ISSN 0012-9593

*quatrième série - tome 59 fascicule 2 mars-avril 2026*

# ANNALES SCIENTIFIQUES de L'ÉCOLE NORMALE SUPÉRIEURE

Valentin BLOMER, Farrell BRUMLEY & Ilya KHAYUTIN

## *The mixing conjecture under GRH*

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

# Annales Scientifiques de l'École Normale Supérieure

Publiées avec le concours du Centre National de la Recherche Scientifique



**Rédaction / *Editor***

Annales Scientifiques de l'École Normale Supérieure,
45, rue d'Ulm, 75230 Paris Cedex 05, France.
Tél. : (33) 1 44 32 20 88.
Email : annales@ens.fr

**Édition et abonnements / *Publication and subscriptions***

Société Mathématique de France
Case 916 - Luminy
13288 Marseille Cedex 09
Tél. : (33) 04 91 26 74 64
Email : abonnements@smf.emath.fr

**Tarifs**

Abonnement électronique : 514 euros.
Abonnement avec supplément papier :
Europe : 722 €. Hors Europe : 813 € ($ 985). Vente au numéro : 77 €.



ISSN 0012-9593 (print) 1873-2151 (electronic)

Directrice de la publication : Isabelle Gallagher
Périodicité : 6 nos / an

*Ann. Scient. Éc. Norm. Sup.*
4$^{e}$ série, t. 59, 2026, p. 437 à 500

# THE MIXING CONJECTURE UNDER GRH

BY Valentin BLOMER, Farrell BRUMLEY
AND Ilya KHAYUTIN

Abstract. – We prove the mixing conjecture of Michel-Venkatesh for the class group action on Heegner points of large discriminant on compact arithmetic surfaces attached to maximal orders in rational quaternion algebras. The proof is conditional on the generalized Riemann hypothesis, and, when the division algebra is indefinite, we furthermore assume the Ramanujan conjecture. We establish the mixing conjecture for the discrete spectrum of the modular surface as well, under the same conditions. Our methods, which provide an effective rate, are based on the spectral theory of automorphic forms and their $L$-functions, together with sieve methods and multiplicative functions.

Résumé. – Nous démontrons la conjecture de mélange de Michel-Venkatesh pour l'action du groupe de classes sur les points de Heegner de grand discriminant sur les surfaces compactes arithmétiques associées aux ordres maximaux dans les algèbres de quaternions rationnelles. La preuve est conditionnelle sur l'hypothèse de Riemann généralisée, et lorsque l'algèbre de division est indéfinie, nous supposons par ailleurs la conjecture de Ramanujan. Nous établissons également la conjecture de mélange pour le spectre discret de la surface modulaire, sous les mêmes conditions. Nos méthodes, qui donnent un taux effectif, passent par la théorie spectrale des formes automorphes et leurs fonctions $L$, ainsi que les méthodes de crible et les fonctions multiplicatives.

## 1. Introduction

A celebrated theorem of Duke [13] and Golubeva-Fomenko [27] states that the primitive integer points of norm $\sqrt{d}$ equidistribute when projected to the unit sphere $S^2$, as $d \to \infty$ along sequences avoiding local obstructions.

The first author was supported in part by Germany's Excellence Strategy grant EXC-2047/1–390685813 and ERC Advanced Grant 101054336. The second author is supported by the Institut Universitaire de France and ANR-FNS Grant ANR-24-CE93-0016. The third author has been supported by National Science Foundation Grant No. DMS-1946333, a Sloan Research Fellowship and an AMS Centennial Fellowship.

0012-9593/02/ doi:10.24033/asens.2642

More precisely, let $\mathbb{Z}^3_{\text{prim}} = \{x \in \mathbb{Z}^3 : \gcd(x_1, x_2, x_3) = 1\}$ denote the primitive points of the standard integral lattice in $\mathbb{R}^3$, and put

$$R_d = \{x \in \mathbb{Z}^3_{\text{prim}} : x_1^2 + x_2^2 + x_3^2 = d\}.$$

Then $\mathbb{D} = \{d \in \mathbb{N} : d \not\equiv 0, 4, 7 \,(\text{mod } 8)\}$ is the set of locally admissible integers. The aforementioned authors, following a breakthrough of Iwaniec [35] on the estimation of Fourier coefficients of half-integral weight Maass forms, showed that, as $d \in \mathbb{D}$ tends to infinity, the rescaled sets $d^{-1/2} R_d$ equidistribute on $S^2$ with respect to the normalized rotationally invariant measure $m$, with a power-saving rate of convergence. Using ergodic methods, Linnik [42] had previously established a similar result that required an auxiliary congruence condition on the set of eligible integers $d$. In fact, Linnik showed that his congruence condition could be removed under the assumption of the generalized Riemann hypothesis (GRH), and his method provided a logarithmic rate of convergence under the GRH assumption. The work of Duke and Golubeva-Fomenko can therefore be seen as rendering Linnik's result unconditional and strongly improving the rate of convergence.

