MOD-GAUSSIAN CONVERGENCE AND THE VALUE DISTRIBUTION OF $\zeta(1/2+it)$ AND RELATED QUANTITIES

E. KOWALSKI AND A. NIKEGHBALI

Abstract. In the context of mod-Gaussian convergence, as defined previously in our work with J. Jacod, we obtain asymptotic formulas and lower bounds for local probabilities for a sequence of random vectors which are approximately Gaussian in this sense, with increasing covariance matrix. This is motivated by the conjecture concerning the density of the set of values of the Riemann zeta function on the critical line. We obtain evidence for this fact, and derive unconditional results for random matrices in compact classical groups, as well as for certain families of L-functions over finite fields.

1. Introduction

It is well-known (see, e.g., [28, Th. 11.9]) that, for $1/2<\sigma<1$, the set of values $\zeta(\sigma+it)$, $t\in\mathbf{R}$, is dense in the complex plane. In fact, much more is true: it was proved by Bohr and Jessen that there exists a Borel probability measure μ_σ on $\mathbf{C}$, such that the support of μ_σ is the whole complex plane, and such that the convergence in law

$$\frac{1}{2T}\int_{-T}^{T} f(\log\zeta(\sigma+it))dt\rightarrow\int_{\mathbf{C}} f(z)d\mu_\sigma(z),$$

holds for $f:\mathbf{C}\rightarrow\mathbf{C}$ continuous and bounded.

The corresponding density question for $\sigma=1/2$ is, however, still open (it was apparently first raised by Ramachandra during the 1979 Durham conference, but seems to appear in print only in Heath-Brown's note in [28, 11.13]): the difficulty is that the values $\zeta(1/2+it)$, $|t|\leqslant T$, do not have a limiting distribution, as evidenced already by the Hardy-Littlewood asymptotic

$$\frac{1}{T}\int_{0}^{T}|\zeta(1/2+it)|^2dt\sim(\log T),\qquad\text{as } T\rightarrow+\infty,$$

or by Selberg's result that $\log|\zeta(1/2+it)|$, $|t|\leqslant T$, is asymptotically normal with variance *growing to infinity* (see also the work of Ghosh [11] for the imaginary part, and [5, §5] for a recent proof). In other words, "most" values of $\zeta(1/2+it)$ are rather large, though the zeta function is zero increasingly often as the imaginary part grows.

In this paper, we show (Corollary 9) how the density of values of zeta on the critical line would follow rather directly from a suitable version of the Keating-Snaith moment conjectures, which we viewed in our previous work with J. Jacod [14] as a refined version of the Gaussian model. In fact, under suitable assumptions, we could prove a quantitative result, bounding from above the smallest $t\geqslant 0$ for which $\zeta(1/2+it)$ lies in a given open disc in $\mathbf{C}$. This argument is based on a very general probabilistic estimate proved in Section 2, which throws some light on the nature of the mod-Gaussian convergence that we defined in [14]. We hope that this result will be of further use. In another paper (jointly with F. Delbaen, see [8, §3.9]), we show that one can weaken considerably the assumption needed in order to prove the density of values of $\zeta(1/2+it)$ (but without quantitative information).

As applications of the general result, we will also prove the following theorems in Section 3 (the precise versions are given there).

2000 *Mathematics Subject Classification.* 11M06, 11T23, 60E10, 60Fxx.

Key words and phrases. Zeta function, L-functions, mod-Gaussian convergence, equidistribution, random matrix theory, characteristic polynomials, Euler products, monodromy.

Theorem 1. *Let $z_0 \in \mathbf{C}^\times$ be arbitrary, $\varepsilon > 0$ such that $\varepsilon \leqslant |z_0|$. There exists $N_0(z_0, \varepsilon)$, which can be bounded explicitly, such that*

$$\mu_N(\{g \in U(N) \mid |\det(1-g) - z_0| < \varepsilon\}) \gg \Big(\frac{\varepsilon}{|z_0|}\Big)^2 \frac{1}{\log N} \tag{1}$$

provided $N \geqslant N_0$, where μ_N denotes probability Haar measure on the unitary group $U(N) \subset GL(N, \mathbf{C})$, and the implied constant is absolute.

Theorem 2. *Define*

$$P_N(t) = \prod_{p \leqslant N} (1 - p^{-1/2-it})^{-1} \tag{2}$$

for $N \geqslant 1$ and $t \in \mathbf{R}$. Let $z_0 \in \mathbf{C}^\times$ be arbitrary, $\varepsilon > 0$ such that $\varepsilon \leqslant |z_0|$. There exists $N_0(z_0, \varepsilon)$, explicitly bounded, such that

$$\liminf_{T \to +\infty} \frac{1}{T} \lambda(\{t \leqslant T \mid P_N(t) \in V\}) \gg \Big(\frac{\varepsilon}{|z_0|}\Big)^2 \frac{1}{\log\log N},$$

for all $N \geqslant N_0$, where λ is the Lebesgue measure and the implied constant is absolute.

In a different direction, we obtain some evidence for the density of $\zeta(1/2 + it)$ by looking at special values of families of L-functions over finite fields. In doing so, we also consider the analogue of Theorem 1 for symplectic and orthogonal matrices. We refer to Section 4 for precise statements and definitions, and only state here one appealing (qualitative) corollary:

Theorem 3. *The set of central values of the L-functions attached to non-trivial primitive Dirichlet characters of $\mathbf{F}_p[X]$, where p ranges over primes, is dense in $\mathbf{C}$.*

Notation. As usual, $|X|$ denotes the cardinality of a set. 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. Similarly, $f \asymp g$ for $x \in X$ means $f \ll g$ and $g \ll f$, both for $x \in X$. We write $(x)_j = x(x+1)\cdots(x+j-1)$ the Pochhammer symbol.

Acknowledgments. The first version of this paper was written while the first author was on sabbatical leave at the Institute for Advanced Study (Princeton, NJ); many thanks are due to this institution for its support. This material is based upon work supported by the National Science Foundation under agreement No. DMS-0635607.

The second author was partially supported by SNF Schweizerischer Nationalfonds Projekte Nr. 200021 119970/1.

Thanks to K. Soundararajan for pointing out that the density conjecture for $\zeta(1/2 + it)$ might be a good problem to study using complex moments of the zeta function, and to R. Heath-Brown for explaining us the history of the question. Many thanks also to N. Katz for discussions and explanations surrounding issues of monodromy computations. Thanks also to F. Delbaen for useful discussions clarifying the underlying probabilistic framework (leading to the paper [8]).

The graphs were produced using Sage 4.2 [26], relying on the Barnes function routines in the mpmath package.

2. Mod-Gaussian convergence and local probabilities

In this section, which is purely probabilistic, we present an asymptotic formula for "local" probabilities in the case of sufficiently uniform mod-Gaussian convergence of sequences of random vectors. This may be compared with the local central limit theorem (see, e.g., [2, §10.4] for the one-dimensional case). In fact, as F. Delbaen pointed out, one can obtain qualitative statements that generalize both the standard local central limit theorem and recover our results below under weaker assumptions (see [8] for many examples). However, our emphasis is on explicit quantitative lower bounds for local probabilities.

We first introduce the definition, generalizing [14] to random vectors. Fix some integer $m \geqslant 1$, and let (X_N) be a sequence of $\mathbf{R}^m$-valued random variables defined on a probability space $(\Omega, \Sigma, \mathbf{P})$ (as is the case for convergence in law, we could work without change with random variables defined on different probability spaces). Let

$$Q_N(t) = Q_N(t_1, t_2, \ldots, t_m)$$

be a sequence of non-negative quadratic forms on $\mathbf{R}^m$. The sequence (X_N) is then said to be convergent in the mod-Gaussian sense with covariance Q_N and limiting function Φ if

$$\lim_{N \to +\infty} \exp(Q_N(t)/2)\,\mathbf{E}(e^{it \cdot X_N}) = \Phi(t) \tag{3}$$

locally uniformly for $t \in \mathbf{R}^m$; Φ is then a function continuous at 0 and $\Phi(0) = 1$. Here, $\cdot$ denotes the standard inner product on $\mathbf{R}^m$.

The intuitive meaning is that, in some sense, X_N is "close" to a (centered) Gaussian vector G_N with covariance matrix Q_N. As in [14], this notion is of most interest if the covariance "goes to infinity". However, in contrast with the case of $m = 1$, this can mean different things because there is more than a single variance parameter involved.

To discuss this, we diagonalize Q_N in an orthonormal basis[1] in the form

$$Q_N(t) = \delta_{1,N} u_1^2 + \cdots + \delta_{m,N} u_m^2, \qquad 0 \leqslant \delta_{1,N} \leqslant \delta_{2,N} \leqslant \cdots \leqslant \delta_{m,N}$$

where $u = H_N(t)$ is the necessary (orthogonal) change of variable. Then "Q_N goes to infinity," in the weakest sense, means that the largest eigenvalue $\delta_{m,N}$ goes to $+\infty$ as $N \to +\infty$.

We are interested in the distribution of values of X_N as N grows; clearly, if (say) the Q_N are already diagonalized in the canonical basis and $\delta_{1,N}$ is constant, these values will have first coordinate much less spread out than the last ones. To simplify our discussion, and because this is the situation in our applications, we will assume this behavior does not occur and that in fact the smallest eigenvalue goes to infinity. For simplicity, we will assume that for some fixed $\mu \geqslant 1$, we have

$$\delta_{m,N} \leqslant \delta_{1,N}^{\mu}, \qquad \delta_{m,N} \to +\infty, \tag{4}$$

so that also $\delta_{1,N} \to +\infty$ (we say that the convergence is *balanced*). In our main applications, this will be the case with $\mu = 1$, which also means that $\delta_{1,N} = \cdots = \delta_{m,N}$ for all N. Note in particular that it follows from (4) that the discriminant

$$\sigma_N = \delta_{1,N} \cdots \delta_{m,N} \geqslant \delta_{1,N}^m$$

goes to infinity as $N \to +\infty$, and moreover

$$\sigma_N \leqslant \delta_{1,N}^{m\mu}. \tag{5}$$

Our basic question is now the following: given (X_N), (Q_N), as above, with this type of mod-Gaussian convergence, can we bound from below the probability

$$\mathbf{P}(X_N \in U),$$

where U is a fixed open set in $\mathbf{R}^m$?

Denoting by $\tilde{Q}_N(x)$ the dual quadratic form, the Gaussian model suggests that, if U is relatively compact (e.g., some non-empty open ball), we could expect

$$\mathbf{P}(X_N \in U) \approx \mathbf{P}(G_N \in U) = \frac{1}{(2\pi)^{m/2}\sqrt{\sigma_N}} \int_U e^{-\tilde{Q}_N(x)/2} dx \sim \frac{\mathrm{Vol}(U)}{(2\pi)^{m/2}\sqrt{\sigma_N}}, \tag{6}$$

as $N \to +\infty$, since $\delta_{1,N} \to +\infty$ implies that $\tilde{Q}_N(x) \to 0$ for all $x \in \mathbf{R}^m$. We will confirm that this holds in certain conditions at least. We strive especially for lower bounds on $\mathbf{P}(X_N \in U)$, which we wish to be quantitative, so that we can determine some N_0 (depending explicitly on U) for which

$$\mathbf{P}(X_{N_0} \in U) > 0.$$

[1] With respect to the standard inner product on $\mathbf{R}^m$.

Note that such a quantitative result must depend on the location of the open set U, whereas the limit itself only depends on the volume, as seen above.

The specific hypothesis we use may seem somewhat arbitrary, but they turn out to be satisfied (with room to spare) in the later applications.

Theorem 4. *Let $m \geqslant 1$ be fixed and let (X_N) be a sequence of $\mathbf{R}^m$-valued random variables defined on $(\Omega, \Sigma, \mathbf{P})$, such that (X_N) converges in the mod-Gaussian sense with covariance (Q_N), and that the convergence is μ-balanced with $\mu \geqslant 1$, with $\sigma_N \geqslant 1$ for all N. Let (G_N) be Gaussian random variables with covariance matrices given by (Q_N), so that*

$$\exp(-Q_N(t)/2) = \mathbf{E}(e^{it\cdot G_N}).$$

Assume moreover the following three conditions:

(1) There exist constants $a > 0$, $\alpha > 0$ and $C > 0$ such that, for any $N \geqslant 1$ and $t \in \mathbf{R}^m$ such that $\|t\| \leqslant \sigma_N^a$, we have

$$\mathbf{E}(e^{it\cdot X_N}) = \Phi(t)\exp(-Q_N(t)/2)\Big\{1 + O\Big(\frac{1}{\exp(\alpha\sigma_N^C)}\Big)\Big\}. \tag{7}$$

(2) The function Φ is of class C^1 on $\{\|t\| < 2\}$.

(3) For some $A \geqslant 1$ and $\beta \geqslant 0$, we have

$$|\Phi(t)| \ll \exp(\beta\|t\|^A), \tag{8}$$

for $t \in \mathbf{R}^m$.

