MOD-GAUSSIAN CONVERGENCE: NEW LIMIT THEOREMS IN PROBABILITY AND NUMBER THEORY

J. JACOD, E. KOWALSKI, AND A. NIKEGHBALI

ABSTRACT. We introduce a new type of convergence in probability theory, which we call "mod-Gaussian convergence". It is directly inspired by theorems and conjectures, in random matrix theory and number theory, concerning moments of values of characteristic polynomials or zeta functions. We study this type of convergence in detail in the framework of infinitely divisible distributions, and exhibit some unconditional occurrences in number theory, in particular for families of L-functions over function fields in the Katz-Sarnak framework. A similar phenomenon of "mod-Poisson convergence" turns out to also appear in the classical Erdős-Kác Theorem.

1. INTRODUCTION

Characteristic polynomials of random matrices are essential objects in Random Matrix Theory, and have also come to play a crucial role in the remarkable results and conjectures linking random matrices with the study of L-functions in number theory (see e.g. [14] for recent surveys of this connection). Our present work finds its source in the study of the asymptotic of moments of characteristic polynomials of random unitary matrices by Keating and Snaith [10], and the corresponding conjecture for the moments of the Riemann zeta function on the critical line. More precisely, Keating and Snaith proved (in probabilistic language) that if (Y_N), for $N \geq 1$, is a sequence of complex random variables, with Y_N distributed like $\det(I - X_N)$ for some random variable X_N taking values in the unitary group $U(N)$ and uniformly distributed on $U(N)$ (i.e., distributed according to Haar measure), then for any complex number λ with $\mathrm{Re}(\lambda) > -1$, we have

$$\lim_{N \to \infty} \frac{1}{N^{\lambda^2}} \mathbb{E}\left[|Y_N|^{2\lambda} \right] = \frac{(G(1 + \lambda))^2}{G(1 + 2\lambda)}, \tag{1.1}$$

where G is the *Barnes (double gamma) function*.

Then, using a (now classical) random matrix analogy, they make the following conjecture for the moments of the Riemann zeta function (see

[10],[14]): for any complex number λ with $\mathrm{Re}(\lambda) > -1$, we should have

$$\lim_{T \to \infty} \frac{1}{(\log T)^{\lambda^2}} \frac{1}{T} \int_0^T \left| \zeta \left(\frac{1}{2} + it \right) \right|^{2\lambda} dt = M(\lambda) A(\lambda) \qquad (1.2)$$

where $M(\lambda)$ is the *random matrix factor*, suggested by (1.1), namely

$$M(\lambda) = \frac{(G(1+\lambda))^2}{G(1+2\lambda)} \qquad (1.3)$$

while $A(\lambda)$ is the *arithmetic factor* defined by the Euler product

$$A(\lambda) = \prod_p \left(1 - \frac{1}{p} \right)^{\lambda^2} \left(\sum_{m=0}^{\infty} \left(\frac{\Gamma(\lambda + m)}{m! \Gamma(\lambda)} \right)^2 p^{-m} \right), \qquad (1.4)$$

where, as usual, p runs over prime numbers, and the product is here absolutely and locally uniformly convergent; see Section 4.1 for details.

We now look at (1.1) slightly differently. If we take $\lambda = iu$ to be purely imaginary in (1.1), then we obtain a limit theorem involving the *characteristic function* (or Fourier transform) of the random variables $Z_N = \log |Y_N|^2$ (note that $|Z_N| \neq 0$ almost surely):

$$\lim_{N \to \infty} e^{u^2 \log N} \mathbb{E}[e^{iu Z_N}] = \lim_{N \to \infty} e^{u^2 \log N} \mathbb{E}[e^{iu \log |Y_N|^2}] = \frac{(G(1+iu))^2}{G(1+2iu)}. \quad (1.5)$$

A renormalized convergence of the characteristic function as it occurs in (1.5) is not standard in probability theory. However, it has now appeared in various places in random matrix theory and number theory, although (to the best of our knowledge) always under the form of the convergence of normalized Mellin transforms as in (1.1) and (1.2).

In probability theory, the characteristic function $\mathbb{E}(e^{iuZ})$ is a more natural object to consider, because contrary to Mellin or Laplace transforms, it always exists and characterizes the distribution of a random variable Z. Hence, in order to look more deeply into the properties of this type of limiting behavior for a sequence (Z_N) of real-valued random variables, we use the characteristic functions (the Fourier transforms of the laws), and introduce the following definition:

Definition 1.1. The sequence (Z_N) is said to *converge in the mod-Gaussian sense* if the convergence

$$e^{-iu\beta_N + u^2 \gamma_N / 2} \mathbb{E}[e^{iu Z_N}] \ \to \ \Phi(u) \qquad (1.6)$$

holds for all $u \in \mathbb{R}$, where $\beta_N \in \mathbb{R}$ and $\gamma_N \geq 0$ are two sequences and Φ is a complex-valued function which is continuous at 0 (note that necessarily $\Phi(0) = 1$). We call (β_N, γ_N) the *parameters*, and Φ the associated *limiting function*.

The main aim of this paper is to provide a general framework in which convergence such as (1.6) occurs naturally. Secondary goals are to give examples, both in probability and number theory, and to argue for the

interest of this notion. As a first example, of course, (1.5) shows that the random variables $\log |Y_N|^2$ converge in mod-Gaussian sense with parameters $(0, 2 \log N)$ and limiting function $G(1 + iu)^2 G(1 + 2iu)^{-1}$.

The paper is organized as follows. In Section 2, we properly define the "mod-Gaussian convergence", give some immediate properties and describe some easy examples where it occurs. In Section 3 we show that, under some conditions on the third moment, mod-Gaussian convergence occurs for sums of Césaro means of triangular arrays of independent random variables. Within this framework, a characterization of the limiting function Φ is found in the case of infinitely divisible distributions, and it is shown to have a representation of Lévy-Khintchine type, with one extra term. More generally, we also give a necessary and sufficient condition for the mod-Gaussian convergence to hold when the laws of the (Z_N) are infinitely divisible, with an explicit expression for the limit function Φ (which again has a Lévy-Khintchine type representation, with two extra terms now).

