigr), \end{aligned}$$

upon using the estimate (3.5) in the range $t \leqslant m/N$, and the estimate (3.6) with $A = 1$ in the range $m/N \leqslant t \leqslant 1/U$ and with $A = 4$ when $t > 1/U$.

An analogous estimate holds for the contribution of negative h to (3.7), and gathering these estimates together we obtain

$$\begin{aligned}|S(\widehat{\varphi},N)| &\ll cmU + c\frac{N}{\sqrt{m}}\\ &\quad + \frac{N}{\sqrt{m}}\int_1^\infty \Big(|S(\varphi,t)|+|S(\varphi,-t)|\Big)\min\Big(\frac{N}{m},\frac{1}{t},\frac{1}{t^4U^3}\Big)dt.\end{aligned}$$

To complete the proof of the proposition, it remains to bound the portion of the integral with $t > m/2$. Write $t > m/2$ as $t = u + km$ where $k \geqslant 1$ is an integer, and $|u| \leqslant m/2$. Then by dividing the intervals $[1,t]$ and $[-t,-1]$ into complete intervals of length m with intervals of length $|u|$ left over we see that

$$|S(\varphi,t)|+|S(\varphi,-t)| \ll |S(\varphi,u)|+|S(\varphi,-u)|+\frac{ct}{\sqrt{m}},$$

since the sum of φ over a complete interval is $\leqslant c\sqrt{m}$ in size. It follows that the terms $t > m/2$ in the integral contribute

$$\begin{aligned}&\ll \frac{N}{\sqrt{m}}\Big(\int_{m/2}^\infty \frac{ct}{\sqrt{m}}\frac{dt}{t^4U^3} + \int_1^{m/2}(|S(\varphi,u)|+|S(\varphi,-u)|)\sum_{k=1}^\infty \frac{1}{(km)^4U^3}du\Big)\\ &\ll \frac{cN}{m^3U^3} + \frac{N}{\sqrt{m}}\int_1^{m/2}(|S(\varphi,u)|+|S(\varphi,-u)|)\frac{du}{m^4U^3}.\end{aligned}$$

The proposition follows. □

We are now ready for the proof of Theorem 1.2.

Proof of Theorem 1.2. — We first demonstrate (1.9), by an application of Proposition 3.1. To estimate the integral in Proposition 3.1, we bound $|S(\varphi,t)|+|S(\varphi,-t)|$ for $1 \leqslant t \leqslant m/2$ by

$$\max_{t\leqslant m/N}\Big(|S(\varphi,t)|+|S(\varphi,-t)|\Big) \leqslant c\frac{m}{N}\Delta\Big(\varphi,\frac{m}{N}\Big),$$

and

$$\max_{m/2\geqslant t\geqslant m/N}\frac{1}{t}\Big(|S(\varphi,t)|+|S(\varphi,-t)|\Big) \leqslant c\Delta\Big(\varphi,\frac{m}{N}\Big).$$

Thus, it follows that

$$|S(\widehat{\varphi},N)|+|S(\widehat{\varphi},-N)| \ll cmU + c\frac{N}{\sqrt{m}} + \frac{cN}{m^3U^3} + c\frac{N}{\sqrt{m}}\frac{1}{U}\Delta\Big(\varphi,\frac{m}{N}\Big).$$

Now choose $U = N^{\frac{1}{2}}m^{-\frac{3}{4}}\Delta(\varphi,m/N)^{\frac{1}{2}}$; since $\Delta(\varphi,m/N) \geqslant 1/\sqrt{m}$, it follows that $U \geqslant N^{\frac{1}{2}}m^{-1} \geqslant 1/m$, and we may also assume that $U \leqslant N/(2m)$

else the estimate (1.9) holds trivially. Thus our bound above applies, and it gives (noting that $\Delta(\varphi, m/N)/(\sqrt{m}U) \geqslant 1/(mU) \geqslant 1/(mU)^3$)

$$\begin{aligned}|S(\widehat{\varphi}, N)| + |S(\widehat{\varphi}, -N)| &\ll c\sqrt{N} m^{\frac{1}{4}} \Delta\Big(\varphi, \frac{m}{N}\Big)^{\frac{1}{2}} + c\frac{N}{\sqrt{m}} \\ &\ll c\sqrt{N} m^{\frac{1}{4}} \Delta\Big(\varphi, \frac{m}{N}\Big)^{\frac{1}{2}}.\end{aligned}$$

