Bulletin

de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

A SPECTRAL RESOLUTION OF THE LARGE SIEVE

Olivier Ramaré

Tome 153
Fascicule 3

2025

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

pages 575-636

Le *Bulletin de la Société Mathématique de France* est un périodique trimestriel de la Société Mathématique de France.

Fascicule 3, tome 153, septembre 2025

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
commandes@smf.emath.fr

AMS
P.O. Box 6248
Providence RI 02940
USA
www.ams.org

Tarifs

Vente au numéro : 50 € ($ 75)
Abonnement électronique : 165 € ($ 247),
avec supplément papier : Europe 251 €, hors Europe 289 € ($ 433)
Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Bulletin de la SMF

Bulletin de la Société Mathématique de France
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 1 44 27 67 99 • Fax : (33) 1 40 46 90 96
bulletin@smf.emath.fr • smf.emath.fr

ISSN 0037-9484 (print) 2102-622X (electronic)

Directrice de la publication : Isabelle GALLAGHER

Bull. Soc. Math. France
153 (3), 2025, p. 575-636

A SPECTRAL RESOLUTION OF THE LARGE SIEVE

BY OLIVIER RAMARÉ

ABSTRACT. — Let $\varphi = (\varphi_n)_{n\le N}$ denote a sequence of complex numbers. The main object of this paper is the quadratic form

$$V(\varphi, Q) = \sum_{Q<q\le 2Q} \sum_{a \bmod^* q} \left|\sum_{n=1}^{N} \varphi_n e^{2i\pi na/q}\right|^2,$$

where $a \bmod^* q$ denotes an integer variable a that goes through the points of $\{1,\dots,q\}$ that are prime to q. The real parameters N and Q are assumed to be large. The eigenvalues of $V(\cdot, Q)$ are well understood when $Q = o(\sqrt{N})$ and $V(\varphi, Q)$ behaves like a Riemann sum when $N = o(Q)$. The behavior in the range $Q \in [\sqrt{N}, 100N]$ is the object of our queries. In particular, we present a full spectral analysis when $Q \ge N^{3/4}$ in terms of the eigenvalues of a one-parameter family of nuclear difference operators. Among the consequences, we show that $V(\varphi, Q)/(Q^2 \sum_n |\varphi_n|^2)$ stays between two positive constants uniformly in φ, when N/Q stays similarly between two positive constants, and that (a smoothed version of) the quadratic form $V(\cdot, Q)$ may stay *away* from the diagonal form $\varphi \mapsto (6/\pi^2)Q^2 \sum_n |\varphi_n|^2$ when N/Q stays between two positive constants, although only on a vector space of φ of positive but small dimension.

Texte reçu le 7 mars 2023, modifié le 25 mai 2024, accepté le 29 mai 2024.

OLIVIER RAMARÉ, Aix Marseille Univ, CNRS, I2M, Marseille, France • *E-mail :* `olivier.ramare@univ-amu.fr`

Mathematical subject classification (2010). — 42A05, 47G10, 11L03, 47N99; 46E10, 11L07, 11N35.

Key words and phrases. — Large sieve inequality, difference operators.

This paper was supported by the joint FWF-ANR project Arithrand: FWF: I 4945-N and ANR-20-CE91-0006.

 0037-9484/2025/575/$ 5.00
 doi:10.24033/bsmf.2907

RÉSUMÉ (*Une resolution spectrale du grand crible*). — Dénotons par $\varphi = (\varphi_n)_{n\le N}$ une suite de nombres complexes. Nous étudions ici la forme quadratique

$$V(\varphi, Q) = \sum_{Q<q\le 2Q}\sum_{a \bmod^* q}\Bigl|\sum_{n=1}^{N}\varphi_n e^{2i\pi na/q}\Bigr|^2$$