In Section 4, we give examples of mod-Gaussian convergence in number theory, in two directions. First, we show that the arithmetic factor $A(\lambda)$ in the moment conjecture, for $\lambda = iu$, arises as limiting function $\Phi(u)$ for the mod-Gaussian convergence of very natural sequences of random variables, and hence so does $M(iu)A(iu)$; this is in particular additional (though modest) evidence in favor of the conjecture (1.2), since if that were not the case, the conjecture would necessarily be false. Second, we explain how Deligne's Equidistribution Theorem and the Katz-Sarnak philosophy lead to the proof of an analogue of the moment conjecture for families of L-functions over function fields; this second problem was raised in particular by B. Conrey. We think that these facts illustrate that the philosophy of mod-Gaussian convergence is a potentially crucial analytic framework underlying deep issues of number theory. In addition, we interpret the classical Erdős-Kác theorem in a similar way, although with "mod-Poisson" convergence.

Remark 1.2. Because of the possible relevance of this paper both to probability theory and number theory, we have tried to write it in a balanced manner, so that experts in either field can understand it. This means, in particular, that we recall precisely some facts which, for one field at least, are entirely standard and well-known (e.g., facts about infinitely divisible distributions, or zeta functions of curves over finite fields). This also means that, even though we are aware of the possibility of extending our results to sharper statements, we have not done so when this would, in our opinion, obscure the main ideas for one half of our readers.

Notation. We use the notation

$$\nu(f), \qquad \int f(x)d\nu(x), \qquad \int f(x)\nu(dx)$$

interchangeably for the integral of a function f with respect to some measure ν. We write, as usual in probability, $x \wedge y$ for $\min(x, y)$. In number-theoretic

contexts, p always refers to a prime number, and sums and products over p (with extra conditions) are over primes satisfying those conditions.

2. General properties of mod-Gaussian convergence

We start with the definition of a slightly stronger form of mod-Gaussian convergence:

Definition 2.1. The sequence (Z_N) is said to *strongly converge in the mod-Gaussian sense* if the convergence in (1.6) holds uniformly in u, on every compact subset of $\mathbb{R}$.

The left side of (1.6) being continuous, the strong convergence implies that Φ is continuous, hence the mere convergence.

For the mod-Gaussian convergence with parameters $\beta_N = \gamma_N = 0$, the convergence and the strong convergence are the same, and amount to the convergence in law of the variables Z_N (this is basically Lévy's Theorem).

2.1. **Formal properties.** It is natural to first ask for the intuitive meaning of mod-Gaussian convergence (and for explanation of the chosen terminology). The following proposition describes what might be called "regular" mod-Gaussian convergence:

Proposition 2.2. *Let (X_N) be a sequence of real random variables converging in law to a limiting variable with characteristic function Φ. If for each N we let*

$$Z_N = X_N + G_N, \tag{2.1}$$

where G_N is a Gaussian random variable independent of X_N, and with mean β_N and variance γ_N, then we have the strong mod-Gaussian convergence of the sequence (Z_N), with limiting function Φ and parameters (β_N, γ_N).

Proof. Because X_N and G_N are independent, we have

$$\mathbb{E}(e^{iuZ_N}) = \mathbb{E}(e^{iuX_N})\,\mathbb{E}(e^{iuG_N}) = e^{iu\beta_N - u^2\gamma_N/2}\,\mathbb{E}(e^{iuX_N}),$$

by the formula for the characteristic function of a Gaussian random variable (see, e.g., [8, (16.2)]).

The convergence in law of (X_N) implies the local uniform convergence of the characteristic function of X_N to Φ (the easy half of the Lévy Criterion), hence the convergence (1.6) holds locally uniformly in u. □

We see that under this scheme, the variable Z_N is decomposed into two terms: a variable X_N, which converges in law, and a Gaussian variable, with arbitrary variance and mean, which can be viewed as a "noise" added to the converging variables. We then think intuitively of looking at Z_N *modulo*

the subset of Gaussian random variables, and then only the convergent sequence remains. It is this way of producing the convergence introduced in Definition 1.1 which motivated the terminology "mod-Gaussian".

Proposition 2.2 does *not* cover all cases of mod-Gaussian convergence: as we will see later, the limiting function Φ of a sequence converging in the mod-Gaussian sense may not be a characteristic function. However, the intuitive picture of some converging "core" hidden by possibly wilder and wilder noise may still be useful.

The next proposition summarizes a few basic properties of mod-Gaussian convergence that follow easily from the definition (the first part, in particular, is another justification for the terminology).

Proposition 2.3. (1) *Let* (Z_N) *be a sequence of real-valued random variables for which mod-Gaussian convergence holds with parameters* (β_N, γ_N) *and limiting function* Φ. *Then the mod-Gaussian convergence holds for some other parameters* (β'_N, γ'_N) *and limiting function*[1] Φ', *if and only if the limits*

$$\beta = \lim_{N \to +\infty} (\beta_N - \beta'_N), \qquad \gamma = \lim_{N \to +\infty} (\gamma_N - \gamma'_N), \qquad (2.2)$$

exist in $\mathbb{R}$. *In this case* Φ' *is given by*

$$\Phi'(u) = e^{i\beta u - u^2\gamma/2}\, \Phi(u), \qquad (2.3)$$

and if the strong convergence holds with the parameters (β_N, γ_N) *it also holds with* (β'_N, γ'_N).

(2) *Let* (Z_N) *and* (Z'_N) *be two sequences of random variable with mod-Gaussian convergence (resp. strong convergence), with respective parameters* (β_N, γ_N) *and* (β'_N, γ'_N), *and limiting functions* Φ *and* Φ'. *If* Z_N *and* Z'_N *are independent for all* N, *then the sums* $(Z_N + Z'_N)$ *satisfy mod-Gaussian convergence (resp. strong convergence) with limiting function the product* $\Phi\Phi'$ *and parameters* $(\beta_N + \beta'_N, \gamma_N + \gamma'_N)$.