Let $D > 0$ be any number such that

$$D > 2(m + 1 + \max\{a^{-1}, A/C, 3m(m+1)\mu A\}). \tag{9}$$

Then, for any fixed non-empty open box

$$U = \{x \in \mathbf{R}^m \mid \|x - x_0\|_\infty < \varepsilon\} \subset \mathbf{R}^m,$$

with width ε such that $0 < \varepsilon \leqslant 1$, we have

$$\mathbf{P}(X_N \in U) = \mathbf{P}(G_N \in U) + O\Big(\frac{1}{\sigma_N^{1/2+1/D}} + \frac{\varepsilon^{-m}}{\sigma_N}\Big), \tag{10}$$

for $N \geqslant 1$, where the implied constant depends only on (m, Φ, a, α, C) and the implied constant in (7).

In particular, for any fixed non-empty open set $U \subset \mathbf{R}^m$, we have

$$\mathbf{P}(X_N \in U) \gg \frac{1}{\sqrt{\sigma_N}}$$

provided $N \geqslant N_0$, where N_0 and the implied constant depend on U and the same data as above.

Note the following elementary lower bound, valid if $\varepsilon \leqslant 1$:

$$\mathbf{P}(G_N \in U) \gg \frac{\varepsilon^m}{\sqrt{\sigma_N}}\exp\Big(-\frac{\tilde{Q}_N(x_0)}{2}\Big) \tag{11}$$

where the implied constant depends only on m; this is where the location of U enters, since the error term will only be smaller than this, roughly, when $\tilde{Q}_N(x_0) \asymp 1$.

Remark 1. The growth condition (8) is in fact a consequence of the uniform mod-Gaussian convergence, at least provided the sequence (σ_N) does not grow too fast. For instance, if

$$\sigma_{N+1} \leqslant M\sigma_N^B \tag{12}$$

for all $N \geqslant 1$, for some constants $M \geqslant 1$, $B \geqslant 0$, we can obtain (8) with $A = 2 + (B\mu)/(am)$. Indeed, we can write

$$|\Phi(t)| = \Big|\Phi_N(t)e^{Q_N(t)/2}\Big(1 + O\Big(\frac{1}{\exp(\alpha\sigma_N^C)}\Big)\Big)\Big| \leqslant 2e^{Q_N(t)/2}$$

if N is large enough and $\|t\| \leqslant \sigma_N^a$. Note then that

$$Q_N(t) \leqslant \delta_{m,N}\|t\|^2 \leqslant \delta_{1,N}^{\mu}\|t\|^2 \leqslant \sigma_N^{\mu/m}\|t\|^2.$$

We now fix $N \geqslant 1$ minimal such that

$$\sigma_{N-1} \leqslant \|t\|^{1/a} \leqslant \sigma_N,$$

and if this value of N is large enough, we get $\sigma_N \leqslant M\sigma_{N-1}^B \leqslant M\|t\|^{B/a}$, and hence

$$|\Phi(t)| \leqslant 2\exp(\sigma_N^{\mu/m}\|t\|^2) \leqslant 2\exp(M^{\mu/m}\|t\|^{2+(B\mu)/(am)}),$$

as desired. On the other hand, if this chosen N is too small, $\|t\|$ is bounded, and the desired estimate is trivial.

Proof of Theorem 4. Let $\delta_N = \delta_{1,N}$ be the smallest eigenvalue of Q_N, so that $Q_N(t) \geqslant \delta_N\|t\|^2$ for all $t \in \mathbf{R}^m$ and $N \geqslant 1$. For simplicity, we denote also

$$\gamma_N = \exp(\alpha\sigma_N^C), \tag{13}$$

as in (7).

We now first fix w such that $0 < w < 1$, and then fix a smooth, compactly supported function g_0 on $\mathbf{R}$ such that

$$0 \leqslant g_0 \leqslant 1,$$
$$g_0(x) = 0 \text{ for } |x| \geqslant 1, \qquad g_0(x) = 1 \text{ for } |x| \leqslant w,$$
$$|g_0^{(j)}(x)| \ll_j \Delta^j, \text{ for } j \geqslant 0,\ x \in \mathbf{R},$$

where $\Delta = (1-w)^{-1}$ and the implied constant depends only on j (we will define w to be a function of N at the end, and hence must be careful to have estimates uniform in terms of w; this is provided by using only the above properties of g_0; the maximal value of j used will also be bounded only in terms of m, Φ and the data in (7)). It is classical that such a function exists (examples are constructed in [12, §1.4]). Then define

$$f_0(x) = f_0(x_1, \ldots, x_m) = \prod_{1 \leqslant j \leqslant m} g_0(x_j)$$

for $x \in \mathbf{R}^m$. It follows that

$$0 \leqslant f_0 \leqslant 1,$$
$$f_0(x) = 0 \text{ for } \|x\|_\infty \geqslant 1, \qquad f_0(x) = 1 \text{ for } \|x\|_\infty \leqslant w.$$

Next, we define

$$f(x) = f_0\Big(\frac{x - x_0}{\varepsilon}\Big),$$

and we start our argument with the obvious inequality

$$\mathbf{P}(X_N \in U) \geqslant \mathbf{E}(f(X_N)) = \int_{\mathbf{R}^m} f(x)d\nu_N(x)$$

where ν_N is the law of X_N. Applying the Plancherel formula, we get

$$\mathbf{P}(X_N \in U) \geqslant \int_{\mathbf{R}^m} f(x)d\nu_N(x) = \int_{\mathbf{R}^m} \hat{f}(t)\Phi_N(t)dt$$

where $\Phi_N(t) = \mathbf{E}(e^{it\cdot X_N})$ is the characteristic function of X_N and

$$\hat{f}(t) = \frac{1}{(2\pi)^{m/2}}\int_{\mathbf{R}^m} f(x)e^{-it\cdot x}dx$$

denotes the Fourier transform of f (the smoothness of f guarantees that $\hat{f}$ is in L^1, so the Plancherel formula is valid by a simple Fubini argument).

We have

$$\hat{f}(t) = \varepsilon^m e^{-it\cdot x_0}\hat{f}_0(\varepsilon t) = \varepsilon^m e^{-it\cdot x_0}\prod_{1 \leqslant j \leqslant m} \hat{g}_0(\varepsilon t_j), \qquad t \in \mathbf{R}^m.$$

Since

$$\hat{g}_0(t) = \frac{1}{\sqrt{2\pi}} \frac{1}{(it)^j} \int_{\mathbf{R}} g_0^{(j)}(x) e^{-itx} dx$$

for $t \neq 0$ and $j \geqslant 0$ (by repeated integration by parts), we find that

$$|\hat{g}_0(t)| \ll \min(1, \Delta^j |t|^{-j}),$$

the implied constant depending on j.

Using the formula for $\hat{f}(t)$, selecting for given t an index j so that $\|t\|_\infty = |t_j|$ and applying the second upper bound above for this index only, if $|t_j| \geqslant 1$, we derive

$$|\hat{f}(t)| \ll \min(\varepsilon^m, \Delta^{B+m} \varepsilon^{-B} \|t\|_\infty^{-B-m}), \qquad t \in \mathbf{R}^m, \tag{14}$$

for any fixed $B \geqslant 1$, where the implied constant depends only on m and B. In particular, for $\|t\|_\infty \leqslant 1$, we will use simply the upper bound $|\hat{f}(t)| \leqslant \varepsilon^m \|\hat{f}_0\|_\infty \leqslant \varepsilon^m$.

We now proceed to approximate. First of all, for any radius $R_N \geqslant 1$, we can estimate the contribution of those t with $\|t\| > R_N$ using the estimate above with a value of $B \geqslant 1$ which will be determined later. After integrating over $\|t\|_\infty > R_N$, we obtain

$$\int_{\|t\| > R_N} \hat{f}(t) \Phi_N(t) dt \ll \varepsilon^{-B} \Delta^{m+B} R_N^{-B}$$

for any $R_N \geqslant 1$. After selecting $R_N = \sigma_N^{1/B} \geqslant 1$, we obtain

$$\int_{\|t\| > R_N} \hat{f}(t) \Phi_N(t) dt \ll \varepsilon^{-B} \Delta^{m+B} \sigma_N^{-1}, \tag{15}$$

for $N \geqslant 1$, the implied constant depending only on f_0.

On the other hand, provided $B > 1/a$, we use (7) and (8) to get

$$\begin{aligned}
\int_{\|t\| \leqslant R_N} \hat{f}(t) \Phi_N(t) dt &= \int_{\|t\| \leqslant R_N} \hat{f}(t) \Phi(t) \exp(-Q_N(t)/2) \Big\{ 1 + O\Big(\frac{1}{\gamma_N}\Big) \Big\} dt \\
&= \int_{\|t\| \leqslant R_N} \hat{f}(t) \Phi(t) \exp(-Q_N(t)/2) dt + O\Big(\gamma_N^{-1} \int_{\|t\| \leqslant R_N} |\Phi(t) \hat{f}(t)| dt\Big) \\
&= \int_{\|t\| \leqslant R_N} \hat{f}(t) \Phi(t) \exp(-Q_N(t)/2) dt + O(\varepsilon^m \gamma_N^{-1} \exp(\beta R_N^A))
\end{aligned}$$

for $N \geqslant 1$, using again the definition of f, the implied constant depending on Φ.

By (13), the last term can be bounded by

$$\varepsilon^m \gamma_N^{-1} \exp(\beta R_N^A) \ll \varepsilon^m \exp(\beta \sigma_N^{A/B} - \alpha \sigma_N^C) \ll \varepsilon^m \sigma_N^{-1}$$

for $N \geqslant 1$ if $B > A/C$, the implied constant depending on (α, A, B, C).

We then split the first term further in two parts, namely where $Q_N(t) \leqslant \kappa_N^2$, and where $Q_N(t) > \kappa_N^2$. The parameter κ_N will be chosen later, in such a way that the region $\{\|t\| \leqslant 1\}$ (which is inside $\{\|t\| \leqslant R_N\}$) contains the region $Q_N(t) \leqslant \kappa_N^2$ (which is a neighborhood of 0 that contracts to 0 as $N \to +\infty$, if κ_N does not grow too fast, since it is an ellipsoid with longest axis $\kappa_N / \sqrt{\delta_{m,N}}$).

The second part of the integral is bounded by

$$\begin{aligned}
\int_{\|t\| \leqslant R_N,\ Q_N(t) > \kappa_N^2} \hat{f}(t) \Phi(t) e^{-Q_N(t)/2} dt &\ll \varepsilon^m R_N^m \exp(\beta R_N^A - \kappa_N^2/2) \\
&= \varepsilon^m \exp\Big(\frac{m}{B} \log \sigma_N + \beta \sigma_N^{A/B} - \frac{\kappa_N^2}{2}\Big),
\end{aligned}$$

and in the first part, we use the approximation

$$\Phi(t) = 1 + O(\|t\|)$$

for $\{\|t\| \leqslant 1\}$, coming from the C^1 assumption on Φ, to get

$$\int_{Q_N(t)\leqslant\kappa_N^2} \hat{f}(t)\Phi(t)e^{-Q_N(t)/2}dt = \int_{Q_N(t)\leqslant\kappa_N^2} \hat{f}(t)e^{-Q_N(t)/2}dt + O\Big(\int_{Q_N(t)\leqslant\kappa_N^2} |\hat{f}(t)|\|t\|dt\Big)$$
$$= \int_{Q_N(t)\leqslant\kappa_N^2} \hat{f}(t)e^{-Q_N(t)/2}dt + O\Big(\frac{\varepsilon^m\kappa_N^{m+1}}{\sqrt{\delta_N\sigma_N}}\Big), \tag{16}$$

the implied constant depending on Φ, where the last integral was estimated using

$$\|t\|^2 \leqslant \frac{1}{\delta_N}Q_N(t) \leqslant \frac{\kappa_N^2}{\delta_N}, \qquad |t_i| \leqslant \frac{\kappa_N}{\sqrt{\delta_{i,N}}}.$$

We can rewind the computation for the first term, with the Gaussian G_N instead of X_N: for $N \geqslant 1$, we have

$$\int_{Q_N(t)\leqslant\kappa_N^2} \hat{f}(t)e^{-Q_N(t)/2}dt = \mathbf{E}(f(G_N)) + O(\varepsilon^m e^{-\kappa_N^2/2})$$

where the implied constant is absolute, and then we write

$$\mathbf{E}(f(G_N)) = \mathbf{P}(\|G_N - x_0\|_\infty < \varepsilon) + O(\mathbf{P}(w\varepsilon \leqslant \|G_N - x_0\|_\infty < \varepsilon))$$
$$= \mathbf{P}(\|G_N - x_0\|_\infty < \varepsilon) + O(\varepsilon^m(1-w)\sigma_N^{-1/2})$$

for $N \geqslant 1$, where the implied constant depends only on m (the last step is obtained using the density of the Gaussian G_N).

Summarizing, we have found

$$\mathbf{P}(X_N \in U) \geqslant \mathbf{P}(G_N \in U) + O\Big(\frac{\varepsilon^m(1-w)}{\sigma_N^{1/2}} + \frac{\Delta^{m+B}}{\varepsilon^m\sigma_N}$$
$$+ \varepsilon^m \exp\Big(\frac{m}{B}\log\sigma_N + \beta\sigma_N^{A/B} - \frac{\kappa_N^2}{2}\Big) + \frac{\varepsilon^m\kappa_N^{m+1}}{\sqrt{\sigma_N\delta_N}}\Big)$$

(where we recall that $\Delta^{-1} = 1 - w$).