Thus we have established (1.9), and with it in hand, it is a simple matter to verify the second assertion of the theorem. If $t \leqslant N$, then by (1.9) we obtain

$$\frac{1}{cN}\Big(|S(\widehat{\varphi}, t)| + |S(\widehat{\varphi}, -t)|\Big) \ll \frac{\sqrt{t} m^{\frac{1}{4}}}{N} \Delta\Big(\varphi, \frac{m}{t}\Big)^{\frac{1}{2}} \ll \frac{m^{\frac{1}{4}}}{\sqrt{N}} \Delta\Big(\varphi, \frac{m}{N}\Big)^{\frac{1}{2}},$$

since $\Delta(\varphi, m/t)$ is a non-decreasing function of t. Finally if $N \leqslant t \leqslant m/2$ then

$$\begin{aligned}\frac{1}{ct}\Big(|S(\widehat{\varphi}, t)| + |S(\widehat{\varphi}, -t)|\Big) &\ll \frac{m^{\frac{1}{4}}}{\sqrt{t}} \Delta\Big(\varphi, \frac{m}{t}\Big)^{\frac{1}{2}} \\ &= m^{-\frac{1}{4}} \Big(\frac{m}{t}\Delta\Big(\varphi, \frac{m}{t}\Big)\Big)^{\frac{1}{2}} \leqslant m^{-\frac{1}{4}} \Big(\frac{m}{N}\Delta\Big(\varphi, \frac{m}{N}\Big)\Big)^{\frac{1}{2}},\end{aligned}$$

since $(m/t)\Delta(\varphi, m/t)$ is a non-increasing function of t. Combining these estimates, and noting that $1/\sqrt{m}$ is smaller than $(m^{\frac{1}{4}}/\sqrt{N})\Delta(\varphi, m/N)^{\frac{1}{2}}$, we obtain the theorem. □

3.2. Applications

We will prove quantitative versions of Corollary 1.5, in the sense of specifying the value of the quantity $\delta > 0$ that appears there. The argument splits naturally in two cases, depending on whether the character χ in (1.11) is trivial or not. We begin with the former case, where we can in fact work with an arbitrary squarefree modulus $m \geqslant 1$.

Theorem 3.2. — *Let $m \geqslant 1$ be a squarefree integer. Let $P \in (\mathbb{Z}/m\mathbb{Z})[X]$ be a polynomial of degree $d \geqslant 3$ with invertible leading coefficient. Let $\varphi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{C}$ be defined by*

$$\varphi(n) = e_m(P(n))$$

and let

$$\widehat{\varphi}(n) = \frac{1}{m^{1/2}} \sum_{1\leqslant h\leqslant m} e_m(P(h) + nh)$$

be its Fourier transform.

For any $\eta < 1/(2^d - 2)$ there exist $\delta > 0$ depending only on η such that if $N \geqslant m^{1/2-\eta}$, we have

$$\sum_{1 \leqslant n \leqslant N} \widehat{\varphi}(n) \ll N^{1-\delta},$$

where the implied constant depends only on η and d.

Proof. — We begin by noting that a combination of the Weil bound for exponential sums with additive characters and of the Chinese Remainder Theorem shows that

$$|\widehat{\varphi}(t)| \leqslant (d-1)^{\omega(m)} \ll m^{\varepsilon}$$

for any $\varepsilon > 0$ and any $t \in \mathbb{Z}/m\mathbb{Z}$, where the implied constant depends only on ε and d (we use here the fact that P is of degree d modulo any prime divisor of m, since we assume that the leading coefficient is invertible modulo m). In particular, we get

$$c = \max(\|\varphi\|_\infty, \|\widehat{\varphi}\|_\infty) \ll m^{\varepsilon}. \tag{3.8}$$