Proof. (2) follows from the multiplicativity of the characteristic functions of independent variables.

As for (1), if (2.2) holds the mod-Gaussian convergence with parameters (β'_N, γ'_N) and limiting function Φ' given by (2.3) is obvious from the definition, as well as the last claim (it is also a special case of (2)).

Conversely, suppose that the mod-Gaussian convergence holds with parameters (β'_N, γ'_N) and limiting function Φ_1. Then

$$e^{-iu\beta_N + u^2\gamma_N/2}\, \mathbb{E}(e^{iuZ_N}) \to \Phi(u), \quad e^{-iu\beta'_N + u^2\gamma'_N/2}\, \mathbb{E}(e^{iuZ_N}) \to \Phi'(u). \quad (2.4)$$

The function Φ and Φ' are both continuous and equal to 1 at 0, so they are non-vanishing on a neighborhood $[-\delta, \delta]$ of 0, with $\delta > 0$. Then for any non-zero $u \in [-\delta, \delta]$, by taking the ratio and the modulus in (2.4), we get

$$\lim_{N \to +\infty} e^{(\gamma'_N - \gamma_N)u^2/2} = \left| \frac{\Phi'(u)}{\Phi(u)} \right| > 0,$$

_____

[1] Here, Φ' is not the derivative of Φ.

hence the second part of (2.2) holds with

$$\gamma = \frac{2}{u^2} \log\left|\frac{\Phi'(u)}{\Phi(u)}\right|$$

(this limit does not depend on the choice of u). Moreover, by (2.4) again,

$$e^{-i(\beta_N - \beta'_N)u} \to \frac{\Phi(u)}{\Phi'(u)} e^{u^2\gamma/2}$$

for all $u \in [-\delta, \delta]$, and the first part of (2.2) follows. $\square$

Remark 2.4. It is important to notice that the mod-Gaussian convergence does *not* require the parameter sequences β_N and γ_N to converge. However, it implies the uniqueness of the parameters (β_N, γ_N), *up to a convergent sequence* (this is what (1) above says).

In the most usual situations, Φ will be smooth and $\mathbb{E}(e^{iuZ_N})$ also, and comparing expansions to second order for the left-hand side and right-hand side of (1.6) around $u = 0$, one finds that, in this situation, the following will hold:

(1) When varying the parameters (using (2.3)), there is a *unique* possible limiting function Φ_0 such that

$$\Phi_0(u) = 1 + o(u^2), \qquad \text{for } u \to 0 \tag{2.5}$$

(2) For this limiting function Φ_0, up to adding sequences converging to 0, we have

$$\beta_N = \mathbb{E}(Z_N), \qquad \gamma_N = \mathbb{V}(Z_N).$$

However, note that in natural situations, it is by no means clear if the limiting function satisfies (2.5), for instance for (1.5). It may also not be the most natural choice (see Proposition 2.2).

Remark 2.5. Observe that (1) in Proposition 2.3 would fail, should we drop the requirement of continuity of Φ at 0. For example if (Z_N) converges in the mod-Gaussian sense with parameters (β_N, γ_N), with $\gamma_N \to \infty$, and if we take $\delta_N \to \infty$ with $0 \le \delta_N < \gamma_N$, then (1.6) holds with the parameters $(\beta_N, \gamma_N - \delta_N)$ as well, and the associated limiting function vanishes outside 0.

2.2. **Remarks, questions and problems.** The introduction of mod-Gaussian convergence suggests quite a few questions which it would be interesting to answer, to deepen the understanding of the meaning of this type of limit behavior of sequences of random variables.

We first remark that, from the point of view of Proposition 2.2, it is also natural to introduce convergence modulo other particular classes of random variables: given a family $\mathcal{F} = (\mu_\lambda)_{\lambda \in \Lambda}$ of probability distributions parametrized by some set Λ, such that the Fourier transforms

$$\hat{\mu}(\lambda, u) = \int_{\mathbb{R}} e^{itx} d\mu_\lambda(t)$$

are non-zero for all $u \in \mathbb{R}$, one would say that a sequence of random variables (Z_N) converges in the mod-$\mathcal{F}$ sense if, for some sequence $\lambda_N \in \Lambda$, we have

$$\lim_{N \to +\infty} \hat{\mu}(\lambda_N, u)^{-1} \mathbb{E}(e^{iuZ_N}) = \Phi(u)$$

for all $u \in \mathbb{R}$, the limiting function Φ being continuous at 0. Weak and strong convergence can be defined accordingly. A particularly natural idea that comes to mind is to look at the family of *symmetric stable* variables with index $\alpha \in (0, 2)$, and parametrized by $\gamma \in \Lambda = (0, +\infty)$, so that

$$\hat{\mu}(\gamma, u) = e^{-\gamma|u|^{\alpha}}.$$

Such examples for $\alpha \neq 2$ have not (yet) been observed "in the wild", but we will see in Section 4.3 that classical results of analytic number theory can be interpreted as an instance of "mod-Poisson" convergence, i.e., with $\mathcal{F}$ the family of Poisson distributions on the integers with parameter $\lambda \in (0, +\infty)$.

Another natural generalization is the fairly obvious notion of multi-dimensional mod-Gaussian convergence for random vectors, or indeed for stochastic processes. The finite-dimensional case may be used, in random-matrix context, to interpret results on moments of products of characteristic polynomials evaluated at different points of the unit circle.

Now here are some obvious questions:

(1) Can one find a convenient criterion for mod-Gaussian convergence to be of the "regular" type of Proposition 2.2? Is there a "weak convergence" description of mod-Gaussian convergence using test functions of some type?