Now if $A/B < 1/(m\mu)$, and

$$\kappa_N = \sigma_N^{A/B},$$

we have first (see (5)) the condition

$$\{Q_N(t) \leqslant \kappa_N^2\} \subset \{\|t\|^2 \leqslant \frac{\kappa_N^2}{\delta_N}\} \subset \{\|t\| \leqslant 1\},$$

and moreover the third error term is absorbed in the second one, while the last becomes

$$\frac{\varepsilon^m\kappa_N^{m+1}}{\sqrt{\sigma_N\delta_N}} \leqslant \varepsilon^m\sigma_N^{-\frac{1}{2}-\frac{1}{2m\mu}+\frac{(m+1)A}{B}}.$$

Thus if we select any $B > \max(a^{-1}, A/C, 3m(m+1)A\mu)$, the previous conditions on B hold, and we find that

$$\mathbf{P}(X_N \in U) \geqslant \mathbf{P}(G_N \in U) + O\Big(\frac{\varepsilon^m(1-w)}{\sigma_N^{1/2}} + \frac{\Delta^{m+B}}{\varepsilon^m\sigma_N} + \frac{\varepsilon^m}{\sigma_N^{1/2+1/(6m\mu)}}\Big). \tag{17}$$

Now, we attempt to select w to equalize the error terms involving it, i.e., so that

$$\frac{\varepsilon^m(1-w)}{\sqrt{\sigma_N}} = \frac{\Delta^{m+B}}{\varepsilon^m\sigma_N},$$

which translates to

$$\Delta = (1-w)^{-1} = (\varepsilon^{2m}\sigma_N^{1/2})^{1/(m+B+1)}$$

and two cases arise:

(i) If $\sigma_N^{1/2} > \varepsilon^{-2m}$, we have $\Delta > 1$ (as is necessary to define w in this way), and we obtain from the above that

$$\mathbf{P}(X_N \in U) \geqslant \mathbf{P}(G_N \in U) + O\Big(\frac{1}{\sigma_N^{1/2+1/D}}\Big),$$

where $D = 2(m+1+B)$ (note that, since A is assumed to be $\geqslant 1$, we have $2(m+B+1) > 6m\mu$.)

(ii) If we have $\sigma_N^{1/2} \leqslant \varepsilon^{-2m}$, we take simply $w = 1/2$ and obtain

$$\frac{\varepsilon^m(1-w)}{\sqrt{\sigma_N}} + \frac{\Delta^{m+B}}{\varepsilon^m \sigma_N} \ll \frac{\varepsilon^{-m}}{\sigma_N},$$

where the implied constant depends on m and B.

The combination of the two cases leads to the lower-bound in (10). The upper bound is proved similarly, using instead of g_0 a function which is $= 1$ for $|x| \leqslant 1$ and $= 0$ for $|x| \geqslant 1+w$ for some suitable $w > 0$; we leave the details to the reader. ☐

Remark 2. If we are interested in obtaining a lower bound only (which is the most interesting aspect in a number of applications), it is simpler and more efficient to fix, e.g., $w = 1/2$, from the beginning of the proof. For

$$U = \{x \in \mathbf{R}^m \mid \|x - x_0\|_\infty < \varepsilon\},$$

this leads for instance to

$$\mathbf{P}(X_N \in U) \geqslant \mathbf{P}(G_N \in U_-) + O\Big(\frac{1}{\sigma_N^{1/2+1/(2m\mu)-\gamma}}\Big) \tag{18}$$

for any $\gamma > 0$ (by taking B large enough depending on γ), where

$$U_- = \{x \in \mathbf{R}^m \mid \|x - x_0\|_\infty < \varepsilon/2\}$$

and the implied constant depends on Φ, (m, a, α, C) and γ.

Remark 3. From the probabilistic point of view, this proposition gives one answer, quantitatively, to the following type of question: given a sequence (X_N) of (real-valued) random variables and parameters $\sigma_N \to +\infty$ such that X_N/σ_N converges in law to a standard centered Gaussian variable (with variance 1), to what extent is X_N itself distributed like a Gaussian with variance σ_N^2?

Here, we perform the comparison by looking at $\mathbf{P}(X_N \in U)$, U a fixed open set. And this shows clear limits to the Gaussian model: for example, any integer-valued random variable X_N will have $\mathbf{P}(X_N \in U) = 0$ for any open set not intersecting $\mathbf{Z}$, and yet may satisfy a Central Limit Theorem (e.g., the N-th step of a symmetric random walk on $\mathbf{Z}$). Even more precisely, denoting

$$d_K(X, Y) = \sup_{x \in \mathbf{R}} |\mathbf{P}(X \leqslant x) - \mathbf{P}(Y \leqslant x)|$$

the Kolmogorov distance, there exist integer-valued random variables X_N with

$$d_K(X_N, G_N) \ll N^{-1/2}, \tag{19}$$

where G_N is a centered Gaussian with variance N, which indicates a close proximity – and yet, again, $\mathbf{P}(X_N \in U) = 0$ if $U \cap \mathbf{Z} = \emptyset$. For instance, take X_N with distribution function $F_N(t) = \mathbf{P}(X_N \leqslant t)$ given by

$$F_N(t) = \mathbf{P}(G_N \leqslant k) \quad \text{for } k \leqslant t < k+1,\ k \in \mathbf{Z}.$$

In particular, it is also impossible to prove results like Theorem 4 using only this type of assumption on the Kolmogorov distance. Of course, if we assume that

$$d_K(X_N, G_N) \ll N^{-1/2}\phi(N)^{-1}, \tag{20}$$

with $\phi(N) \to +\infty$ (arbitrarily slowly), we get

$$\mathbf{P}(X_N \in U) \geqslant \mathbf{P}(G_N \in U) - 2d_K(X_N, G_N) \gg N^{-1/2},$$

for $U = [\alpha, \beta]$, $\alpha < \beta$. But such an assumption is unrealistic in practice. For instance, if one assumes that (X_N) converges in the mod-Gaussian sense with covariance $Q_N(t) = \sigma_N t^2$, and if the limiting function Φ is C^1 and the convergence holds in C^1 topology, one can straightforwardly estimate the Kolmogorov distance[2] by

$$d_K(X_N, G_N) = \sup_{x \in \mathbf{R}} |\,\mathbf{P}(X_N \leqslant x) - \mathbf{P}(G_N \leqslant x)| \ll \sigma_N^{-1/2},$$

which is comparable to (19), but one can also check that this can not be improved in general to something like (20).

In Example 4 in Section 3, we will also describe a much deeper and more illuminating situation concerning the limits of what can be hoped, even with something like mod-Gaussian convergence.

Remark 4. Other variants could easily be obtained. In particular, it is clear from the proof that if Φ has sub-gaussian growth, i.e., we can take $A = 2$ in (8), the results can be substantially improved. However, in our main applications, this condition fails. Also, one could use test functions f which decay at infinity faster than polynomials to weaken the uniformity requirement in the convergence condition (7) (for instance, for $m = 1$, it is possible to find f which is smooth, non-negative and compactly supported in any fixed open interval and satisfies

$$\hat{f}(t) \ll \exp(-|t|^{1-\varepsilon})$$

for any $\varepsilon > 0$, as constructed, e.g., in [12, Th. 1.3.5] or [13]). Again, for our main unconditional applications, our conditions hold with room to spare, so we avoided this additional complexity.

Remark 5. We can also introduce a linear term (corresponding roughly to the expectation of X_N) in addition to the covariance terms in the definition of mod-Gaussian convergence (as in [14] for $m = 1$), but this amounts to saying that (X_N) converges in the mod-Gaussian sense with covariance (Q_N) and mean (ξ_N), $\xi_N \in \mathbf{R}^m$, if the sequence $(X_N - \xi_N)$ converges in our original sense above. But note that the interpretation of a lower bound for $\mathbf{P}(X_N - \xi_N \in U)$, as given by Theorem 4 for a fixed $U \subset \mathbf{R}^m$, is quite different, if ξ_N is itself “large”. Maybe one should see the statements in that case as giving natural examples of sets U_N for which one knows that $\mathbf{P}(X_N \in U_N)$ has the specific decay behavior $\sigma_N^{-1/2}$ as $N \to +\infty$.

In particular, lower bounds for $\mathbf{P}(X_N - \xi_N \in U)$ do not give control of $\mathbf{P}(X_N \in U)$, and indeed this may be zero for all N large enough (see, for instance the example in Section 4.2 below of values at 1 of characteristic polynomials of unitary symplectic matrices, which is always $\geqslant 0$).

3. Random unitary matrices and the zeta function

We present now some applications of Theorem 4 (in particular, proving Theorems 1 and 2). We also give an example that illustrates the limitations of such results, suggesting strongly that one can not replace mod-Gaussian convergence with the existence of the limits (3) only for t in a neighborhood of the origin.

Example 1. One of the canonical motivating examples of mod-Gaussian convergence is due to Keating and Snaith [20], and this leads to Theorem 1. We switch however to a probabilistic notation to follow more closely the setting of the previous section. Thus, we let

$$X_N = \log \det(1 - T_N),$$

where T_N is a Haar-distributed random unitary matrix in the compact group $U(N)$. We view these random variables as $\mathbf{R}^2$-valued (via the real and imaginary parts), so if $t = (t_1, t_2)$, we have

$$t \cdot X_N = t_1 \operatorname{Re}(X_N) + t_2 \operatorname{Im}(X_N). \tag{21}$$

[2] Using the Berry-Esseen inequality, see e.g. [27, §7.6].

We first clarify the choice of the branch of logarithm: X_N is defined almost everywhere (when 1 is not an eigenvalue of T_N), and for a matrix $g \in U(N)$ with $\det(1-g) \neq 0$, such that

$$\det(1-Tg) = \prod_{1 \leqslant j \leqslant N} (1-\alpha_j T), \qquad |\alpha_j| = 1,$$

we define

$$\log\det(1-g) = \lim_{\substack{r\to 1\\ r<1}} \log\det(1-rg) = \sum_{1\leqslant j\leqslant N} \lim_{\substack{r\to 1\\ r<1}} \log(1-r\alpha_j),$$

where the last logarithms are given by the Taylor expansion around 0. This is the same convention as in [20, par. after (7)].

Keating and Snaith show that (X_N) satisfies

$$\mathbf{E}(e^{it\cdot X_N}) = \prod_{1\leqslant j\leqslant N} \frac{\Gamma(j)\Gamma(j+it_1)}{\Gamma(j+\frac{1}{2}(it_1+t_2))\Gamma(j+\frac{1}{2}(it_1-t_2))} \tag{22}$$

for $t=(t_1,t_2)\in\mathbf{R}^2$ (note the asymmetry between it_1 and t_2), see [20, eq. (71)], taking into account a slightly different normalization: their t is our it_1 and their s is our t_2. It is also useful to observe that, in the connection with Töplitz determinants (see [4]), this characteristic function is the N-th Töplitz determinant corresponding to the symbol which is a pure Fisher-Hartwig singularity of type

$$b(e^{i\theta}) = (2-2\cos\theta)^{it_1/2}\exp(i(\theta-\pi)t_2/2), \qquad 0<\theta<2\pi$$

(this is denoted

$$t_{t_2/2}(e^{i\theta})u_{it_1/2}(e^{i\theta}) = \xi_{(it_1-t_2)/2}(e^{i\theta})\eta_{(it_1+t_2)/2}(e^{i\theta})$$

in [9], where the formula (22) is stated as Eq. (41); see [6] for two elementary computations of the corresponding Töplitz determinants.)

We rewrite this in terms of the Barnes function $G(z)$, as is customary. We recall (see, e.g., [3]) that G is an entire function of order 2, such that $G(1)=1$ and $G(z+1)=\Gamma(z)G(z)$ for all z, and that its zeros are located at the negative integers. In particular, it satisfies

$$\prod_{j=1}^{N}\Gamma(j+\theta) = \frac{G(1+N+\theta)}{G(1+\theta)} \tag{23}$$

for all $N\geqslant 1$ and $\theta\in\mathbf{C}$.