où $a \bmod^* q$ désigne une variable entière a qui parcourt les points de $\{1,\ldots,q\}$ qui sont premiers à q. Les paramètres réels N et Q sont entendus comme étant grands. Nous comprenons convenablement les valeurs propres de $V(\cdot, Q)$ lorsque $Q = o(\sqrt{N})$; par ailleurs, $V(\varphi, Q)$ se comporte comme une somme de Riemann quand $N = o(Q)$. Nous examinons ici le comportement de ces valeurs propres dans le domaine $Q \in [\sqrt{N}, 100N]$ et, en particulier, présentons une analyse spectrale complète lorsque $Q \ge N^{3/4}$ à partir des valeurs propres d'une famille à un paramètre d'opérateurs différence nucléaires. Une des conséquences notables de notre étude est que le quotient $V(\varphi, Q)/(Q^2\sum_n|\varphi_n|^2)$ reste entre deux constantes strictement positives, uniformément en φ, lorsque N/Q reste de même entre deux constantes strictement positives. De plus, nous montrons que la forme quadratique $V(\cdot, Q)$ (sous une version lissée) peut *ne pas* s'approcher de la forme diagonale $\varphi \mapsto (6/\pi^2)Q^2\sum_n|\varphi_n|^2$, toujours lorsque N/Q reste entre deux constantes strictement positives, bien que ce comportement ne se produise que sur un espace vectoriel en φ de dimension petite mais supérieure à 1.

1. Introduction and main consequence

This manuscript studies a fundamental tool in analytic number theory, namely *the large sieve inequality.* In the context relevant to the present paper, it is an inequality of the following shape: for any sequence $(\varphi_n)_{1\le n\le N}$ and all $Q \ge 1$, we have

$$\sum_{q\le Q}\sum_{a \bmod^* q}\Bigl|\sum_{n=1}^{N}\varphi_n e^{2i\pi na/q}\Bigr|^2 \le (N+Q^2)\sum_n|\varphi_n|^2, \tag{1}$$

where $a \bmod^* q$ denotes an integer variable a that goes through the values of $\{1,\cdots,q\}$ that are prime to q. The readers may consult, for instance, [31, 32] by H. Montgomery and R.C. Vaughan on this inequality, which emerged from the fundatory work of Y. Linnik in the 1940s. In many applications to Diophantine equations with primes, the large sieve inequality is used as a substitute for the Riemann hypothesis (for instance, in the 1965 Bombieri–Vinogradov theorem on primes in arithmetic progressions).

In the present paper, we look at the situation when Q is large. In this situation, the large sieve inequality (1) is expected to be sharp by a random sampling heuristic: for a generic sequence (φ_n) the two sides will be of the same order of magnitude. Finding a reverse inequality, as sharp as possible relative to the upper-bound (1), has been studied since the 1980s. So far, this problem has been successfully addressed in three instances:

- For sequences (φ_n) taken at random by P. Erdős and A. Rényi in [17], by D. Wolke in [49], and by J.-C. Schlage-Puchta in [42].
- For the specific instance of a sequence (φ_n) related to the Möbius function by B. Conrey, H. Iwaniec, and K. Soundararajan in [9].
- When (φ_n) is the convolution of a shortly supported sequence with a smooth sequence in [37, Theorem 2.6]. See also [19] by J. Friedlander and H. Iwaniec.

A major consequence of our work is the next uniform lower bound valid for *all* sequences (φ_n).

THEOREM 1.1. — *There exists $c > 0$ such that for every N large enough and $Q \in [N/(c\sqrt{\log N}), 20N]$, we have*

$$Q^2 e^{-cN/Q} \sum_m |\varphi_m|^2 \leq \sum_{Q<q\leq 2Q} \sum_{a\ mod^* q} \left| \sum_{n=1}^{N} \varphi_n e^{2i\pi na/q} \right|^2 \leq cQ^2 \sum_m |\varphi_m|^2.$$

The crucial point is that this is uniform in (φ_n), which requires a much more complicated machinery than in earlier work. The large size of Q is the price that is being paid for this uniformity.