(2) Is the idea useful in analysis also? Here one could think that the analogue of the "regular" mod-Gaussian convergence would be to have a sequence of distributions (T_N) satisfying

$$T_N = g_N \star S_N$$

where $\star$ is the convolution product, g_N is the distribution associated to a Schwartz function of the type $\exp(iu\beta_N - u^2\gamma_N/2)$, and S_N is some convergent sequence of distributions. For instance, is it possible that some approximation schemes for solutions of some kind of equations converge in the mod-Gaussian sense? Is there, then, a more direct way to recover S_N (numerically, for instance) than by performing an inverse Fourier transform? In other words, can the Gaussian noise g_N be "filtered out" naturally?

(3) Is there a convenient criterion for a function Φ defined on $\mathbb{R}$, with $\Phi(0) = 1$ and Φ continuous at 0, to be a limiting function for mod-Gaussian convergence, similar to Bochner's Theorem (a function $\varphi : \mathbb{R} \to \mathbb{C}$ is a characteristic function of a probability measure if and only if φ is continuous, $\varphi(0) = 1$, and φ is a positive-definite function)?

3. Limit theorems with mod-Gaussian behavior

In this section, we provide several theorems characterizing situations in which mod-Gaussian convergence, as introduced in Definition 1.1, holds.

3.1. **The central limit theorem for mod-Gaussian convergence.** We start with a result which provides a very general criterion for mod-Gaussian convergence in the framework of the classical limit theorems of probability theory. This suggests that mod-Gaussian convergence is a "higher order" analogue of the classical convergence in distribution.

We recall first the standard limit theorems in the setting of triangular arrays of independent identically distributed (in short, i.i.d.) random variables.

Let (X_i^n), for $n \geq 1$ and $1 \leq i \leq n$, be random variables, where the variables
$$X_1^n, \ldots, X_n^n$$
in each row are i.i.d. with law denoted by μ_n. For any integer $n \geq 1$, let
$$S_n = X_1^n + \ldots + X_n^n$$
denote the sum of the n-th row.

If the X_i^n have expectation zero and variance 1, the Law of Large Numbers states that S_n/n converges in probability to 0 as $n \to +\infty$, and the Central Limit Theorem states that the random variables $S_n/\sqrt{n}$, which are centered with variance 1, converge in law to the standard Gaussian variable $\mathcal{N}(0,1)$.

The latter can be interpreted as a "second order" type of behavior of S_n/n, beyond the "first order" convergence to 0, by rescaling by $\sqrt{n}$ to obtain variance 1. Instead of this classical normalization, we want to look for finer information by normalizing with a growing variance.

Working with S_n directly does not seem to lead to fruitful results, but for $N \geq 1$, we can consider the *logarithmic mean* of the S_n, i.e., the random variables
$$Z_N = \sum_{n=1}^N \frac{S_n}{n} = \sum_{n=1}^N \frac{1}{n}\left(X_1^n + \ldots + X_n^n\right) \tag{3.1}$$
which have variance given by the N-th harmonic number H_N, i.e., we have
$$\mathbb{V}(Z_N) = H_N = \sum_{n=1}^N \frac{1}{n}.$$

Note that it is well-known that, for a numerical sequence (u_n) that converges to a limit α, the analogue *logarithmic means*
$$v_N = \frac{1}{\log N} \sum_{n=1}^N \frac{u_n}{n}$$
also converge to α (see, e.g., [20, III.9]). This shows that, intuitively, the Z_N can "amplify" the sums S_N by a logarithmic factor.

We now show that, under quite general conditions, the Z_N converge in the mod-Gaussian sense.

Theorem 3.1. *Let $(X_i^n)_{i.n \geq 1}$ be a triangular array of random variables,* all independent*, and such that the variables in the nth row have the same law*

μ_n, and let assume that μ_n has mean zero, variance 1 and third absolute moment satisfying

$$\sum_{n=1}^{\infty} \frac{m_n}{n^2} < \infty, \quad \text{where} \quad m_n = \int_{\mathbb{R}} |x|^3 \mu_n(dx). \qquad (3.2)$$

Then the logarithmic means Z_N defined by (3.1) strongly converge in the mod-Gaussian sense, with parameters $(0, H_N)$, or with parameters $(0, \log N)$.

For the proof, we recall the following useful lemma.

Lemma 3.2 ([3], Proposition 8.44, p.180). *If X is a random variable with $\mathbb{E}[|X|^k] < \infty$, then the characteristic function ϕ of X has the expansion:*

$$\phi(u) = \sum_{j=0}^{k-1} \frac{(iu)^j}{j!} \mathbb{E}[X^j] + \frac{(iu)^k}{k!} \left(\mathbb{E}(X^k) + \delta(u) \right),$$

where $\delta(u)$ is a function of u that satisfies $\lim_{u \to 0} \delta(u) = 0$ and $|\delta(u)| \leq 3\,\mathbb{E}(|X|^k)$ for all u.

Proof of Theorem 3.1. Let $\phi_n(u)$ be the characteristic function of μ_n, and let

$$G_N(u) = e^{u^2 H_N/2}\, \mathbb{E}[e^{iu Z_N}],$$

which is continuous in u. It then suffices to show that G_N converges locally uniformly to a limiting function. By the independence assumption and standard properties of characteristic functions, we have

$$G_N(u) = e^{u^2 H_N/2} \prod_{n=1}^{N} \phi_n(u/n)^n.$$

Let $A > 0$ be fixed. Applying Lemma 3.2 with $k = 2$ and using the fact that the μ_n's are centered with variance 1, we obtain that for $|u| \leq A$ and $n \geq 2A$, we have

$$|\phi_n(u/n) - 1| \leq 2u^2/n^2 \leq 1/2.$$

Taking log to be the principal branch of the logarithm (which is zero at 1) on the disk $\{z \in \mathbb{C} : |z - 1| \leq 1/2\}$, we have for $N > M \geq 2A$ and $|u| \leq A$:

$$G_N(u) = G_M(u) e^{H_{M,N}(u)} \qquad (3.3)$$

where

$$H_{M,N}(u) = \sum_{n=M+1}^{N} n \left(\log \phi_n(u/n) + \frac{u^2}{2n^2} \right). \qquad (3.4)$$