Thus, we have

$$\begin{aligned}\mathbf{E}(e^{it\cdot X_N}) = \prod_{1\leqslant j\leqslant N}\frac{\Gamma(j)\Gamma(j+it_1)}{\Gamma(j+\frac{it_1+t_2}{2})\Gamma(j+\frac{it_1-t_2}{2})} &= \frac{G(1+\frac{it_1-t_2}{2})G(1+\frac{it_1+t_2}{2})}{G(1+it_1)}\\ &\quad\times\frac{G(1+it_1+N)G(1+N)}{G(1+\frac{it_1-t_2}{2}+N)G(1+\frac{it_1+t_2}{2}+N)}\end{aligned}$$

(see, e.g., [9, eq. (41)]). We now get from [9, Cor. 3.2] that

$$\begin{aligned}\mathbf{E}(e^{it\cdot X_N}) &\sim N^{(it_1-t_2)(it_1+t_2)/4}\frac{G(1+\frac{it_1-t_2}{2})G(1+\frac{it_1+t_2}{2})}{G(1+it_1)}\\ &= \exp(-Q_N(t)/2)\frac{G(1+\frac{it_1-t_2}{2})G(1+\frac{it_1+t_2}{2})}{G(1+it_1)},\end{aligned}$$

where

$$Q_N(t_1,t_2) = \delta_N(t_1^2+t_2^2), \qquad \delta_N = \tfrac{1}{2}\log N,$$

hence we have complex mod-Gaussian convergence with limiting function

$$\Phi_g(t_1,t_2) = \frac{G(1+\frac{it_1-t_2}{2})G(1+\frac{it_1+t_2}{2})}{G(1+it_1)}. \tag{24}$$

Here we can take $\mu=1$ in (4).

Remark 6. Note that this is *not* the product of the two individual limiting functions for mod-Gaussian convergence of the real and imaginary parts of X_N separately (which are $\Phi_g(t_1,0)$ and $\Phi_g(0,t_2)$), although after normalizing, one obtains convergence in law of

$$(\mathrm{Re}(X_N)/\sqrt{\delta_N}, \mathrm{Im}(X_N)/\sqrt{\delta_N})$$

to *independent* standard Gaussian variables, as noted by Keating and Snaith.

We now check that Theorem 4 can be applied to the sequence of random variables (X_N). The fact that Φ_g is of class C^1 on $\mathbf{R}^2$ is clear in view of the analytic properties of the Barnes function. Condition (3) is also obvious. A uniformity estimate like (7) is not found in [20] or [9], though it is proved for t in a fixed compact region of $\mathbf{R}^2$ in [9, Cor. 3.2]. In Proposition 17 in the Appendix, we prove

$$\Phi_N(t) = \Phi(t)e^{-Q_N(t)/2}\Big(1 + O\Big(\frac{1+\|t\|^3}{N}\Big)\Big)$$

for $\|t\| \leqslant N^{1/6}$. In view of $\sigma_N = (\log N)^2/4$, this is compatible with (7) and (13), with a arbitrarily large, $C = \frac{1}{2}$ and A (defined by (8)) can be taken to be any $A > 2$. Thus the constant D in (10) can be any number

$$D > 2(3 + \max(4, 36)) = 78.$$

Moreover, since

$$\tilde{Q}_N(x_1, x_2) = \frac{x_1^2 + x_2^2}{\frac{1}{2}\log N},$$

we see by using Remark 2 (namely, (18)) and (11) that we have the following corollary:

Corollary 5. *For $0 < \varepsilon < 1$ we have*

$$\mathbf{P}(|X_N - z_0| < \varepsilon) \gg \varepsilon^2 (\log N)^{-1} \tag{25}$$

for all N with

$$N \gg \max\{\exp(|z_0|^2), \exp(C\varepsilon^{-9})\}$$

where both implied constants are absolute.

(The first condition on N ensures the main term is $\gg \varepsilon^2(\log N)^{-1}$, while the second ensures that the error term is smaller; we have taken $2/9 = 1/(2m\mu) - \gamma = 1/4 - 1/36$ for definiteness; any number > 8 can replace 9).

Now we appeal to the following elementary lemma:

Lemma 6. *Let $z_0 \in \mathbf{C}^\times$ and $\varepsilon > 0$, and denote*

$$w_0 = \log|z_0| + i\theta_0, \qquad \theta_0 = \mathrm{Arg}(z_0) \in]-\pi, \pi].$$

Then, provided $\varepsilon \leqslant |z_0|$, we have

$$|e^w - z_0| < \varepsilon$$

for all $w \in \mathbf{C}$ such that

$$|w - w_0| < \frac{\varepsilon}{2|z_0|}.$$

For given $z_0 \in \mathbf{C}$, non-zero, we get from this and from (25), applied to $\log|z_0| + i\,\mathrm{Arg}(z_0)$ and to $\varepsilon/|z_0|$ instead of ε, the following explicit form of Theorem 1:

Theorem 7. *Let $z_0 \in \mathbf{C}^\times$ be arbitrary, $\varepsilon > 0$ such that $\varepsilon \leqslant |z_0|$. We have*

$$\mu_N(\{g \in U(N) \mid |\det(1-g) - z_0| < \varepsilon) = \mathbf{P}(|\det(1 - T_N) - z_0| < \varepsilon) \gg \Big(\frac{\varepsilon}{|z_0|}\Big)^2 \frac{1}{\log N}$$

for $N \geqslant N_0(z_0, \varepsilon)$, where

$$N_0(z_0, \varepsilon) \ll \max\Big\{\exp\big((\log|z_0|)^2\big), \exp\Big(C\Big(\frac{\varepsilon}{2|z_0|}\Big)^{-9}\Big)\Big\}$$

and C and the implied constants are absolute.

Remark 7. It follows from the asymptotic formulas for the Barnes function (due to Barnes [3, §15], see also, e.g., [10]) that

$$\tfrac{1}{\|t\|^2}\log|\Phi_g(t)| \asymp \log(2\|t\|),$$

which is illustrated in Figure 1. This super-gaussian behavior is the main cause of difficulty in the proof of Theorem 4.

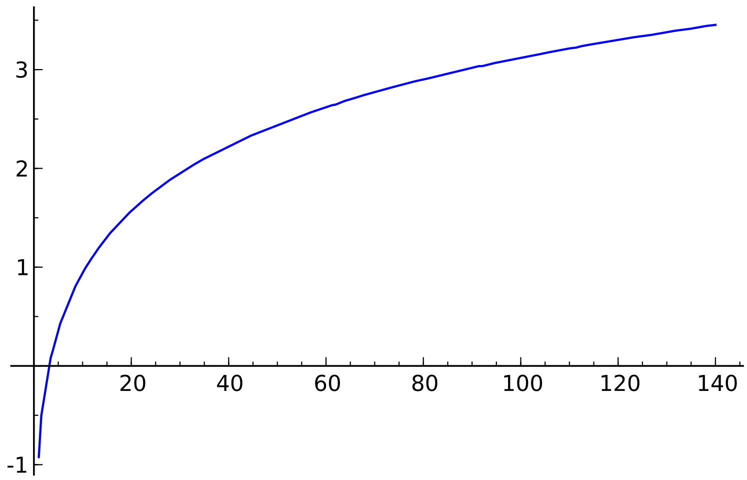

FIGURE 1. Graph of $\frac{1}{t_2^2}\log|\Phi_g(1,t_2)|$, $1 \leqslant t_2 \leqslant 140$

Remark 8. Note that if one only wants to say that $\det(1-T_N)$, for N growing, has dense image in $\mathbf{C}$, much simpler topological arguments suffice.

Example 2. Another conspicuous example of mod-Gaussian convergence is the arithmetic Euler factor in the moment conjecture for $\zeta(1/2+it)$. In [14, §4.1], we considered this factor for the real part $\log|\zeta(\frac{1}{2}+it)|$ only, and we first generalize this as in the previous section.

Consider a sequence (X_p) of independent random variables uniformly distributed on the unit circle and indexed by prime numbers, and let

$$L_N = -\sum_{p\leqslant N}\log(1-p^{-1/2}X_p)$$

where the logarithm is given here by the Taylor expansion around 0. For each individual term $E_p = -\log(1-p^{-1/2}X_p)$, we have

$$\mathbf{E}(e^{it\cdot E_p}) = \frac{1}{2\pi}\int_0^{2\pi}(1-ae^{i\theta})^{-\frac{1}{2}(t_2+it_1)}(1-ae^{-i\theta})^{\frac{1}{2}(t_2-it_1)}d\theta$$

with $a=p^{-1/2}$. Expanding by the binomial theorem and picking up the constant term in the expansion in Fourier series, we obtain

$$\begin{aligned}\mathbf{E}(e^{it\cdot E_p}) &= \sum_{j\geqslant 0} a^{2j}\binom{-\frac{1}{2}(t_2+it_1)}{j}\binom{\frac{1}{2}(t_2-it_1)}{j}\\ &= \sum_{j\geqslant 0}\frac{(\frac{1}{2}(t_2+it_1))_j(\frac{1}{2}(it_1-t_2))_j}{(j!)^2}a^{2j}\\ &= {}_2F_1(\tfrac{1}{2}(it_1+t_2),\tfrac{1}{2}(it_1-t_2);1;a^2)\end{aligned}$$

in terms of the Gauss hypergeometric function.

Arguing as in [14], we see now that

$$\mathbf{E}(e^{it\cdot L_N}) = \prod_{p\leqslant N} {}_2F_1(\tfrac{1}{2}(it_1+t_2), \tfrac{1}{2}(it_1-t_2); 1; p^{-1})$$
$$= \prod_{p\leqslant N} \Bigl(1 - \frac{t_1^2+t_2^2}{4}\frac{1}{p} + O\Bigl(\frac{1}{p^2}\Bigr)\Bigr),$$

and hence, denoting

$$\delta_N = -\frac{1}{2}\sum_{p\leqslant N}\log(1-p^{-1}) \sim \frac{1}{2}\log\log N, \qquad Q_N(t) = \delta_N(t_1^2+t_2^2) = \delta_N\|t\|^2,$$

we get

$$\mathbf{E}(e^{it\cdot L_N}) \sim \exp(-Q_N(t)/2)\Phi_a(t),$$

as $N\to+\infty$, with limiting function

$$\Phi_a(t) = \prod_p \Bigl(1-\frac{1}{p}\Bigr)^{-\|t\|^2/4} {}_2F_1(\tfrac{1}{2}(it_1+t_2), \tfrac{1}{2}(it_1-t_2); 1; p^{-1}). \tag{26}$$

We have here also $\mu = 1$ in (4). Now, to check the uniformity required in (7), we write

$$\mathbf{E}(e^{it\cdot L_N}) = \exp(-Q_N(t)/2)\Phi_a(t)R_N(t)$$

with

$$R_N(t) = \prod_{p>N} \Bigl(1-\frac{1}{p}\Bigr)^{-\|t\|^2/4} {}_2F_1(\tfrac{1}{2}(it_1+t_2), \tfrac{1}{2}(it_1-t_2); 1; p^{-1}).$$

If we expand the p-factor using the binomial theorem, we obtain

$$1 + \sum_{j\geqslant 2}\frac{1}{p^j}\sum_{a+b=j}\frac{(\frac{1}{2}(it_1+t_2))_a(\frac{1}{2}(it_1-t_2))_a}{(a!)^2}\binom{-\|t\|^2/4}{b},$$

and if we assume that $\|t\|\leqslant A$ with $A\geqslant 1$, crude bounds show that this p-factor is

$$1 + O\Bigl(\sum_{j\geqslant 2}\frac{jA^{2j}}{p^j}\Bigr),$$

where the implied constant is absolute, so that if $\|t\|\leqslant N^{1/8}$, for instance, we get

$$R_N(t) = \prod_{p>N}\Bigl(1 + O\Bigl(\sum_{j\geqslant 2} jp^{-3j/4}\Bigr)\Bigr) = 1 + O(N^{-1/2}).$$

Although this is crude, it already gives much more than (7), both in terms of range of uniformity and sharpness of approximation.

Since Condition (3) is also obviously valid here, Theorem 4 (or rather (18)) applies with A any real number > 2, a and C arbitrarily large, and shows that

$$\mathbf{P}(|L_N - z_0| < \varepsilon) \gg \varepsilon^2(\log\log N)^{-1}$$

for any $z_0\in\mathbf{C}$ and $\varepsilon < 1$, provided

$$N \gg \max\Bigl(\exp(\exp(|z_0|^2)), \exp(\exp(C\varepsilon^{-9}))\Bigr)$$

for some large constant $C\geqslant 1$.

From this we deduce easily the more arithmetic-looking statement of Theorem 2. Indeed, let $P_N(t)$ be given by (2). For fixed N, it is well-known that the random variables $t\mapsto P_N(t)$ on the probability spaces $([0,T], T^{-1}\lambda)$ converge in law, as $T\to+\infty$, to

$$\tilde{P}_N = \prod_{p\leqslant N}(1-p^{-1/2}X_p)^{-1} = \exp(L_N),$$

where X_p are as above (independent and uniformly distributed on the unit circle; the independence is due to the fundamental theorem of arithmetic). For any open set V,[3] it follows that

$$\liminf_{T\to+\infty} \frac{1}{T}\lambda(\{t \leqslant T \mid P_N(t) \in V\}) \geqslant \mathbf{P}(\tilde{P}_N \in V).$$

Applying Lemma 6 as in the proof of Theorem 7, we obtain Theorem 2 with

$$N_0(z_0,\varepsilon) \ll \max\Big\{\exp\Big(\exp\Big((\log|z_0|)^2\Big)\Big), \exp\Big(\exp\Big(C\Big(\frac{\varepsilon}{2|z_0|}\Big)^{-9}\Big)\Big)\Big\}$$

for some absolute constant C.