Let $\kappa = 1/2^{d-1}$. The key ingredient is the Weyl bound

$$\Big|\sum_{1 \leqslant h \leqslant H} e_m(P(h))\Big| \ll H^{1+\varepsilon}\Big(\frac{1}{H} + \frac{m}{H^d}\Big)^{\kappa} \tag{3.9}$$

valid for an arbitrary $\varepsilon > 0$ and $1 \leqslant H \leqslant m$, with an implied constant that depends only on d and ε (see [17, Lemma 20.3] or [23, Lemma 2.4], and for recent bounds that are much stronger for large d, see [24, Th. 1.5]). This implies that for $1 \leqslant t \leqslant m/2$, we have

$$|S(\varphi, \pm t)| \ll \min\Big(|t|, |t|^{1+\varepsilon}\Big(\frac{1}{|t|} + \frac{m}{|t|^d}\Big)^{\kappa}\Big)$$

for any $\varepsilon > 0$, where the implied constant depends on d and ε only. By (1.6), this leads to

$$\Delta(\varphi, H) \ll \frac{1}{\sqrt{m}} + \frac{m^{\varepsilon}}{c}\Big(\frac{1}{H^{\kappa}} + \frac{m^{\kappa}}{H^{d\kappa}}\Big)$$

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

Appealing to (1.9) from Theorem 1.2, we conclude that

$$\Big|\sum_{n \leqslant N} \widehat{\varphi}(n)\Big| \ll cN^{1/2} + c^{1/2} N^{\frac{1}{2}} m^{\frac{1}{4}+\epsilon}\Big(\frac{N^{\kappa}}{m^{\kappa}} + \frac{N^{d\kappa}}{m^{(d-1)\kappa}}\Big)^{\frac{1}{2}},$$

which, with a small calculation using (3.8), yields the theorem. □

When the character χ in (1.11) is non-trivial, we will need to assume that the modulus is prime.

Theorem 3.3. — *Let p be a prime number. Let $P \in \mathbb{F}_p[X]$ be a polynomial of degree $d \geqslant 0$, let χ be a non-trivial multiplicative character modulo p and let $m \in \mathbb{F}_p$. Define $\varphi : \mathbb{F}_p \longrightarrow \mathbb{C}$ by*

$$\varphi(n) = \chi(n+m)e_p(P(n))$$

and let

$$\widehat{\varphi}(n) = \frac{1}{p^{1/2}} \sum_{1 \leqslant h \leqslant p} \chi(h+m)\, e_p(P(h)+nh)$$

be its Fourier transform.

For any $\eta < \frac{1}{8(d^2+d+1)}$ there exists $\delta > 0$ such that for all N with $N \geqslant p^{1/2-\eta}$, we have

$$\sum_{1 \leqslant n \leqslant N} \widehat{\varphi}(n) \ll N^{1-\delta},$$

where the implied constant depends only on η and d.

Proof. — The method is similar to the previous case. However, we now use instead of the Weyl bound a recent result of Heath-Brown and Pierce, namely

$$\Big| \sum_{1 \leqslant n \leqslant N} \chi(n+m)e_p(P(n)) \Big| \ll_{d,r} (\log p)^2 \min\Big(p^{1/2}, p^{\frac{r+1+D}{4r^2}} N^{1-\frac{1}{r}} \Big)$$

where $D = d(d+1)/2$ (see [16, Th. 1.2], noting that the bound is stated there only for $N \leqslant q^{1/2+1/4r}$, but that it becomes weaker than the Pólya–Vinogradov bound when $N \geqslant p^{1/2+1/4r}$). Thus

$$\Delta(\varphi, N) \ll_{d,r} (\log p)^2 p^{\frac{r+1+D}{4r^2}} N^{-\frac{1}{r}}.$$

Applying (1.9) of Theorem 1.2, we obtain (for $N > p^{\frac{1}{4}}$)

$$\Big| \sum_{n \leqslant N} \widehat{\varphi}(n) \Big| \ll p^{\frac{1}{4} + \frac{r+1+D}{8r^2} - \frac{1}{2r}} N^{\frac{1}{2} + \frac{1}{2r}} (\log p).$$

Choosing $r = 2(D+1)$, the theorem follows. □

Remark 3.4. — The bound of Heath-Brown and Pierce is the latest of a series of works by Enflo, Heath-Brown and Chang, see [7, 15, 6], any one of which would lead to the qualitative form in Corollary 1.5.

We now consider the special case of the cubic Birch sums to prove Corollary 1.6.