Theorem 1.1 can be compared with the lower bound given by W. Duke and H. Iwaniec in [12]; the summation therein extends over every class a modulo q rather than over the reduced ones. In particular, the class $a = 0$ is included with a definite influence; see the remark following [37, Theorem 2.7].

More generally, we obtain an explicit expression for the left-hand side of (1) in the large Q regime as an identity of the shape

$$\sum_{Q<q\leq 2Q} \sum_{a \bmod^* q} \left| \sum_{n=1}^{N} \varphi_n e^{2i\pi na/q} \right|^2 \approx Q^2 \|\varphi\|_2^2 - Q^2 \sum_{h\leq N/Q} \frac{1}{h} \sum_{a \bmod^* h} \mathcal{Q}_h\big((\varphi_n e^{2i\pi na/h})_n\big),$$

where $\mathcal{Q}_h$ is some quadratic form on sequences on $\{1, \ldots, N\}$. This constitutes roughly half of the paper and replaces the moduli q of size Q by the moduli h of size at most N/Q. In the second half, we carry out a spectral analysis of the quadratic forms, getting enough information on their eigenvalues through an instance of the uncertainty principle to obtain the lower bound in Theorem 1.1.

Setting the horizon for a lower bound. —

QUESTION. — *Does the inequality*

$$\sum_{Q<q\leq 2Q} \sum_{a\ mod^* q} \left| \sum_{n=1}^{N} \varphi_n e^{2i\pi na/q} \right|^2 \gg N \sum_m |\varphi_m|^2$$

hold as soon as $Q \geq N^{1/2+\varepsilon}$ for some positive ε?

When $N = \sum_{q \le Q} \phi(q)$, we gave in [37, Theorem 1.2] the (rather weak) lower bound $\|\varphi\|_2^2 \exp(\frac{-1+o(1)}{2} N \log N)$ for the quantity $\sum_{q \le Q} \sum_{a \bmod^* q} |S(\varphi, a/q)|^2$. Theorem 2.2 implies that the better lower bound $Q^2 \|\varphi\|_2^2$ holds true as soon as φ oscillates enough along small arithmetic progressions in intervals of length about Q. The main result of [9, Theorem 2.4] by B. Conrey, H. Iwaniec, and K. Soundararajan implies a similar lower bound for functions φ that are the convolution product of an oscillating factor supported on $[1, Q^{1-\varepsilon}]$ and a rather general sequence.

Notation. — By $a \sim A$, we mean that $1 \le a/A \le 2$, while $f(x) \ll g(x)$ means that there exists a constant c such that $|f(x)| \le c g(x)$ for all the values of x under consideration. In case, this constant depends on some parameters, like some positive ε otherwise introduced, and we write $f(x) \ll_\varepsilon g(x)$. When we write a mod q, we mean that the integer variable a ranges through $\{1, \dots, q\}$, while a mod* q restricts a similar variable a to range the values of $\{1, \dots, q\}$ that are prime to q, sometimes called the *reduced* residue classes. Both a mod 1 and a mod* 1 are equivalent to $a = 1$. In practice, we use a mod q or a mod* q only when the summand depends only on the residue class of a modulo q, and we may confuse this residue class with an integer representative.

We denote the Mellin transform by $\check{W}(s) = \int_0^\infty W(t) t^{s-1} dt$ and the Fourier transform by $\hat{W}(u) = \int_{-\infty}^\infty W(t) e(-ut) dt$. Some other transforms of W will be used, $W^\sharp$, W, $\tilde{W}$ and $W^\star$; they are described in Section 6. We note here that the transform $W^\sharp$ is very close to what appears in [25, Section 20.5, (20.145)] provided that the change of notation is incorporated: our $W(y)$ is their $w(y/C)$. We also define

$$\mathfrak{L}(u) = \exp -\sqrt{\log(2+u)}. \tag{2}$$

Given a positive integer h and an integer z, we denote by $\sigma_h(z)$ the unique integer b in $\{1 \cdots h\}$ that is congruent to z modulo h. We denote the Euler totient function by ϕ and distinguish it from the sequence by using a different script for the latter, namely φ. Finally, we employ the shortcut

$$\tau = N/Q. \tag{3}$$

2. Detailed results and global proof scheme

Let us now present the players and results more precisely.