Another application of Lemma 3.2 with $k = 3$ combined with the inequality $|\log(1+z) - z| \leq 4|z|^2$ for $|z| \leq 1/2$, yields for $n \geq M$:

$$\left| \log \phi_n(u/n) + \frac{u^2}{2n^2} \right| \leq \frac{u^3}{n^3} m_n + \frac{16 u^4}{n^4}.$$

It now follows from the assumption (3.2) that for any fixed $M \geq 2A$, $H_{M,N}(u)$ is the partial sum (in N) of a series starting at $M + 1$, which

converges uniformly in $u \in [-A, A]$ to a limit $\tilde{H}_M(y)$, as $N \to \infty$. Consequently, we deduce from (3.3) that $G_N(u)$ converges, as $N \to \infty$, to $G_M(u) \exp \tilde{H}_N(u)$, uniformly in $u \in [-A, A]$. Since A is arbitrarily large, the result follows. $\square$

As an easy consequence of Theorem 3.1 one obtains the following central limit theorem for the sum of Césaro means as introduced in Theorem 3.1.

Corollary 3.3. *With the assumptions and notations of Theorem 3.1, the re-scaled random Césaro means $Z_N/\sqrt{\log N}$ converge in law to the standard Gaussian law $\mathcal{N}(0, 1)$.*

Proof. With the notation G_N of the previous proof, the characteristic function of $Z_N/\sqrt{\log N}$ is

$$e^{-u^2 H_N/\log N} \, G_N(u/\sqrt{\log N}).$$

Now G_N converges locally uniformly to a function equal to 1 at 0, hence $G_N(u/\sqrt{\log N}) \to 1$, whereas we have $H_N \sim \log N$. So the result follows from Lévy's theorem. $\square$

Example 3.4. The observation of the following example, arising from Random Matrix Theory, was the source and motivation for the considerations in this and the next sections.

Consider a sequence (γ_n) of independent random variables, with γ_n having a gamma distribution with scale parameter 1 and index n, that is with the density $\frac{1}{\Gamma(n)} x^{n-1} e^{-x} \mathbf{1}_{\mathbb{R}_+}(x)$. We are interested in the behavior of

$$Z_N = \sum_{n=1}^{N} \frac{\gamma_n}{n} - N.$$

Recalling that one can represent γ_n as the sum $\gamma_n = \sum_{i=1}^{n} Y_i^n$, where the Y_i^n for $i = 1, \cdots, n$ are i.i.d. with gamma distribution with index 1 (or, "exponential distribution"), we see that Z_N is associated by (3.1) with the variables $X_i^n = Y_i^n - 1$, which have mean 0 and variance 1 and a finite third moment (so (3.2) holds). Hence we obtain the limit formula:

$$\lim_{N \to \infty} e^{u^2 H_N/2} \, \mathbb{E} \left[\exp \left(iu \left(\sum_{n=1}^{N} \frac{\gamma_n}{n} - N \right) \right) \right] = \Phi(u) \qquad (3.5)$$

for some continuous function $\Phi(u)$ with $\Phi(0) = 1$.

Now it turns out that this limit can also be computed explicitly (as was first done in [15, Th. 1.2]), as a consequence of a decomposition of the probability law of the characteristic polynomial of random unitary matrices (distributed according to Haar measure) as product of independent gamma and beta random variables. Indeed, it was shown that for any complex

number z with $\mathrm{Re}(z) > -1$, we have

$$\lim_{N\to\infty} \frac{1}{N^{\frac{z^2}{2}}} \mathbb{E}\left[\exp\left(-z\left(\sum_{n=1}^{N} \frac{\gamma_n}{n} - N\right)\right)\right] =$$
$$\left(A^z \exp\left(\frac{z^2}{2}\right) G\left(1+z\right)\right)^{-1} \quad (3.6)$$

where $A = \sqrt{\dfrac{e}{2\pi}}$ and G is the Barnes function.

When $z = -iu$, the left-hand side is just the left-hand side of (3.5), so this argument gives a formula for $\Phi(u)$. More precisely, a representation of the Barnes function obtained in [15, Proposition 2.3], shows that the limiting function $\Phi(u)$ in (3.5) is equal to

$$\exp\left(-\frac{u^2}{2} + \int_0^\infty \frac{1}{x(2\sinh(\frac{x}{2}))^2}\left(e^{iux} - 1 - iux + \frac{u^2 x^2}{2}\right) dx\right). \quad (3.7)$$

This formula, for a probabilist, is very strongly reminiscent of the *Lévy-Khintchine representation* for the characteristic function of infinitely divisible distributions. Since the gamma variables are themselves infinitely divisible, it is natural to wonder whether this example has natural generalizations to other such random variables. We will now see that this is indeed the case.

3.2. **Infinitely divisible distributions.** In this section, we will refine Theorem 3.1, by finding an expression for the limiting function $\Phi(u)$. The context in which we do this is that of *infinitely divisible distributions*. Since readers with number-theoretic background, in particular, may not be familiar with this theory, we first recall some basic facts, referring to the standard textbooks [3] and [17] for proofs and further details.

Definition 3.5 ([17], p. 31)**.** Denote by μ^{n*} the n-fold convolution of a probability measure μ with itself. The probability measure μ on $\mathbb{R}$ is said to be infinitely divisible if for any positive integer n, there is a probability measure μ_n on $\mathbb{R}$ such that $\mu = \mu_n^{n*}$.