Remark 9. Again, the density of values of $P_N(t)$ for $N \geqslant 1$ and $t \in \mathbf{R}$ (or of $\tilde{P}_N$, which amounts to the same thing) is an easier matter that can be dealt with using topological tools.

Example 3. The two previous examples are of course motivated by their conjectural relation with the behavior of the Riemann zeta function on the critical line (this is the arithmetic essence of [20]). Indeed, Keating and Snaith conjecture that:

Conjecture 8. *Define* $\log\zeta(1/2+iu)$*, when* $u \in \mathbf{R}$ *is not the ordinate of a non-trivial zero of* $\zeta(s)$*, by continuation along the horizontal line* $\mathrm{Im}(s) = u$*, with limit* 0 *when* $\mathrm{Re}(s) \to +\infty$*.*

For any $t = (t_1, t_2) \in \mathbf{R}^2$*, we have*

$$\frac{1}{T}\int_0^T e^{it\cdot\log\zeta(1/2+iu)}du = \Phi_a(t)\Phi_g(t)\exp\Big(-\frac{|t|^2}{4}(\log\log T)\Big)(1+o(1))$$

as $T \to +\infty$*, where* $\cdot$ *is the inner product on* $\mathbf{R}^2$ *as in* (21)*.*

Hence, we see in particular that the following holds:

Corollary 9. *Assume there exist* $\alpha > 0$*,* $\delta > 0$ *and* $\theta > 0$ *such that Conjecture* 8 *holds with the error term* $o(1)$ *replaced by*

$$\exp(-\alpha(\log\log T)^\delta)$$

uniformly for $\|t\| \leqslant (\log\log 6T)^\theta$*. Then the set of values* $\zeta(1/2+it)$ *is dense in the complex plane. In fact, there exists* $C > 0$*,* $D \geqslant 0$*, such that, for any* $z_0 \in \mathbf{C}^\times$ *and* $\varepsilon \leqslant |z_0|$*, there exists* t *with*

$$0 \leqslant t \ll \max\Big\{\exp(\exp((\log|z_0|)^2)), \exp\Big(\exp\Big(C\Big(\frac{\varepsilon}{2|z_0|}\Big)^{-D}\Big)\Big)\Big\},$$

such that

$$|\zeta(\tfrac{1}{2}+it) - z_0| < \varepsilon.$$

Of course, such a strong conjecture concerning the imaginary moments of $\zeta(1/2+it)$ looks quite hopeless at the current time: there is no known non-trivial result available, even assuming the Riemann Hypothesis. But Example 4 below suggests that (with this approach) it is indeed necessary to require that the characteristic function converge uniformly for t in a region growing with T. In [8, §3.9], jointly with F. Delbaen, we explain how the general limit statement

$$\lim_{T\to+\infty} \frac{\frac{1}{2}\log\log T}{T}\lambda(\{u \in [0,T] \mid \log\zeta(\tfrac{1}{2}+iu) \in V\}) = \frac{\lambda(U)}{2\pi}.$$

for a fixed open set $V \subset \mathbf{C}$ with boundary of measure zero (which of course gives a positive answer to Ramachandra's question) can be proved under much weaker assumptions than a uniform version of Conjecture 8.

---

[3] Because we do not know if the probability that $\tilde{P}_N$ is in the boundary of V is zero or not, we do not claim – or need to claim – an equality; see, e.g., [1, Th. 2.1, (iv)].

Remark. Another remark concerning Conjecture 8 has to do with the factored form of the limiting function $\Phi_a(t)\Phi_g(t)$, which seems to imply some asymptotic independence property. Recall that the real and imaginary parts of Φ_a and Φ_g are themselves asymptotically independent *after renormalization*, but are not products of the limiting functions for the two parts separately. So Conjecture 8, if correct, is evidence of quite particular probabilistic behavior.[4]

Example 4. Our assumptions in Theorem 4 are probably not optimal. We now describe an illuminating (counter)-example in the direction of understanding when a result like this could be true.

We again look at random matrices T_N in the compact group $U(N)$ (as in Example 1), but this time we consider the random variables counting the number of eigenvalues in certain fixed arcs of the unit circle: fix $\gamma \in]0, 1/2[$, and let

$$I = \{e^{2i\pi\theta} \mid |\theta| \leqslant \gamma\} \subset \mathbf{C}.$$

Then let X_N be the number of eigenvalues ϑ of T_N such that $\vartheta \in I$. Note that X_N is an integer-valued random variable. It was proved by Costin and Lebowitz that

$$\frac{X_N - 2\gamma N}{\pi^{-1}\sqrt{\log N}}$$

converges in law to a standard normal random variable. Wieand [29] gave a proof[5] based on asymptotics of Töplitz determinants with discontinuous symbols; as noted by Basor, this gives the asymptotic

$$\mathbf{E}(e^{it(X_N-2\gamma N)}) \sim \exp\Bigl(-\frac{t^2}{2}\frac{1}{\pi^2}\log N\Bigr)(2-2\cos 4\pi\gamma)^{\frac{t^2}{4\pi^2}} G\Bigl(1-\frac{t}{2\pi}\Bigr)G\Bigl(1+\frac{t}{2\pi}\Bigr)$$

as $N \to +\infty$, for all t *with* $|t| < \pi$ (see, e.g., [9, Th. 5.47], applied with $N = 2$, $\alpha_1 = \alpha_2 = 0$, $\beta_1 = \frac{t}{2\pi}$, $\beta_2 = -\frac{t}{2\pi}$, and the condition on t is equation (5.79) in loc. cit., or [4, p. 331]). This asymptotic is of course of the form (3) for these values of t, but the restriction $|t| < \pi$ is necessary, since the characteristic function of X_N is 2π-periodic for all N. The convergence is sufficiently uniform for t close to 0 to allow the deduction of the renormalized normal behavior (as Wieand did, using the Laplace transform instead of the characteristic function), but when γ is rational, the set of possible values of $X_N - 2\gamma N$ for $N \geqslant 1$ is a discrete set in $\mathbf{R}$.[6]

4. Distribution of central values of L-functions over finite fields

We now consider examples related to L-functions over finite fields. Our main input will be deep results of Deligne and Katz, and we are of course motivated by the philosophy of Katz and Sarnak [19].

The goal is to make statements about the distribution of values at the central point 1/2 of L-functions over finite fields. The appealing aspect is that these form discrete sets, hence proving that they are dense in $\mathbf{C}$ (as in Theorem 3), for instance, is obviously interesting and meaningful. We consider examples of our results for the three basic symmetry types in turn: unitary, symplectic, and orthogonal. For the last two, this means first obtaining a suitable analogue of Example 1. The corresponding limiting functions have already been studied in some respect by Keating-Snaith [21] and Conrey-Farmer [7], though our expressions seem somewhat more natural.

---

[4] The fourth moment of $\zeta(1/2+it)$ and a few other results do provide evidence of a factored limiting function, with "random matrix" term split from the Euler factor. The mod-Poisson analogy is also consistent with this, in the case of the number of prime factors of an integer, as discussed in detail in [25, §4, 5, 6].

[5] Including a more general result concerning the joint distribution of the number of eigenvalues in more than one interval.

[6] For what it's worth, one may mention that the density of values $X_N - 2\gamma N$ is true for irrational γ, by Dirichlet's approximation theorem, and by the existence of matrices in $U(N)$ where the number of eigenvalues in I takes any value between 0 and N.

4.1. **Unitary symmetry.** Let $\mathbf{F}_q$ be a finite field with q elements. Unitary symmetry arises (among other cases) for certain types of one-variable exponential sums over finite fields, which are associated to Dirichlet characters of $\mathbf{F}_q[X]$. These will lead to a proof of Theorem 3.

Let $\mathbf{F}_q$ be a finite field with q elements of characteristic $p \neq 0$. A *Dirichlet character* modulo $g \in \mathbf{F}_q[X]$ is a map

$$\eta : \mathbf{F}_q[X] \to \mathbf{C},$$

defined by

$$\eta(f) = \begin{cases} 0 & \text{if } f \text{ and } g \text{ are not coprime} \\ \underline{\eta}(f) & \text{otherwise,} \end{cases}$$

where $\underline{\eta}$ is a group homomorphism

$$\underline{\eta} : (\mathbf{F}_q[X]/g\mathbf{F}_q[X])^\times \longrightarrow \mathbf{C}^\times.$$

This character is non-trivial if $\underline{\eta} \neq 1$, and primitive if it can not be defined (in the obvious way) modulo a proper divisor of g. The associated L-function is defined by the Euler product

$$L(s, \eta) = \prod_\pi (1 - \eta(\pi)|\pi|^{-s})^{-1},$$

for $s \in \mathbf{C}$, where the product ranges over monic irreducible polynomials in $\mathbf{F}_q[X]$ and $|\pi| = q^{\deg(\pi)}$. One shows quite easily that this is in fact a polynomial (which we denote $Z(\eta, T)$) in the variable $T = q^{-s}$ of degree $\deg(g) - 1$, if η is primitive modulo g and non-trivial.

The examples used in proving Theorem 3 arise from the following well-known construction. For any integer $d \geqslant 1$, with $p \nmid d$, any non-trivial multiplicative character

$$\chi : \mathbf{F}_q \to \mathbf{C}^\times$$

such that $\chi^d \neq 1$, and any squarefree polynomial $g \in \mathbf{F}_q[X]$ of degree d, we let

$$S(\chi, g) = \sum_{x \in \mathbf{F}_q} \chi(g(x)),$$

where $\chi(0)$ is defined to be 0. These are multiplicative exponential sums, and have been studied intensively, due in part to their many applications to analytic number theory (for their generalizations to multiple variables, see the paper [15] of Katz).

It is also well-known that one can construct a non-trivial Dirichlet character $\eta = \eta(g, \chi)$, primitive modulo g, such that

$$Z(\eta, T) = \exp\Bigl(\sum_{m \geqslant 1} \frac{S_m(\chi, g)}{m} T^m\Bigr),$$

where $S_m(\chi, g)$ denotes the "companion" sums over extensions of $\mathbf{F}_q$, namely

$$S_m(\chi, g) = \sum_{x \in \mathbf{F}_{q^m}} \chi(N_{\mathbf{F}_{q^m}/\mathbf{F}_q}(g(x))),$$

where $N_{\mathbf{F}_{q^m}/\mathbf{F}_q}$ is the norm map. We will denote $L(s, g, \chi)$ the corresponding L-function.

Moreover, we have the Riemann Hypothesis for these L-functions (due to A. Weil), which gives the link with random unitary matrices: there exists a unique conjugacy class $\theta_{\chi,g}(q)$ in the unitary group $U(d-1)$ such that

$$L(s + \tfrac{1}{2}, g, \chi) = \det(1 - q^{-s}\theta_{\chi,g}(q)),$$

(so that, in particular, we recover the Weil bound

$$|S(\chi, g)| \leqslant (d-1)q^{1/2},$$

by looking at the trace of $\theta_{\chi,g}(q)$). For all this, one can see, for instance, [24, §4.2], which contains a self-contained account.

We will first prove the following theorem, which is clearly a stronger form of Theorem 3 in view of the preceding remarks:

Theorem 10. *For $d \geqslant 1$ and $t \in \mathbf{Z}$, let $g_{d,t} = X^d - dX - t \in \mathbf{Z}[X]$. For p prime, let $X(p)$ denote the set of pairs (χ, t) where χ is non-trivial character of $\mathbf{F}_p$ and $t \in \mathbf{F}_p$.*

Let $z_0 \in \mathbf{C}^\times$ and $\varepsilon > 0$ with $\varepsilon \leqslant |z_0|$ be given. For all integers $d \geqslant d_0(z_0, \varepsilon)$, we have

$$\liminf_{p \to +\infty} \frac{|\{(\chi, t) \in X(p) \mid \chi^d \neq 1, |L(\frac{1}{2}, g_{d,t}, \chi) - z_0| < \varepsilon\}|}{|X(p)|} \gg \Bigl(\frac{\varepsilon}{|z_0|}\Bigr)^2 \frac{1}{\log d},$$

where

$$d_0(z_0, \varepsilon) \ll \max\Bigl\{\exp\bigl((\log |z_0|)^2\bigr), \exp\Bigl(C\Bigl(\frac{\varepsilon}{|z_0|}\Bigr)^{-9}\Bigr)\Bigr\},$$

where $C \geqslant 0$ and the implied constants are absolute.

This result depends on the mod-Gaussian convergence for characteristic polynomials on $U(N)$ (i.e., on Example 1). Indeed, denoting by $U(N)^\sharp$ the space of conjugacy classes in $U(N)$, we have the following:

Theorem 11. *For any integer $d > 5$, any odd prime p with $p \nmid d(d-1)$, the conjugacy classes*

$$\{\theta_{\chi, g_{d,t}}(p) \mid \chi \,(\mathrm{mod}\, p),\ \chi \neq 1,\ \text{and } t \in \mathbf{F}_p \text{ with } t^{d-1} - (1-d)^{d-1} \neq 0 \,(\mathrm{mod}\, p)\}$$

become equidistributed in $U(d-1)^\sharp$ as $p \to +\infty$, with respect to Haar measure.