In recent years a growing body of work has been devoted to the topic of going beyond uniform distribution of integral points on the sphere and exploring their fine-scale spatial statistics, especially when measured by deviation, variance, and energy estimates [22, 10, 32, 51]. Central to Linnik's approach is the action of the Picard group of the quadratic order of discriminant $-d$ on the set of primitive integral points $R_d$. This paper addresses an ergodic theoretic property of the class group trajectories on these integral points, namely, the *mixing conjecture* of Michel and Venkatesh [43, Conjecture 2], which we now describe. For convenience of exposition, we shall restrict ourselves to the set $\mathbb{D}^\flat$ of *square-free* locally admissible integers.

### 1.1. The mixing conjecture

The set $R_d$ enjoys some natural symmetries coming from the finite rotation group $\mathrm{SO}_3(\mathbb{Z})$. It will be more convenient to work modulo these symmetries, setting

$$\mathcal{R}_d = \Gamma \backslash R_d \quad \text{and} \quad \mathcal{S}^2 = \Gamma \backslash S^2, \tag{1.1}$$

where $\Gamma$ is the unique index 2 subgroup of $\mathrm{SO}_3(\mathbb{Z})$. Let $\mu$ denote the pushforward measure of $m$ under the quotient map $S^2 \to \mathcal{S}^2$. The equidistribution of $d^{-1/2} R_d$ on $(S^2, m)$ is then equivalent to that of $d^{-1/2} \mathcal{R}_d$ on $(\mathcal{S}^2, \mu)$.

A key structural observation, which undergirds both the classical cardinality estimate $|R_d| = d^{1/2+o(1)}$ and Duke's equidistribution theorem, is the existence, for $d > 3$, of a free action on $\mathcal{R}_d$ of the class group $\mathrm{Pic}(\mathcal{O}_E)$ of the ring of integers $\mathcal{O}_E$ of the imaginary quadratic field $E = \mathbb{Q}(\sqrt{-d})$. If $d \equiv 3 \pmod 8$, then $\mathcal{R}_d$ splits into two class group orbits, and when $d \equiv 1, 2 \pmod 4$, the action is transitive. This fact was discovered by Gauß [25] and put into a robust algebraic framework by Venkov [53], using the theory of optimal embeddings of quadratic number fields into quaternion algebras. We may then view $\mathcal{R}_d$, equipped with the uniform probability measure, as a measure-preserving dynamical system under the action of $\mathrm{Pic}(\mathcal{O}_E)$.

In the seminal work [24], Furstenberg introduced a theory of arithmetic operations on dynamical systems, which relies on the following key concept. Given two Borel probability spaces $(X, \mu_X)$ and $(Y, \mu_Y)$ on which an abelian group $S$ acts by measure-preserving transformations, a *joining* between them is an $S$-invariant Borel probability measure on the product space $X \times Y$, whose marginals are $\mu_X$ and $\mu_Y$. Joinings of non-isomorphic systems are related to questions of simultaneous equidistribution [18]. By contrast, a certain class of self-joinings of a single system is related to the ergodic theoretic notion of mixing. Indeed, given $(X, \mu_X)$ as above, and an element $s \in S$, the associated *off-diagonal* self-joining $(X \times X, \mu^{\Delta}_{X,s})$, supported on the graph of $s$, is defined by the rule $\mu^{\Delta}_{X,s}(A, B) = \mu_X(A \cap s^{-1}B)$. With $S$ assumed to be infinite, the transformation $s$ is mixing on $X$ precisely when the sequence of off-diagonals $\{\mu^{\Delta}_{X,s^n}\}_{n\in\mathbb{N}}$ converges to the trivial joining $\mu_X \times \mu_X$.