Theorem 3.6 ([17], Theorem 8.1, p. 37)**.** *The following properties hold:*
(1) If μ is an infinitely divisible distribution on $\mathbb{R}$, then for $u \in \mathbb{R}$, we have

$$\widehat{\mu}(u) \equiv \int_{-\infty}^{\infty} e^{iux} \mu(dx) = \exp\left[-\frac{1}{2}\sigma u^2 + i\beta u\right.$$
$$\left. + \int_{\mathbb{R}} \left(e^{iux} - 1 - iux \mathbb{1}_{|x|\leq 1}\right) \nu(dx)\right] \quad (3.8)$$

where $\sigma \geq 0$, $\beta \in \mathbb{R}$ and ν is a measure on $\mathbb{R}$, called the Lévy measure, satisfying

$$\nu(\{0\}) = 0 \text{ and } \int_{\mathbb{R}} \left(x^2 \wedge 1\right) \nu(dx) < \infty. \quad (3.9)$$

(2) *The representation of $\widehat{\mu}(u)$ in (3.8) by σ, β and ν is unique.*

(3) *Conversely, if $\sigma \geq 0$, $\beta \in \mathbb{R}$ and ν is a measure satisfying (3.9), then there exists an infinitely divisible distribution μ whose characteristic function is given by (3.8).*

The parameters (σ, β, ν) are called the generating triplet of μ.

Remark 3.7. If we compare (3.7) with (3.8), we see that the formula (3.7) arising from the mod-Gaussian convergence in Example 3.4 is *not* an actual Lévy-Khintchine formula, because the function $x^2 \wedge 1$ is not integrable with respect to the measure $\frac{dx}{x(2\sinh(x/2))^2}$ (although $|x|^3 \wedge 1$ is); this explains why an additional second order term is required in the integrand.

Remark 3.8. The theorem above is the usual representation of the Fourier transform of an infinitely divisible probability distribution. There are many other ways of getting an integrable integrand with respect to the Lévy measure ν, and this will be important for us (see the discussion in [17, p. 38]).

Let h be a *truncation function*, that is a real function on $\mathbb{R}$, bounded, with conpact support, and such that $h(x) = x$ on a neighborhood of 0. Then for every $u \in \mathbb{R}$, $x \mapsto (e^{iux} - 1 - uh(x))$ is integrable with respect to ν, and (3.8) may be rewritten as:

$$\widehat{\mu}(u) = \exp\left[-\frac{1}{2}\sigma u^2 + i\beta_h u + \int_{\mathbb{R}} \left(e^{iux} - 1 - iuh(x)\right)\nu(dx)\right] \qquad (3.10)$$

where

$$\beta_h = \beta + \int_{-\infty}^{\infty} (h(x) - x\mathbb{1}_{|x|\leq 1})\nu(dx).$$

The triplet (σ, β_h, ν) is called the generating triplet of μ with respect to the truncation function h.

One can also express the moments of μ in terms of the Lévy measure ν. This is dealt with in Section 25 (p. 159 onwards) in [17]. For example one can show that $\int_{\mathbb{R}} |x|\mu(dx) < \infty$ if and only if $\int_{|x|>1} |x|\nu(dx) < \infty$. More generally, the measure μ admits a moment of order n if and only if $\int_{|x|>1} |x|^n \nu(dx) < \infty$; in this case, the cumulants (c_k) are related to the moments of ν as follows:

$$c_1 \equiv \int_{\mathbb{R}} x\mu(dx) = \gamma + \int_{|x|>1} x\nu(dx),$$

$$c_2 \equiv \int_{\mathbb{R}} x^2\mu(dx) - c_1^2 = \sigma + \int_{-\infty}^{\infty} x^2\nu(dx),$$

$$c_k = \int_{-\infty}^{\infty} x^k\nu(dx), \quad \text{for} \quad 3 \leq k \leq n.$$

In particular, if μ admits a first moment, then $\int_{|x|>1} |x|\nu(dx) < \infty$ and we can write:

$$\widehat{\mu}(u) = \exp\left[-\frac{1}{2}\sigma u^2 + ic_1 u + \int_{\mathbb{R}} \left(e^{iux} - 1 - iux\right)\nu(dx)\right]. \qquad (3.11)$$

3.3. **Mod-Gaussian convergence in the case of infinitely divisible variables.** Motivated by Example 3.4, we now consider the setting of Section 3.1 when the random variables forming the triangular array (X_i^n) are infinitely divisible. All other assumptions (concerning expectation, variance, third moment) remain in force; recall that μ_n is the law of the n-th row of the array and ϕ_n its characteristic function.

We will see that, in fact, when the probability measures μ_n are infinitely divisible, we can give an explicit representation of the limiting function Φ of Theorem 3.1 in terms of the generating triplets for the measures μ_n.

Indeed, using the results recalled in subsection 3.2, it is easily seen that in the current situation, we can write

$$\phi_n(u) = \exp(\psi_n(u)), \tag{3.12}$$

where

$$\psi_n(u) = -\frac{\sigma_n u^2}{2} + \int_{-\infty}^{\infty} \left(e^{iux} - 1 - iux\right) \nu_n(dx), \tag{3.13}$$

and

$$\int_{-\infty}^{\infty} x^2 \nu_n(dx) = 1 - \sigma_n \in [0,1], \qquad \int_{-\infty}^{\infty} |x|^3 \nu_n(dx) < \infty, \tag{3.14}$$

$$\sum_{n=1}^{\infty} \frac{1}{n^2} \int_{-\infty}^{\infty} |x|^3 \nu_n(dx) < \infty. \tag{3.15}$$

We now find a generalization of (3.7) in the present situation.

Theorem 3.9. *In the setting of Theorem 3.1, assume further that the probability measures μ_n are infinitely divisible and satisfy the conditions (3.12) up to (3.15). Then the sequence (Z_N) strongly converges in the mod-Gaussian sense, with the parameters $(0, H_N)$ and limiting function $\Phi = e^{\Psi}$, where*

$$\Psi(u) = \int_{-\infty}^{\infty} \left(e^{iux} - 1 - iux + \frac{u^2 x^2}{2}\right) \nu(dx)$$

and

$$\nu = \sum_{n=1}^{\infty} n\nu_n', \tag{3.16}$$

and the measures ν_n' are defined by

$$\nu_n'(A) = \int_{-\infty}^{\infty} \mathbb{1}_A(x/n)\nu_n(dx),$$

for any Borel set A. Consequently, ν is a positive measure which satisfies $\nu(\{0\}) = 0$ and $\int_{-\infty}^{\infty} |x|^3 \nu(dx) < \infty$.