Proof. This is an easy consequence of results of Katz (see [16, Th. 5.13]), the only "twist" being the extra averaging over all non-trivial Dirichlet characters to obtain unitary instead of special unitary (or similar) equidistribution.

First of all, it is easy to check that if $p \nmid d(d-1)$ and $t \in \mathbf{F}_p$ is such that $t^{d-1} \neq (1-d)^{d-1}$, the polynomial $g_{d,t} = X^d - dX - t \in \mathbf{F}_p[X]$ is a squarefree "weakly-supermorse" polynomial, in the sense of [16, §5.5.2], i.e., its degree is invertible in $\mathbf{F}_p$, it has d distinct zeros, its derivative has $d-1$ distinct zeros and the values of f at those critical points are distinct. In particular, the conjugacy classes in the statement are well-defined.

For simplicity, denote $\mathcal{U}$ the open subset of the affine t-line where $t^{d-1} \neq (1-d)^{d-1}$. Then, according to the Weyl equidistribution criterion, we must show that

$$\lim_{p \to +\infty} \frac{1}{p-2} \sideset{}{^*}\sum_{\chi \,(\mathrm{mod}\, p)} \frac{1}{|\mathcal{U}(\mathbf{F}_p)|} \sum_{t \in \mathcal{U}(\mathbf{F}_p)} \mathrm{Tr}\, \Lambda(\theta_{\chi, g_{d,t}}(p)) = 0.$$

for any (fixed) non-trivial irreducible unitary representation Λ of the compact group $U(d-1)$.

We isolate in the sum those characters χ where $\chi^{2d} = 1$: there are at most $2d$ of them. For any other character $\chi \,(\mathrm{mod}\, p)$, the inner sum over $t \in \mathcal{U}(\mathbf{F}_p)$ is of the type handled by the Deligne Equidistribution Theorem. Let $k = k(\chi)$ be the order of the Dirichlet character $\chi\chi_2$, where χ_2 is the real character modulo p. By [16, Th. 5.13, (2)] (the restriction $\chi^{2d} \neq 1$ ensures the assumptions hold), provided $p \nmid d(d-1)$, e.g., $p > d(d-1)$, the relevant geometric monodromy group is equal to

$$GL_k(d-1) = \{g \in GL(d-1) \mid \det(g)^k = 1\},$$

with maximal compact subgroup

$$U_k(d-1) = \{g \in U(d-1) \mid \det(g)^k = 1\}.$$

For simplicity, we write $U = U(d-1)$, $U_k = U_k(d-1)$. The restriction of Λ to U_k is a finite sum of irreducible representations of this group (possibly including trivial components). Applying [19, Th. 9.2.6, (5)] to each of the non-trivial ones (and the obvious identity for the trivial components), we find that

$$\frac{1}{|\mathcal{U}(\mathbf{F}_p)|} \sum_{t \in \mathcal{U}(\mathbf{F}_p)} \mathrm{Tr}\, \Lambda(\theta_{\chi, g_{d,t}}(p)) = \langle \Lambda \mid U_k, 1 \rangle + O((\dim \Lambda) d p^{-1/2})$$

where the implied constant is *absolute* (this is because we have a one-parameter family, so we can apply [19, 9.2.5] and the fact proved in [16, 5.12] that the relevant sheaf is everywhere tame, so the Swan-conductor contribution is zero; the parameter curve $\mathcal{U}$ has d points at infinity, which give the factor d above).

Using Frobenius reciprocity or direct integration (using, e.g, [19, Lemma AD.7.1]), we find that the multiplicity of the trivial representation in Λ (restricted to U_k) satisfies

$$\langle \Lambda \mid U_k, 1\rangle = \sum_{h\in\mathbf{Z}} \langle \Lambda, \det(\cdot)^{hk}\rangle = \begin{cases} 1 & \text{if } \Lambda = \det(\cdot)^{hk} \text{ for some } h \in \mathbf{Z} - \{0\},\\ 0 & \text{otherwise.}\end{cases}$$

For a given Λ, this is equal to 1 only if $\dim\Lambda = 1$, so $\Lambda = \det(\cdot)^r$ for some $r \in \mathbf{Z} - \{0\}$, and if χ is such that $k(\chi) \mid r$. The number of such characters χ is therefore $\ll 1$, the implied constant depending on Λ. Hence we find, after adding back the characters with $\chi^{2d} = 1$, that

$$\frac{1}{p-2} \sideset{}{^*}\sum_{\chi \,(\mathrm{mod}\, p)} \frac{1}{|\mathcal{U}(\mathbf{F}_p)|} \sum_{t\in\mathcal{U}(\mathbf{F}_p)} \mathrm{Tr}\,\Lambda(\theta_{\chi,g_{d,t}}(p)) \ll \frac{d}{p} + \frac{(\dim\Lambda)d}{p^{1/2}},$$

where the implied constant depends on Λ. This confirms the claimed equidistribution. ☐

Proof of Theorem 10. This an easy consequence of Theorem 11: for any open set $V \subset \mathbf{C}$, we have first that

$$|\mathcal{U}(\mathbf{F}_p)| \sim p$$

as p goes to infinity, and then we can write

$$\liminf_{p\to+\infty} \frac{1}{|X(p)|} |\{(\chi,t) \in X(p) \mid \chi^d \neq 1, \quad L(\tfrac{1}{2}, g_{d,t}, \chi) \in V\}| \geqslant \mu_{d-1}(\{g \in U(d-1) \mid \det(1-g) \in V\}),$$

and then we apply Theorem 7. ☐

Remark 10. In Theorem 11, we performed the average over χ, because for "standard" families of exponential sums (those parametrized by points of algebraic varieties), the (connected component of the) geometric monodromy group is always semisimple, so its center is finite and its maximal compact subgroup can never be $U(N)$.

However, thanks to recent results of Katz [18, §24, Th. 25.1], it is possible to *fix* t (with some conditions) in the example above. For example, we can take $t = 1$, and from [18, Th. 25.1], it follows that the conjugacy classes

$$\{\theta_\chi(p) = \theta_{\chi,X^d-dX-1} \mid \chi \,(\mathrm{mod}\, p) \text{ non-trivial}\}$$

corresponding to the exponential sums

$$S(\chi) = \sum_{x\in\mathbf{F}_p} \chi(x^d - dx - 1)$$

(where $d > 6$, $p \nmid d(d-1)$) become equidistributed in $U(d-1)^\sharp$ as $p \to +\infty$ (the only thing that must be checked to apply the result of Katz is that the set S_d of critical values of f in $\mathbf{C}$ is not a multiplicative translate of itself; but that set is given by

$$S_d = \{(1-d)\xi - 1 \mid \xi \in \boldsymbol{\mu}_{d-1}\},$$

and the condition $S_d = aS_d$ for some $a \in \mathbf{C}^\times$ implies $a = 1$, since both sets contain a unique point of maximal modulus, namely $(1-d) - 1 = -d \in S$ and $-ad \in aS_d$).

This leads to a corresponding variant of Theorem 10.

4.2. **Symplectic symmetry.** A typical example of symplectic symmetry involves families of L-functions of algebraic curves over finite fields. For simplicity, we will consider one of the simplest ones, but we first start by proving distribution results for characteristic polynomials of symplectic matrices, which are of independent interest.

We first remark that for $A \in USp(2g, \mathbf{C})$, the characteristic polynomial can be expressed in the form

$$\det(1 - TA) = \prod_{1 \leqslant j \leqslant g} (1 - e^{i\theta_j} T)(1 - e^{-i\theta_j} T)$$

for some eigenangles θ_j, $1 \leqslant j \leqslant g$, and it follows that

$$\det(1 - A) = \prod_{1 \leqslant j \leqslant g} |(1 - e^{i\theta_j})|^2 \geqslant 0.$$

This positivity is reflected in a shift in expectation in the mod-Gaussian convergence (it also means that the argument is not an interesting quantity here). We obtain:

Proposition 12. *For $g \geqslant 1$, let*

$$X_g = \log\det(1 - T_g) - \tfrac{1}{2}\log(\tfrac{\pi g}{2}),$$

where T_g is a Haar-distributed random matrix in the unitary symplectic group $USp(2g, \mathbf{C})$. Then X_g converges in mod-Gaussian sense with $Q_g(t) = (\log \frac{1}{2} g) t^2$ and limiting function[7]

$$\Phi_{Sp}(t) = \frac{G(\frac{3}{2})}{G(\frac{3}{2} + it)}. \tag{27}$$

Indeed, we have

$$\mathbf{E}(e^{itX_g}) = \exp(-(\log \tfrac{1}{2} g) t^2/2) \Phi_{Sp}(t) \Big(1 + O\Big(\frac{1 + |t|^3}{g}\Big)\Big)$$

for $|t| \leqslant g^{1/6}$, where the implied constant is absolute.

Figure 2 is a graph illustrating the logarithmic growth of $\frac{1}{t^2} \log|\Phi_{Sp}(t)|$.

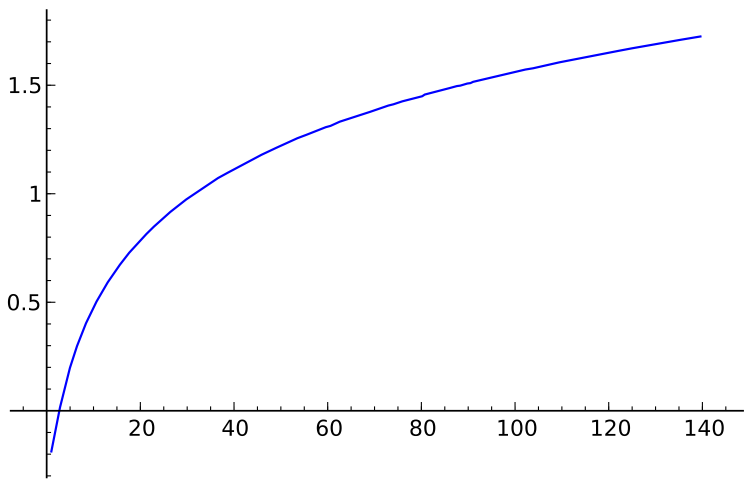

FIGURE 2. Graph of $\frac{1}{t^2} \log|\Phi_{Sp}(t)|$, $1 \leqslant t \leqslant 140$

[7] The expressions in [21, (32), (67)] and [7, Cor. 4.2] are rather more complicated, but of course they are equivalent.

Proof. (Compare [14, Prop. 4.9]) Keating-Snaith [21, (10)] compute that

$$\mathbf{E}(e^{it\log\det(1-T_g)}) = 2^{2git}\prod_{j=1}^{g}\frac{\Gamma(1+g+j)\Gamma(\frac{1}{2}+it+j)}{\Gamma(\frac{1}{2}+j)\Gamma(1+it+g+j)},$$

which, together with the formula (23), gives

$$\mathbf{E}(e^{itX_g}) = \Bigl(\frac{\pi g}{2}\Bigr)^{-it/2}\frac{G(\frac{3}{2})}{G(\frac{3}{2}+it)} \times 2^{2git}\frac{G(\frac{3}{2}+it+g)G(2+2g)G(2+it+g)}{G(\frac{3}{2}+g)G(2+g)G(2+it+2g)}.$$

By applying Proposition 17, (3) in the Appendix, we get

$$\mathbf{E}(e^{itX_g}) = \Bigl(\frac{g}{2}\Bigr)^{-t^2/2}\Phi_{Sp}(t)\Bigl(1+O\Bigl(\frac{1+|t|^3}{g}\Bigr)\Bigr),$$

as claimed. □

In particular, the Central Limit Theorem for $\det(1-T_g)$ takes the form of the convergence in law

$$\frac{\log\det(1-T_g)-\frac{1}{2}\log\frac{\pi g}{2}}{(\log(g/2))^{1/2}} \overset{\text{law}}{\Rightarrow} \text{(standard Gaussian)},$$

so, for any $a<b$, we have

$$\mathbf{P}\Bigl(\Bigl(\frac{\pi g}{2}\Bigr)^{1/2}e^{a\sqrt{\log(g/2)}} < \det(1-T_g) < \Bigl(\frac{\pi g}{2}\Bigr)^{1/2}e^{b\sqrt{\log(g/2)}}\Bigr) \to \frac{1}{\sqrt{2\pi}}\int_a^b e^{-t^2/2}dt.$$

On the other hand, by applying Theorem 4, as we can according to the previous proposition, we can control the probability of the values of $\det(1-T_g)$ in much smaller (dyadic or similar) intervals:

Corollary 13. *Let $U=]a,b[$ with $a<b$ real numbers. We have*

$$\mathbf{P}\Bigl(e^a\Bigl(\frac{\pi g}{2}\Bigr)^{1/2} < \det(1-T_g) < e^b\Bigl(\frac{\pi g}{2}\Bigr)^{1/2}\Bigr) = \frac{1}{\sqrt{2\pi\log\frac{1}{2}g}}\int_a^b \exp\Bigl(-\frac{t^2}{2\log\frac{1}{2}g}\Bigr)dt + O\Bigl(\frac{\max(b-a,(b-a)^{-1})}{\log g}+\frac{\max(1,b-a)}{(\log g)^{1/2+1/29}}\Bigr)$$

for $g\geqslant 2$, where the implied constant is absolute. In particular

$$\mathbf{P}\Bigl(\Bigl(\frac{\pi g}{2}\Bigr)^{1/2} < \det(1-T_g) < 2\Bigl(\frac{\pi g}{2}\Bigr)^{1/2}\Bigr) = \frac{1}{\sqrt{2\pi\log\frac{1}{2}g}}\int_0^{\log 2} \exp\Bigl(-\frac{t^2}{2\log\frac{1}{2}g}\Bigr)dt + O\Bigl(\frac{1}{(\log g)^{1/2+1/29}}\Bigr).$$