In the setting of the Picard group action on Linnik points on the sphere, for $d \in \mathbb{D}^{\flat}$ and $[\mathfrak{s}] \in \mathrm{Pic}(\mathcal{O}_E)$, the set

$$\mathcal{R}^{\Delta}_d([\mathfrak{s}]) = \{([x], [\mathfrak{s}].[x]) \mid [x] \in \mathcal{R}_d\}, \tag{1.2}$$

equipped with the diagonal action of the class group $\mathrm{Pic}(\mathcal{O}_E)$, defines an off-diagonal self-joining of $\mathcal{R}_d$. A beautiful conjecture of Michel and Venkatesh [43] states that, although the acting group here is finite, the rescaled sequence $d^{-1/2}\mathcal{R}^{\Delta}_d([\mathfrak{s}])$ should converge to the trivial self-joining $(\mathcal{S}^2 \times \mathcal{S}^2, \mu \times \mu)$, as the size of the group $|\mathrm{Pic}(\mathcal{O}_E)|$, as well as the "complexity" of the ideal class $[\mathfrak{s}]$, go to infinity. To be more precise, let $q$ denote the smallest norm of an integral ideal representing $[\mathfrak{s}]$. The following is the mixing conjecture of the title.

CONJECTURE 1 (Michel-Venkatesh). – *The set $d^{-1/2}\mathcal{R}^{\Delta}_d([\mathfrak{s}])$ equidistributes relative to the product measure $\mu \times \mu$ on $\mathcal{S}^2 \times \mathcal{S}^2$ provided that $q \to \infty$ as $d \to \infty$ along $\mathbb{D}^{\flat}$.*

To better understand the statement of the mixing conjecture, it is helpful to restrict the action of the class group on $\mathcal{R}_d$ to certain monogenic subgroups, as in [22]. Fix an odd prime $p$ and let $\mathbb{D}^{\flat}(p)$ be the subset of $d \in \mathbb{D}^{\flat}$ for which $p$ splits in $E = \mathbb{Q}(\sqrt{-d})$. After choosing a prime ideal $\mathfrak{p}$ lying over $p$, we may then consider the action of $\mathbb{Z}$ on $\mathcal{R}_d$ given by taking integral powers of the fixed ideal class $[\mathfrak{p}] \in \mathrm{Pic}(\mathcal{O}_E)$. For every $d \in \mathbb{D}^{\flat}(p)$ and natural number $n \in \mathbb{N}$ we may consider the set of trajectories $\{([\mathfrak{p}]^i.[x])_{i=0,1,\dots,n} \mid [x] \in \mathcal{R}_d\}$ in $\mathcal{R}_d$. Then $\mathcal{R}^{\Delta}_d([\mathfrak{p}]^n)$, as defined in (1.2), consists of all starting points and their corresponding endpoints. If these trajectories are sufficiently random, the former should retain very little information of the latter. In this set-up one might say that the sequence $\mathcal{R}^{\Delta}_d([\mathfrak{p}]^n)$, $d \to \infty$, with the diagonal $[\mathfrak{p}]^{\mathbb{Z}}$ action is *mixing*, if the rescaled set $d^{-1/2}\mathcal{R}^{\Delta}_d([\mathfrak{p}]^n)$ equidistributes in the product space $(\mathcal{S}^2 \times \mathcal{S}^2, \mu \times \mu)$. A necessary condition for this to hold is that the length of the trajectories should go to infinity with $d \in \mathbb{D}^{\flat}(p)$. This length[(1)] is given by the unique representative $n_{[\mathfrak{p}]}$ in $\{0, \dots, \mathrm{ord}([\mathfrak{p}]) - 1\}$ of the congruence class of $n$ modulo $\mathrm{ord}([\mathfrak{p}])$. In other words, we require $\log_p \mathrm{N}\mathfrak{q} \to \infty$, where $\mathfrak{q} = \mathfrak{p}^{n_{[\mathfrak{p}]}}$ is the integral ideal of smallest norm representing $[\mathfrak{p}^n]$.

Returning to the setting of Conjecture 1, a fundamental obstacle to mixing is the possible existence of low degree Hecke correspondences on which the sets $\mathcal{R}^{\Delta}_d([\mathfrak{s}])$ could accumulate.

(1) Note that the endpoint $[\mathfrak{p}]^n.[x]$ depends on $n$ only through its class modulo the order of $[\mathfrak{p}]$ in $\mathrm{Pic}(\mathcal{O}_E)$.