Proof of Corollary 1.6. — Let p be prime and let φ be defined on $\mathbb{F}_p$ by

$$\varphi(h) = e_p(h^3).$$

As before, we denote by

$$\mathrm{B}_3(n) = \frac{1}{p^{1/2}} \sum_{1\leqslant h\leqslant p} e_p(h^3 + nh)$$

its Fourier transform. Note that for any fixed $m \in \mathbb{Z}$, the shifted Birch sums $n \mapsto \mathrm{B}_3(n+m)$ is also a Fourier transform of a polynomial, namely of

$$h \mapsto e_p(h^3 + hm).$$

Thus the estimate (1.12) for the first moment is a special case of Theorem 3.2: for any $\eta < 1/6$, there exists $\delta > 0$, depending only on η, such that

$$\sum_{m\leqslant n\leqslant m+N} \mathrm{B}_3(n) \ll N^{1-\delta}$$

for all $m \in \mathbb{Z}$, provided $N > p^{1/2-\eta}$.

We now consider the second moment. We assume $p \geqslant 5$ and we define

$$\psi(n) = |\mathrm{B}_3(n)|^2 - 1,$$

and compute its Fourier transform. For any $h \in \mathbb{F}_p^\times$, we have

$$\begin{aligned}
\widehat{\psi}(h) &= \frac{1}{p^{1/2}} \sum_{n\in\mathbb{F}_p} (|\mathrm{B}_3(n)|^2 - 1) e_p(nh) \\
&= \frac{1}{p^{3/2}} \sum_{u,v,n\in\mathbb{F}_p} e_p\big(u^3 - v^3 + n(u - v + h)\big) \\
&= \frac{1}{p^{1/2}} \sum_{u\in\mathbb{F}_p} e_p(u^3 - (u+h)^3).
\end{aligned}$$

This is a quadratic complete sum, hence it can be evaluated exactly. Precisely, we obtain by completing the square the formula

$$\widehat{\psi}(h) = \varepsilon_p \Big(\frac{h}{p}\Big) e_p(-h^3/4)$$

for $h \in \mathbb{F}_p^\times$, where ε_p is a complex number of modulus one independent of h. In fact, the same formula holds for $h = 0$, as one checks immediately by a similar computation.

By the discrete Fourier inversion formula, we deduce that ψ is the Fourier transform of the function $n \mapsto \varepsilon_p\big(\frac{n}{p}\big)e_p(n^3/4)$. Hence Theorem 3.3 implies

(after using an additive shift by m as above to get the estimate for any interval)

$$\sum_{m\leqslant n\leqslant m+N} (|\mathrm{B}_3(n)|^2 - 1) \ll N^{-\delta}$$

for any $\eta < 1/104$ and some $\delta > 0$ depending only on η, which is more precise than (1.13).

We now prove the final part of Corollary 1.6 concerning the distribution of values of Birch sums. Let $\eta < 1/104$ be fixed and let I be an interval in $\mathbb{Z}$ with $|I| \geqslant p^{1/2-\eta}$. From our work above, we know that for some $\delta > 0$ (depending only on η) we have

$$(1 + O(p^{-\delta}))|I| = \sum_{n\in I} |\mathrm{B}_3(n)|^2 \leqslant t^2 \sum_{\substack{n\in I\\ \mathrm{B}_3(n)\in[0,t]}} 1 + 4 \sum_{\substack{n\in I\\ \mathrm{B}_3(n)\notin[0,t]}} 1,$$

where we have used the Weil bound $|\mathrm{B}_3(n)| \leqslant 2$. With a little rearranging, this yields

$$\sum_{\substack{n\in I\\ \mathrm{B}_3(n)\in[0,t]}} 1 \leqslant \Big(\frac{3}{4-t^2} + o(1)\Big)|I|. \tag{3.10}$$

On the other hand, since $\sum_{n\in I} \mathrm{B}_3(n) = o(|I|)$ we have

$$\begin{aligned}\sum_{\substack{n\in I\\ \mathrm{B}_3(n)<0}} \mathrm{B}_3(n)^2 \leqslant 2 \sum_{\substack{n\in I\\ \mathrm{B}_3(n)<0}} |\mathrm{B}_3(n)| &= 2 \sum_{\substack{n\in I\\ \mathrm{B}_3(n)\geqslant 0}} \mathrm{B}_3(n) + o(|I|)\\ &\leqslant 2t \sum_{\substack{n\in I\\ \mathrm{B}_3(n)\in[0,t]}} 1 + 4 \sum_{\substack{n\in I\\ \mathrm{B}_3(n)\in(t,2]}} 1 + o(|I|),\end{aligned}$$

and therefore

$$\begin{aligned}(1 + o(1))|I| = \sum_{n\in I} |\mathrm{B}_3(n)|^2 \leqslant t^2 &\sum_{\substack{n\in I\\ \mathrm{B}_3(n)\in[0,t]}} 1 + 4 \sum_{\substack{n\in I\\ \mathrm{B}_3(n)\in(t,2]}} 1\\ &+ 2t \sum_{\substack{n\in I\\ \mathrm{B}_3(n)\in[0,t]}} 1 + 4 \sum_{\substack{n\in I\\ \mathrm{B}_3(n)\in(t,2]}} 1 + o(|I|).\end{aligned}$$