Proof. If $b-a\leqslant 1$, we apply Theorem 4, with the constants $\mu=1$, A arbitrarily close to 2, a arbitrarily large and $C=1/2$, so that D can be any number with

$$D > 2(1+1+12) = 28,$$

and in particular $D=29$ is valid. If $b-a>1$, we split the interval $]a,b[$ into $2\lceil b-a\rceil$ intervals of length

$$\frac{1}{4}\leqslant\frac{b-a}{2\lceil b-a\rceil}\leqslant 1,$$

and apply the previous case to the interior of those intervals. Since the joint distribution of eigenvalues of T_g is absolutely continuous with respect to Lebesgue measure, the probability of falling on one of the missing endpoints is zero, and summing over these intervals gives the result. □

We now deduce an arithmetic corollary, using families of hyperelliptic curves over finite fields. For any odd q, any integer $g \geqslant 1$ and any squarefree monic polynomial $f \in \mathbf{F}_q[X]$ of degree $2g+1$, let C_f be the smooth projective model of the affine hyperelliptic curve

$$C_f \,:\, y^2 = f(x).$$

The number of $\mathbf{F}_{q^m}$-rational points on C_f satisfies

$$|C_f(\mathbf{F}_{q^m})| = q^m + 1 - \sum_{x \in \mathbf{F}_{q^m}} \chi_2(N_{\mathbf{F}_{q^m}/\mathbf{F}_q}(f(x))) = q^m + 1 - S_m(\chi_2, f)$$

where χ_2 is the quadratic character of $\mathbf{F}_q^\times$ and the notation is as in Section 4.1. The associated L-function (the numerator of the zeta function) is defined by

$$L(C_f, s) = L(s, f, \chi_2),$$

or, in other words, we have

$$L(C_f, s) = Z(C_f, q^{-s}), \qquad Z(C_f, T) = \exp\Bigl(\sum_{m \geqslant 1} \frac{S_m(\chi_2, f)}{m} T^m\Bigr).$$

Weil proved that $Z(C_f, T)$ is a polynomial in $\mathbf{Z}[T]$, of degree $2g$, all roots of which have modulus $\sqrt{q}$, and which is *symplectic*: there is a unique conjugacy class $\theta_f(q)$ in $USp(2g, \mathbf{C})$ such that

$$L(C_f, s + \tfrac{1}{2}) = \det(1 - q^{-s}\theta_f(q)).$$

Theorem 14. *Let $\mathcal{H}_g(\mathbf{F}_q)$ be the set of squarefree, monic, polynomials of degree $2g+1$ in $\mathbf{F}_q[X]$. Fix a non-empty open interval $]\alpha, \beta[\subset]0, +\infty[$. For all g large enough, we have*

$$\liminf_{q \to +\infty} \frac{1}{|\mathcal{H}_g(\mathbf{F}_q)|} \Bigl| \Bigl\{ f \in \mathcal{H}_g(\mathbf{F}_p) \ \mid\ \frac{L(C_f, 1/2)}{\sqrt{\pi g/2}} \in]\alpha, \beta[\Bigr\} \Bigr| \gg \frac{1}{\sqrt{\log g}}. \tag{28}$$

(Note that this is in fact a very weak version of what we can prove).

Proof. Let first $\mathcal{H}_g^*(\mathbf{F}_q)$ be the set of $f \in \mathcal{H}_g(\mathbf{F}_q)$ for which $L(C_f, 1/2) \neq 0$. In [14, Prop. 4.9], we showed, using the relevant equidistribution computation in [19, 10.8.2] that the (real-valued) random variables

$$L_g = \log\det(1 - \theta_F(q)) - \tfrac{1}{2}\log(\tfrac{\pi g}{2}),$$

on $\mathcal{H}_g^*(\mathbf{F}_q)$ (with counting measure) converges in law to

$$X_g = \log\det(1 - T_g) - \tfrac{1}{2}\log(\tfrac{\pi g}{2}),$$

where T_g is a random matrix in the unitary symplectic group $USp(2g, \mathbf{C})$, distributed according to Haar measure. The previous proposition shows that Theorem 4 is applicable to X_g with covariance $Q_g(t) = (\log \frac{1}{2}g)t^2$ and limiting function $\Phi_{Sp}(t)$. Letting $q \to +\infty$ as in the previous section, we get

$$\liminf_{q \to +\infty} \frac{1}{|\mathcal{H}_g^*(\mathbf{F}_q)|} \Bigl| \Bigl\{ f \in \mathcal{H}_g^*(\mathbf{F}_p) \ \mid\ \log L(C_f, 1/2) - \tfrac{1}{2}\log(\tfrac{\pi g}{2}) \in]\alpha, \beta[\Bigr\} \Bigr| \gg \frac{1}{\sqrt{\log g}}$$

for g large enough. Since

$$|\mathcal{H}_g^*(\mathbf{F}_q)| = |\mathcal{H}_g(\mathbf{F}_q)|(1 + o(1)) = q^{2g+1}(1 + o(1))$$

for fixed g and $q \to +\infty$ (by an easy application of the equidistribution, see [14, Prop. 4.9]), we get the result stated by exponentiating. ☐

Remark 11. The lower bound (28) is good enough to combine with various other statements proving arithmetic properties of L-functions which hold for "most" hyperelliptic curves. For instance, from [23, Prop. 1.1] (adapted straightforwardly to all hyperelliptic curves instead of special one-parameter families), it follows that if we denote by $\tilde{\mathcal{H}}_g(\mathbf{F}_q)$ the set of $f \in \mathcal{H}_g(\mathbf{F}_q)$ such that the eigenvalues of $\theta_f(q)$ satisfy no non-trivial multiplicative relation,[8] then we have

$$|\{f \in \mathcal{H}_g(\mathbf{F}_q) \mid f \notin \tilde{\mathcal{H}}_g(\mathbf{F}_q)\}| \ll_g q^{1-\gamma}$$

for some $\gamma = \gamma(g) > 0$, and hence we get

$$\liminf_{q\to+\infty} \frac{1}{|\mathcal{H}_g(\mathbf{F}_q)|}\Big|\Big\{f \in \tilde{\mathcal{H}}_g(\mathbf{F}_p) \mid \frac{L(C_f,1/2)}{\sqrt{\pi g/2}} \in]\alpha,\beta[\Big\}\Big| \gg \frac{1}{\sqrt{\log g}}$$

for g large enough.

4.3. **Orthogonal symmetry.** Orthogonal symmetry, in number theory, features prominently in families of elliptic curves. In contrast with symplectic groups, there are a number of "flavors" involved, due to the "functional equation"

$$T^N \det(1 - T^{-1}A) = \det(-A)\det(1 - TA)$$

for an orthogonal matrix $A \in O(N, \mathbf{R})$ (the standard maximal compact subgroup of the orthogonal group $O(N, \mathbf{C})$), which implies that $\det(1 - A)$ is zero for "trivial" reasons if N is even and $\det(A) = -1$ or N is odd and $\det(A) = 1$. When this happens, it is of great interest to investigate the distribution of the first derivative at $T = 1$ of the reversed characteristic polynomial. For simplicity, however, we restrict our attention here to N even and matrices with determinant 1, i.e., to the subgroup $SO(2N, \mathbf{R})$ of $O(2N, \mathbf{R})$, where $N \geqslant 1$. In that case, it is also true that eigenangles come in pairs of inverses, and therefore we have $\det(1 - A) \geqslant 0$.

As in the previous section, we start with random matrix computations.

Proposition 15. *For $N \geqslant 1$, let*

$$X_N = \log\det(1 - T_N) - \tfrac{1}{2}\log(\tfrac{8\pi}{N}),$$

where T_N is a Haar-distributed random matrix in the special orthogonal group $SO(2N, \mathbf{R})$. Then X_N converges in mod-Gaussian sense with $Q_N(t) = (\log \frac{1}{2}N)t^2$ and limiting function

$$\Phi_{SO}(t) = \frac{G(\frac{1}{2})}{G(\frac{1}{2} + it)}. \tag{29}$$

Indeed, we have

$$\mathbf{E}(e^{itX_N}) = \exp(-(\log \tfrac{1}{2}N)t^2/2)\Phi_{SO}(t)\Big(1 + O\Big(\frac{1 + |t|^3}{N}\Big)\Big)$$

for $|t| \leqslant N^{1/6}$, where the implied constant is absolute.

Proof. Using [21, (56)] and (23), we get

$$\begin{aligned}\mathbf{E}(e^{it\log\det(1-T_N)}) &= 2^{2Nit}\prod_{j=1}^{N}\frac{\Gamma(N+j-1)\Gamma(it+j-\frac{1}{2})}{\Gamma(j-\frac{1}{2})\Gamma(it+N+j-1)},\\ &= \frac{G(\frac{1}{2})}{G(\frac{1}{2}+it)} \times 2^{2Nit}\frac{G(\frac{1}{2}+it+N)G(2N)G(it+N)}{G(\frac{1}{2}+N)G(N)G(it+2N)},\end{aligned}$$

and by applying Proposition 17, (4) in the Appendix, we get the desired formula

$$\mathbf{E}(e^{itX_N}) = \Big(\frac{N}{2}\Big)^{-t^2/2}\Phi_{SO}(t)\Big(1 + O\Big(\frac{1+|t|^3}{N}\Big)\Big).$$

∎

Remark 12. If we compare with the symplectic case, we observe the (already well-established) phenomenon that the value $\det(1-A)$, for $A \in SO(2N, \mathbf{R})$ tend to be small, whereas they tend to be large for symplectic matrices in $USp(2g, \mathbf{C})$.

[8] An analogue of the hypothetical statement of $\mathbf{Q}$-linear independence of the ordinates of zeros of the Riemann zeta function; non-trivial refers to a relation that can not be deduced from the fact that, if $e^{i\theta}$ is an eigenvalue, so is its inverse $e^{-i\theta}$.

Our arithmetic corollary is based on families of quadratic twists of elliptic curves over function fields, and we select a specific example for concreteness (see [22, §4]); the basic theory, which we illustrate here, is again due to Katz [17].

For any odd prime power $q \geqslant 3$, any integer $N \geqslant 1$, we consider the elliptic curves over the functional field $\mathbf{F}_q(T)$ given by the Weierstrass equations

$$\mathcal{E}_z \,:\, Y^2 = (T^N - NT - 1 - z)X(X+1)(X+T),$$

where $z \in \mathbf{F}_q$ is a parameter such that z is not a critical value of $T^N - NT - 1$.

Katz proved that the associated L-function (which is now defined by the "standard" Euler product over primes in $\mathbf{F}_q[T]$, with suitable ramified factors) is of the form

$$L(\mathcal{E}_z, s+1) = \det(1 - \theta_z(q)q^{-s})$$

where $\theta_z(q)$ is a unique conjugacy class in $O(2N, \mathbf{R})$.

Theorem 16. *Fix a non-empty open interval* $]\alpha, \beta[\subset]0, +\infty[$. *For all N large enough, we have*

$$\liminf_{\substack{p\to+\infty\\(p-1,N-1)=1}} \frac{1}{p}\Big|\Big\{z \in \mathbf{F}_p \mid \Big(\frac{N}{8\pi}\Big)^{1/2} L(\mathcal{E}_z, 1/2) \in]\alpha, \beta[\Big\}\Big| \gg \frac{1}{\sqrt{\log N}}.$$

Proof. As recalled in [22, Cor. 4.4 and before], for all $N \geqslant 146$ and primes p with $p \nmid N(N-1)(N+1)$ and $(p-1, N-1) = 1$, the conjugacy classes $\theta_z(p)$, for $z \in \mathbf{F}_p$ not a critical value, become equidistributed in $O(2N, \mathbf{R})^\sharp$ for the image of Haar measure (precisely, this is stated for the "vertical direction" where p is fixed and finite fields of characteristic p and increasing degree are used; however, because the parameter variety is a curve with $N+1$ points at infinity and the relevant sheaf is tame, we can recover the horizontal statement as in the proof of Theorem 11). In particular, there is a subset $V_p \subset \mathbf{F}_p$ with $|V_p| \sim p/2$ where $\det(\theta_z(p)) = 1$ and those restricted conjugacy classes become equidistributed in $SO(2N, \mathbf{R})^\sharp$. Hence, for N large enough, we get

$$\liminf_{\substack{p\to+\infty\\(p-1,N-1)=1}} \frac{1}{|V_p|}\Big|\Big\{z \in V_p \mid \Big(\frac{N}{8\pi}\Big)^{1/2} L(\mathcal{E}_z, 1/2) \in]\alpha, \beta[\Big\}\Big|$$

$$\geqslant \mu_{SO(2N,\mathbf{R})}(\{A \mid \log\det(1-A) \in]\log\alpha, \log\beta[\}) \gg \frac{1}{\sqrt{\log N}},$$

as desired. □

Remark 13. Obviously, this result (or its generalizations to other families of quadratic twists over function fields) has interesting consequences concerning the problem of the distribution of the order of Tate-Shafarevich groups of the associated elliptic curves, through the Birch and Swinnerton-Dyer conjecture (which is known to be valid in its strong form for many elliptic curves over function fields over a finite field with analytic rank 0 or 1). We hope to come back to this question, and its conjectural analogue over number fields, in another work.