Proof. With the notations of the proof of Theorem 3.1, and combining (3.3), (3.4) and (3.12)-(3.15) we have:

$$H_{0,N}(u) = \sum_{n=1}^{N} n \int_{-\infty}^{\infty} \left(e^{iux} - 1 - iux + \frac{u^2 x^2}{2}\right) \nu_n'(dx) \tag{3.17}$$

and the result of the theorem follows immediately, with

$$\int_{-\infty}^{\infty} |x|^3 \nu(dx) = \sum_{n=1}^{\infty} \frac{1}{n^2} \int_{-\infty}^{\infty} |x|^3 \nu_n(dx).$$

$\square$

3.4. **A criterion for mod-Gaussian convergence.** We now want to prove a general result characterizing the existence of mod-Gaussian convergence of a sequence (Z_N) such that the random variables Z_N are infinitely divisible. This is the analogue of the classical criterion for convergence in distribution of infinitely divisible random variables due to Gnedenko and Kolmogorov (see for example [17, Th. 8.7]).

Theorem 3.10. *Let (Z_N) be a sequence of real-valued random variables whose respective laws μ_N are infinitely divisible, with generating triplets (σ_N, b_N, ν_N) relative to a fixed continuous truncation function h.*

Then we have mod-Gaussian strong convergence if and only if the following two conditions hold:

(1) The sequence $\kappa_N = \int_{-\infty}^{\infty} h(x)^3 \nu_N(dx)$ converges to a finite limit κ;

(2) There exists a nonnegative measure ν satisfying

$$\nu(\{0\}) = 0, \quad \int_{\mathbb{R}} (x^4 \wedge 1)\nu(dx) < +\infty$$

and such that $\nu_N(f) \to \nu(f)$ for any continuous function f with $|f(x)| \le C(x^4 \wedge 1)$ for $x \in \mathbb{R}$ and some constant $C \ge 0$.

Under these conditions, one may take the parameters

$$\beta_N = b_N, \qquad \gamma_N = \sigma_N + \nu_N(h^2), \tag{3.18}$$

and the limiting function is then $\Phi = \exp(\Psi)$, where

$$\Psi(u) = -i\frac{u^3}{6}\kappa + \int_{-\infty}^{\infty} \left(e^{iux} - 1 - iuh(x) + \frac{u^2 h(x)^2}{2} + i\frac{u^3 h(x)^3}{6} \right) \nu(dx). \tag{3.19}$$

Proof. The left-hand side of (1.6) can be written, in our case, as $\exp(\Psi_N(u))$ where

$$\Psi_N(u) = iu(b_N - \beta_N) - \frac{u^2}{2}(\sigma_N - \gamma_N) + \int_{\mathbb{R}} (e^{iux} - 1 - iuh(x))\nu_N(dx) \tag{3.20}$$

$$= iu(b_N - \beta_N) - \frac{u^2}{2}(\sigma_N + \nu_N(h^2) - \gamma_N) - i\frac{u^3}{6}\kappa_N + \nu_N(k_u), \tag{3.21}$$

where

$$k_u(x) = e^{iux} - 1 - iuh(x) + \frac{u^2 h(x)^2}{2} + i\frac{u^3 h(x)^3}{6}. \tag{3.22}$$

(a) First assume that Conditions (1) and (2) above hold, and define β_N and γ_N by (3.18). Since h is bounded with compact support and $h(x) = x$ in a neighborhood of 0, it is easily seen that $|k_u(x)| \le C_u(x^4 \wedge 1)$, where C_u is a

constant depending on u. It thus follows from (3.21), (3.18) and Conditions (1) and (2) that $\Psi_N(u) \to \Psi(u)$, as defined by (3.19). Thus, it only remains to prove that we have $\nu_N(k_u) \to \nu(k_u)$ uniformly (with respect to u) on all compact sets $K \subset \mathbb{R}$. For this, we use fairly standard arguments.

Let K be a compact subset of $\mathbb{R}$, and let $\varepsilon > 0$ be fixed. For any $A > 1$, let

$$g_A(x) = \begin{cases} 0 & \text{if } -|x| < A \\ \frac{|x|}{A} - 1 & \text{if } A \le |x| \le 2A \\ 1 & \text{if } |x| > A, \end{cases}$$

and $h_A = 1 - g_A$. The function g_A is continuous with $0 \le g_A \le x^4 \wedge 1$, and $g_A \to 0$ pointwise as $A \to \infty$. Therefore we have the limits

$$\lim_{n \to +\infty} \nu_n(g_A) = \nu(g_A), \quad \lim_{A \to +\infty} \nu(g_A) = 0. \tag{3.23}$$

Now write

$$|\nu_n(k_u) - \nu(k_u)| \le |\nu_n(g_A k_u)| + |\nu(g_A k_u)| + |\nu_n(h_A k_u) - \nu(h_A k_u)|.$$

There exists a constant $C_K \ge 0$, depending only on K, such that

$$|k_u(x) g_A(x)| \le C_K g_A(x)$$

for all $u \in \mathbb{R}$, $x \in \mathbb{R}$. Consequently, combining the two limits in (3.23), we see that there exists $N_0 \ge 1$ and $B > 0$ such that, for any $N \ge N_0$, we have

$$|\nu_n(g_B k_u)| + |\nu(g_B k_u)| \le 2\varepsilon, \tag{3.24}$$

uniformly for $u \in \mathbb{R}$.