Combining this with (3.10), we deduce that (for $t < 1/2$)

$$\sum_{\substack{n\in I\\ \mathrm{B}_3(n)>t}} 1 \geqslant \frac{1}{8}\Big(1 - \frac{3t}{2-t} + o(1)\Big)|I| = \Big(\frac{1-2t}{4(2-t)} + o(1)\Big)|I|,$$

as desired. The bound on the number of $\mathrm{B}_3(n) < -t$ is obtained similarly. The last bound on the frequency of n with $|\mathrm{B}_3(n)| \geqslant t$ follows upon noting that

$$|I| \sim \sum_{n\in I} |\mathrm{B}_3(n)|^2 \leqslant t^2 \sum_{\substack{n\in I\\ |\mathrm{B}_3(n)|\leqslant t}} 1 + 4 \sum_{\substack{n\in I\\ |\mathrm{B}_3(n)|>t}} 1 \sim t^2|I| + (4-t^2) \sum_{\substack{n\in I\\ |\mathrm{B}_3(n)|>t}} 1.$$

□

Finally, we prove Corollary 1.7.

Proof of Corollary 1.7. — Let p be prime and $a \in \mathbb{F}_p^\times$. Let $k = 1$ or $k = 2$, and define

$$\varphi(h) = e_p(ah^{-k})$$

for $h \in \mathbb{F}_p^\times$ and $\varphi(0) = 0$. Then

$$\widehat{\varphi}(n) = \frac{1}{p^{1/2}} \sum_{h\in\mathbb{F}_p^\times} e_p(ah^{-k} + nh).$$

In [4, 3], Bourgain and Garaev have obtained non-trivial estimates for sums of φ. Precisely, they proved that there exist absolute constants $\delta > 0$ and $0 < \eta < 1$ such that

$$\max_{a\in\mathbb{F}_p^\times} \Big| \sum_{1\leqslant h\leqslant H} e_p\big(ah^{-k}\big) \Big| \ll H(\log p)^{-\delta} \tag{3.11}$$

provided $H \geqslant \exp((\log p)^\eta)$. Thus, if $H \geqslant \exp((\log p)^\eta)$, then $\Delta(\varphi, H) \ll (\log p)^{-\delta}$.

Applying (1.9) of Theorem 1.2, we obtain for $p^{\frac{1}{2}}(\log p)^{-\frac{\delta}{2}} \leqslant N \leqslant p^{\frac{1}{2}}(\log p)^2$,

$$S(\varphi, N) \ll \sqrt{N} p^{\frac{1}{4}} (\log p)^{-\frac{\delta}{2}} \ll N(\log p)^{-\frac{\delta}{4}}.$$

Since this bound holds also in the range $N \geqslant p^{\frac{1}{2}}(\log p)^2$ by Pólya–Vinogradov, our proof is complete. □

BIBLIOGRAPHY

[1] B. J. Birch, "How the number of points of an elliptic curve over a fixed prime prime varies", *J. Lond. Math. Soc.* **43** (1968), p. 57-60.

[2] V. Blomer, É. Fouvry, E. Kowalski, P. Michel & D. Milićević, "On moments of twisted L–functions", `http://arxiv.org/abs/1411.4467`, to appear in *American J. Math.*

[3] J. Bourgain, "A Remark on Solutions of the Pell Equation", *Int. Math. Res. Not.* **2015** (2015), no. 10, p. 2841-2855.

[4] J. Bourgain & M. Z. Garaev, "Sumsets of reciprocals in prime fields and multilinear Kloosterman sums", *Izv. Math.* **78** (2014), no. 4, p. 656-707, translation from *Izv. Ross. Akad. Nauk. Mat.* **78** (2014), no. 4, p. 656-707.

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

[6] M.-C. Chang, "An estimate of incomplete mixed character sums", in *An irregular mind*, Bolyai Soc. Math. Stud., vol. 21, Springer, 2010, p. 243-250.