A smoothed setup. — Our analysis revolves around the quantity

$$\sum_{q \ge 1} \frac{W(q/Q)}{q} \sum_{a \bmod^* q} \left| \sum_{n=1}^{N} \varphi_n e^{2i\pi na/q} \right|^2 \tag{4}$$

for some weight function W satisfying the following:

(W_1) The function W is C^3 over $(-\infty,\infty)$ and C^4 by parts.
(W_2) It is even and its support lies inside $[-2,-1]\cup[1,2]$.
(W_3) We have $\int_0^\infty W(u)du \neq 0$.

We do not need W to be non-negative, although nothing is done to avoid this natural condition. We do not seek generality but, on the other hand, we restrict ourselves to as smooth a situation as necessary. The Mellin transform of W is defined by

$$\check{W}(s) = \int_0^\infty W(u)u^{s-1}ds. \tag{5}$$

This is classical, save that we add the precision that we only consider the interval $[0,\infty)$, while the Fourier transform is defined by

$$\hat{W}(v) = \int_{-\infty}^\infty W(u)e(-uv)du. \tag{6}$$

Repeated integrations by parts ensure that $\check{W}(s) \ll 1/(1+|s|)^4$ and $\hat{W}(v) \ll 1/(1+|v|)$. We further define

$$I_0(W) = \sum_q \frac{\phi(q)W(q/Q)}{qQ} = \frac{6}{\pi^2}\int_0^\infty W(u)du + \mathcal{O}((\log Q)/Q), \tag{7}$$

where $\phi(q)$ is the value of the Euler ϕ-function at q. The quantity $I_0(W)$ depends on Q, but in a very mild manner.

Some functional transforms. — The δ-symbol technique involves several functional transforms of the weight function W that we treat before starting the analysis proper. The assumptions on W being as above, we may define $W^\star$ by (29) with $C=\infty$, but the following expression, valid for $z\in\mathbb{R}$, is better:

$$W^\star(z) = -2\sum_{n\geq 1}\frac{\phi(n)}{n}\int_0^\infty \cos(2\pi n y)W(z/y)dy/y. \tag{8}$$

By Lemma 6.10, the function $W^\star$ is even, twice differentiable outside $z=0$, where it vanishes, is of bounded variations over $[0,1]$ and decreases like $1/z^{\frac{7}{2}-\varepsilon}$ at infinity. The expression for its Mellin transform, valid when $\Re s\in[0,3/2)$, is simply $\check{W^\star}(s) = \check{W}(s)\zeta(1-s)/\zeta(1+s)$; see Lemma 6.7. The following expression for its Fourier transform, valid for $u\neq 0$ is obtained in Lemma 6.8:

$$\hat{W}^\star(u) = \frac{6}{\pi^2}\int_0^\infty W(t)dt - \frac{1}{|u|}\sum_{n\geq 1}\frac{\phi(n)}{n}W(n/|u|). \tag{9}$$

This Fourier transform satisfies $\hat{W}^\star(u) = \frac{6}{\pi^2}\int_0^\infty W(t)dt$ when $|u|\leq 1/2$ and $|u\hat{W}^\star(u)| \ll \exp -c_0\sqrt{\log|u|}$ otherwise, for some positive constant c_0, ensuring that $\hat{W}^\star(u)$ belongs to L^1. It is worth specifying that $\hat{W}^\star(u)$ varies in sign when