Appendix: estimates for the Barnes function

We present in this appendix some uniform analytic estimate for the Barnes function, which are needed to verify the strong convergence assumption (7) for sequences of random matrices in compact classical groups. Note that we did not try to optimize the results.

Proposition 17. (1) *For all $z \in \mathbf{C}$ and $n \geqslant 1$ with $|z| \leqslant n^{1/6}$, we have*

$$\frac{G(1+z+n)}{G(1+n)} = (2\pi)^{z/2} e^{-(n+1)z}(1+n)^{z^2/2+nz}\Big(1 + O\Big(\frac{z^2+z^3}{n}\Big)\Big). \tag{30}$$

(2) *For all $N \geqslant 1$ and all $t = (t_1, t_2) \in \mathbf{R}^2$ with $\|t\| \leqslant N^{1/6}$ we have*

$$\frac{G(1+it_1+N)G(1+N)}{G(1+\frac{it_1-t_2}{2}+N)G(1+\frac{it_1+t_2}{2}+N)} = N^{-(t_1^2+t_2)/4}\Big(1 + O\Big(\frac{1+\|t\|^3}{N}\Big)\Big).$$

(3) *For all $g \geqslant 1$ and all $t \in \mathbf{R}$ with $|t| \leqslant g^{1/6}$ we have*

$$2^{2git}\frac{G(\frac{3}{2}+it+g)G(2+2g)G(2+it+g)}{G(\frac{3}{2}+g)G(2+g)G(2+it+2g)} = \Big(\frac{g}{2}\Big)^{-t^2/2}\Big(\sqrt{\frac{\pi g}{2}}\Big)^{it}\Big(1+O\Big(\frac{1+|t|^3}{g}\Big)\Big).$$

(4) *For all $N \geqslant 1$ and all $t \in \mathbf{R}$ with $|t| \leqslant N^{1/6}$ we have*

$$2^{2Nit}\frac{G(\frac{1}{2}+it+N)G(2N)G(it+N)}{G(\frac{1}{2}+N)G(N)G(it+2N)} = \Big(\frac{N}{2}\Big)^{-t^2/2}\Big(\sqrt{\frac{8\pi}{N}}\Big)^{it}\Big(1+O\Big(\frac{1+|t|^3}{N}\Big)\Big).$$

In all estimates, the implied constants are absolute.

Proof. One can use the asymptotic expansions in [3, §15] or [10], but we follow instead the nice arrangement of the Barnes function in [9, Cor. 3.2], which leads to a quicker and cleaner proof.

(1) First, the ratio of Barnes function is well-defined since $n \geqslant 1$. We now use the formula

$$\frac{G(1+z+n)}{G(1+n)} = (2\pi)^{z/2}e^{-(n+1)z}(1+n)^{z^2/2+nz}S_n(z), \tag{31}$$

where

$$S_n(z) = e^{-z(z-1)/2}\prod_{k\geqslant n+1}\Big(1+\frac{z}{k}\Big)^{k-n}\Big(1+\frac{1}{k}\Big)^{z^2/2+nz}e^{-z},$$

which is valid for $z \in \mathbf{C}$, $n \geqslant 1$ (see [9, p. 241]).

If we expand the logarithm, defined using the Taylor expansion of $\log(1+w)$ at the origin, we have

$$\log(1+w) = w - \frac{w^2}{2} + O(w^{-3})$$

for $|w| \leqslant 1/2$, with an absolute implied constant. Hence we obtain

$$\begin{aligned}\log S_n(z) &= -\frac{z(z-1)}{2} + \sum_{k>n}\Big(k\log\Big(1+\frac{z}{k}\Big)+\frac{z^2}{2}\log\Big(1+\frac{1}{k}\Big)-z\Big)\\ &\quad + \sum_{k>n} n\Big(z\log\Big(1+\frac{1}{k}\Big)-\log\Big(1+\frac{z}{k}\Big)\Big)\\ &= -\frac{z(z-1)}{2} - \frac{z^2}{2}\sum_{k>n}\frac{1}{k^2} + n\frac{z(z-1)}{2}\sum_{k>n}\frac{1}{k^2} + O\Big(\sum_{k>n}\Big(\frac{z^2}{k^3}+\frac{z^3}{k^2}\Big)\Big)\end{aligned}$$

with an absolute implied constant, for $n \geqslant 1$ and $|z| \leqslant n/2$, hence for $|z| \leqslant n^{1/6}$ we get

$$\log S_n(z) = O\Big(\frac{z^2+z^3}{n}\Big),$$

since

$$\sum_{k>n}\frac{1}{k^2} = \frac{1}{n} + O\Big(\frac{1}{n^2}\Big), \quad \sum_{k>n}\frac{1}{k^3} = \frac{1}{2n^2} + O\Big(\frac{1}{n^3}\Big),$$

for $n \geqslant 1$, with absolute implied constants. Hence, we have

$$S_n(z) = 1 + O\Big(\frac{z^2+z^3}{n}\Big)$$

for $|z| \leqslant n^{1/6}$, for some absolute implied constant, and we get the stated formula

$$\frac{G(1+z+n)}{G(1+n)} = (2\pi)^{z/2}e^{-(n+1)z}(1+n)^{z^2/2+nz}\Big(1+O\Big(\frac{z^2+z^3}{n}\Big)\Big).$$

(2) Note first that the conditions $N \geqslant 1$ and $\|t\| \leqslant N^{1/6}$ ensure that the values of the Barnes function in the denominator are non-zero. Next, let $u = (it_1 - t_2)/2$, $v = (it_1 + t_2)/2$; we can express the ratio of Barnes function as

$$\frac{G(1+u+v+N)G(1+N)}{G(1+u+N)G(1+v+N)} = \frac{G(1+u+v+N)}{G(1+N)}\frac{G(1+N)}{G(1+u+N)}\frac{G(1+N)}{G(1+v+N)},$$

and $\|t\| \leqslant N^{1/6}$ gives $|u|$, $|v| \leqslant N^{1/6}$, allowing us to apply (30) three times. The exponential terms cancel out, leading to

$$\frac{G(1+u+v+N)G(1+N)}{G(1+u+N)G(1+v+N)} = (1+N)^{-\|t\|^2/4}\Bigl(1+O\Bigl(\frac{|t|^2+|t|^3}{N}\Bigr)\Bigr)$$

which gives the first part of the proposition.

(3) We use a similar computation, applying (30) six times with the parameters (n, z)

$$(2g, 1),\ (g, 1+it),\ (g, \tfrac{1}{2}+it),\ (g, 1),\ (2g, 1+it),\ (g, \tfrac{1}{2}),$$

leading, after an easy calculation, to a main term

$$(2\pi)^{it/2}e^{-it}(1+g)^{-t^2+3it/2+2igt}(1+2g)^{t^2/2-it-2igt}$$

for the ratio of Barnes functions, and some further computation leads to the stated result (each parameter z has $|z| \leqslant |t|+1$, so the error term is also as given).

(4) We argue exactly as in the previous case, with parameters (n, z) given now by

$$(2N-1, 0),\ (N-1, 0),\ (N-1, it+\tfrac{1}{2}),\ (N-1, it),\ (2N-1, it),\ (N-1, \tfrac{1}{2}),$$

and we get a main term

$$(2\pi)^{it/2}N^{-t^2-3it/2+2iNt}(2N)^{t^2/2+it-2itN} = 2^{t^2/2+it-2itN}(2\pi)^{it/2}N^{-t^2/2-it/2},$$

which leads to the conclusion. □

References

[1] P. Billingsley: *Convergence of probability measures*, Wiley 1968.

[2] L. Breiman: *Probability*, Classics in Applied Mathematics 7, SIAM, 1992.

[3] E.W. Barnes: *The theory of the G-function*, Quarterly J. Pure and Appl. Math. 31 (1900), 264–314.

[4] E. Basor: *Toeplitz determinants, Fisher-Hartwig symbols, and random matrices*, in "Recent perspectives in Random Matrix Theory and number theory", LMS Lecture Note 322, CUP 2005.

[5] E. Bombieri and D. Hejhal: *On the distribution of zeros of linear combinations of Euler products*, Duke Math. J. 80 (1995), 821–862.

[6] A. Böttcher and T. Widom: *Two elementary derivations of the pure Fisher-Hartwig determinant*, Integral Equations Operator Theory 53 (2005), 593–596.

[7] J.B. Conrey and D.W. Farmer: *Mean values of L-functions and symmetry*, IMRN 2000 (17), 883–908.

[8] F. Delbaen, E. Kowalski and A. Nikeghbali: *Mod-φ convergence*, preprint `arXiv:1107.5657`

[9] T. Ehrhardt and B. Silbermann: *Toeplitz determinants with one Fisher-Hartwig singularity*, Journal Funct. Analy. 148 (1997), 229–256.

[10] C. Ferreira and J.L. López: *An asymptotic expansion of the Double Gamma function*, J. Approx. Theory 111 (2001), 298–314.

[11] A. Ghosh: *On the Riemann zeta function – Mean value theorems and the distribution of $|S(t)|$*, J. Number Theory 17 (1983), 93–102.

[12] L. Hörmander: *The analysis of linear partial differential operators I: distribution theory and Fourier analysis*, Springer-Verlag, Classics in Mathematics, 2003.

[13] A.E. Ingham: *A note on Fourier transforms*, J. London Math. Soc. s1–9 (1934), 29–32.

[14] J. Jacod, E. Kowalski and A. Nikeghbali: *Mod-Gaussian convergence: new limit theorems in probability and number theory*, Forum Math. 23 (2011), 835–873.

[15] N.M. Katz: *Estimates for nonsingular multiplicative character sums*, IMRN 7 (2002), 333–349.

[16] N.M. Katz: *Affine cohomological transforms, perversity, and monodromy*, Journal of the A.M.S 6 (1993), 149–222.

[17] N.M. Katz: *Twisted L-functions and monodromy*, Annals of Math. Studies 150, Princeton Univ. Press 2002.

[18] N.M. Katz: *Convolution and equidistribution: Sato-Tate theorems for finite field Mellin transforms*, Annals of Math. Studies 180, Princeton Univ. Press 2012; also available on `www.math.princeton.edu/~nmk`

[19] N.M. Katz and P. Sarnak: *Random matrices, Frobenius eigenvalues, and monodromy*, A.M.S Colloquium Publ. 45, A.M.S, 1999.

[20] J.P. Keating and N.C. Snaith: *Random matrix theory and $\zeta(1/2+it)$*, Commun. Math. Phys. 214, (2000), 57–89.

[21] J.P. Keating and N.C. Snaith: *Random matrix theory and L-functions at $s = 1/2$*, Comm. Math. Phys. 214 (2000), 91–110.

[22] E. Kowalski: *On the rank of quadratic twists of elliptic curves over function fields*, Int. J. Number Theory 2 (2006), 267–288.

[23] E. Kowalski: *The Large Sieve, Monodromy, and Zeta Functions of Algebraic Curves, 2: Independence of the Zeros*, International Mathematics Research Notices (2008), article rnn091, 57 pages, doi:10.1093/imrn/rnn091

[24] E. Kowalski: *Exponential sums over finite fields, I: elementary methods*, in preparation; available at www.math.ethz.ch/~kowalski/exp-sums.pdf

[25] E. Kowalski and A. Nikeghbali: *Mod-Poisson convergence in probability and number theory*, International Mathematics Research Notices 2010; doi: 10.1093/imrn/rnq019; arXiv:0905.0318

[26] W. Stein and D, Joyner: *Sage: System for algebra and geometry experimentation*, Comm. Computer Algebra 39 (2005), 61–64; sagemath.org

[27] G. Tenenbaum: *Introduction to analytic and probabilistic number theory*, Cambridge Studies Adv. Math. **46**, Cambridge Univ. Press, 1995.

[28] E.C. Titchmarsh: *The theory of the Riemann zeta function*, 2nd edition, Oxford Univ. Press, 1988.

[29] K. Wieand: *Eigenvalue distribution of random unitary matrices*, Probab. Theory Relat. Fields 123 (2002), 202–224.

ETH Zürich – D-MATH, Rämistrasse 101, 8092 Zürich, Switzerland
E-mail address: kowalski@math.ethz.ch

Institut für Mathematik, Universität Zürich, Winterthurerstrasse 190, 8057 Zürich, Switzerland
E-mail address: ashkan.nikeghbali@math.uzh.ch