[7] P. Enflo, "Some problems in the interface between number theory, harmonic analysis and geometry of Euclidean space", *Quaest. Math.* **18** (1995), no. 1-3, p. 309-323.

[8] É. Fouvry, E. Kowalski & P. Michel, "Counting sheaves using spherical codes", *Math. Res. Lett.* **20** (2013), no. 2, p. 305-323.

[9] ———, "An inverse theorem for Gowers norms of trace functions over $\mathbf{F}_p$", *Math. Proc. Camb. Philos. Soc.* **155** (2013), no. 2, p. 277-295.

[10] ———, "Algebraic trace functions over the primes", *Duke Math. J.* **163** (2014), no. 9, p. 1183-1736, `http://arxiv.org/abs/1211.6043`.

[11] ———, "Algebraic twists of modular forms and Hecke orbits", *Geom. Funct. Anal.* **25** (2015), no. 2, p. 580-657, `http://arxiv.org/abs/1207.0617`.

[12] ———, "On the exponent of distribution of the ternary divisor function", *Mathematika* **61** (2015), no. 1, p. 121-144.

[13] ———, "Trace functions over finite fields and their applications", in *Colloquium de Giorgi 2013 and 2014*, vol. 5, Scuola Normale Superiore de Pisa, 2015, p. 7-35.

[14] D. A. Frolenkov & K. Soundararajan, "A generalization of the Pólya-Vinogradov inequality", *Ramanujan J.* **31** (2013), no. 3, p. 271-279.

[15] D. R. Heath-Brown, "MR review of "Some problems in the interface between number theory, harmonic analysis and geometry of Euclidean space" by P. Enflo", MR 1340486 (96h:11079).

[16] D. R. Heath-Brown & L. B. Pierce, "Burgess bounds for short mixed character sums", *J. Lond. Math.Soc.* **91** (2015), no. 3, p. 693-708.

[17] H. Iwaniec & E. Kowalski, *Analytic Number Theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004, xi+615 pages.

[18] N. M. Katz, *Gauss sums, Kloosterman sums and monodromy groups*, Annals of Mathematics Studies, vol. 116, Princeton University Press, 1988, viii+246 pages.

[19] ———, *Convolution and equidistribution: Sato-Tate theorems of finite-field Mellin transforms*, Annals of Mathematics Studies, vol. 180, Princeton University Press, 2012, vi+203 pages.

[20] N. M. Korobov, *Exponential sums and their applications*, Mathematics and its Applications (Soviet Series), vol. 80, Kluwer Academic Publishers Group, 1992, xv+209 pages.

[21] E. Kowalski & W. Sawin, "Kloosterman paths and the shape of exponential sums", *Compositio Math.* **152** (2016), no. 7, p. 1489-1516.

[22] R. Livné, "The average distribution of cubic exponential sums", *J. Reine Angew. Math.* **375-376** (1987), p. 362-379.

[23] R. C. Vaughan, *The Hardy–Littlewood method.*, 2nd ed., Cambridge Tracts in Mathematics, vol. 125, Cambridge University Press, 1997, vii+232 pages.

[24] T. D. Wooley, "Vinogradov's mean value theorem via efficient congruencing", *Ann. Math.* **175** (2012), no. 3, p. 1575-1627.

Manuscrit reçu le 3 août 2015,
révisé le 23 juin 2016,
accepté le 12 juillet 2016.

Étienne FOUVRY
Laboratoire de Mathématiques d'Orsay
Université Paris-Sud CNRS
Université Paris-Saclay
91405 Orsay (France)
etienne.fouvry@math.u-psud.fr

Emmanuel KOWALSKI
ETH Zürich – D-MATH
Rämistrasse 101
8092 Zürich (Switzerland)
kowalski@math.ethz.ch

Philippe MICHEL
EPFL Mathgeom-TAN
Station 8
C1015 Lausanne (Switzerland)
philippe.michel@epfl.ch

Chandra Sekhar RAJU
Department of Mathematics
450 Serra Mall, Stanford
California 94305 (USA)
chandras@stanford.edu

Joël RIVAT
Institut de Mathématiques de Marseille
Case 907
Université d'Aix-Marseille
163, avenue de Luminy
13288 Marseille Cedex 9 (France)
joel.rivat@univ-amu.fr

Kannan SOUNDARARAJAN
Department of Mathematics
450 Serra Mall, Stanford
California 94305 (USA)
ksound@stanford.edu