The other term, where now $A = B$ is fixed, is also easily dealt with. First, $k_u h_B$ is continuous and satisfies $|k_u(x) h_B(x)| \le C_u(x^4 \wedge 1)$, for some C_u depending on u, so that by assumption we have

$$\lim_{N \to +\infty} \nu_N(k_u h_B) = \nu(k_u h_B),$$

for any $u \in \mathbb{R}$. In addition, for each fixed x, the map

$$u \mapsto k_u(x) h_B(x)$$

is differentiable and its derivative is bounded by $D_K(x^4 \wedge 1)$ for $x \in \mathbb{R}$ and $u \in K$, the constant D_K depending only on K. Consequently, the function $u \mapsto \nu_N(k_u h_B)$ is differentiable on $\mathbb{R}$, and its derivative is uniformly bounded on the compact set K. It follows that the family of functions $(u \mapsto \nu_N(k_u h_B))_N$ is equicontinuous on K, and therefore its pointwise convergence to $\nu(k_u h_B)$ is uniform on K. Thus for some N_1, we have

$$|\nu_n(h_B k_u) - \nu(h_B k_u)| \le \varepsilon$$

for all $N \ge N_1$ and $u \in K$. From this and the previous estimate (3.24), the uniform convergence on compact sets follows.

(b) Conversely, we assume that (1.6) holds, locally uniformly in u, with some parameters (β_N, γ_N) and limiting function Φ. Since Φ is continuous and non-vanishing on some neighborhood $I = (-2\delta, 2\delta)$ of 0 and $\Phi(0) = 1$, it

follows from basic results of complex analysis (see, e.g., [17, Lemmas 7.6 and 7.7]) that on I we have $\Phi = \exp(\Psi)$, where Ψ is continuous with $\Psi(0) = 0$, and moreover Ψ_N, as defined by (3.21), converges to Ψ uniformly on I.

We deduce that, if θ is a locally bounded function on $\mathbb{R}$, we have

$$A_N(u) \;=\; \int_{-\delta}^{\delta} \left(\Psi_N(u+y) - \Psi_N(u)\right)\vartheta(y)dy$$

$$\to\; A(u) \;=\; \int_{-\delta}^{\delta} \left(\Psi(u+y) - \Psi(u)\right)\vartheta(y)dy \qquad (3.25)$$

for all u such that $|u| < \delta$.

Now, we observe that the orthogonality properties

$$\int_{-\delta}^{\delta} \vartheta(y)y\,dy = \int_{-\delta}^{\delta} \vartheta(y)y^2\,dy = 0 \quad \text{for} \quad \vartheta(y) = \frac{\delta^7}{105}\left(5y^2 - 3\delta^2\right), \quad (3.26)$$

together with Fubini's Theorem allow us to eliminate the terms involving $h(x)$, σ_N and b_N in (3.20), to yield

$$A_N(u) \;=\; \int_{\mathbb{R}} e^{iux}g(x)\nu_N(dx), \qquad (3.27)$$

where

$$g(x) \;=\; \int_{-\delta}^{\delta} \vartheta(y)(e^{ixy} - 1)dy$$

$$=\; \frac{\delta^7}{105}\left(\frac{8\delta^3}{3} + \frac{4\delta^2\sin(\delta x)}{x} + \frac{20\delta\cos(\delta x)}{x^2} - \frac{20\sin(\delta x)}{x^3}\right).$$

The function g is continuous and, as checked by straightforward calculus, satisfies

$$g(x) \sim x^4 \text{ as } x \to 0, \quad C^{-1}(x^4 \wedge 1) \le g(x) \le C(x^4 \wedge 1) \quad \forall x \in \mathbb{R}, \quad (3.28)$$

for some constant $C > 0$ (in particular, $g(x) = 0$ if and only if $x = 0$). Note that A_N is the Fourier transform of the positive finite measure $\mu_N(dx) = g(x)\nu_N(dx)$, and the convergence (3.25) for all u with $|u| \le \delta$ implies (see for example the proof of Theorem 19.1 in [8]) that the sequence of measures μ_N is relatively compact for the weak convergence (or, tight).

In particular, there is a subsequence (μ_{N_k}) which converges weakly to a positive finite measure μ. Then obviously Condition (2) is satisfied by the sequence (ν_{N_k}), with the limiting measure ν defined by

$$\nu(dx) \;=\; \frac{1}{g(x)}\mathbb{1}_{\mathbb{R}\setminus\{0\}}\,\mu(dx).$$

Next, we check that Condition (1) is satisfied by the subsequence (κ_{N_k}). To this end, we observe that the imaginary part of $\Psi_N(u)$, as given by (3.21),

can be written as follows:

$$\text{Im}(\Psi_N(u)) = u(b_N - \beta_N) + \int_{\mathbb{R}} (\sin(ux) - uh(x))\nu_N(dx)$$

$$= u(b_N - \beta_N) - \frac{u^3}{6}\,\kappa_N + \nu_N(\ell_u),$$

where

$$\ell_u(x) = \sin(ux) - uh(x) + \frac{u^3 h(x)^3}{6}.$$

Since $\Psi_N(u) \to \Psi(u)$, we have $\text{Im}(\Psi_N(u)) \to \text{Im}(\Psi(u))$ for all $u \in I$. The function ℓ_u is continuous and also satisfies $|\ell_u(x)| \le C_u(x^4 \wedge 1)$, for some constant $C_u \ge 0$, and hence $\nu_{N_k}(\ell_u) \to \nu(\ell_u)$. Consequently,

$$u(b_{N_k} - \beta_{N_k}) - \frac{u^3}{6}\,\kappa_{N_k} \;\to\; \text{Im}(\Psi(u)) - \nu(\ell_u)$$

as $k \to +\infty$, and for $u \in I$. Then obviously $\text{Im}(\Psi(u)) - \nu(\ell_u) = au + bu^3$ for some $a, b \in \mathbb{R}$, and it follows that $\kappa_{N_k} \to \kappa = 6b$. This proves Condition (1) for (κ_{N_k}).

To conclude the proof, we apply the sufficient condition (a) of our theorem to the subsequence (Z_{N_k}), which implies that $\Phi = e^\Psi$, where Ψ is given by (3.19). Therefore Φ does not vanish, and henceforth we can take $I = \mathbb{R}$ in the previous proof. We deduce that the convergence (3.25) holds for all $u \in \mathbb{R}$, and then Lévy's Theorem yields that not only is the sequence (μ_N) tight, but it actually converges to a limit μ. Therefore the previous proof holds for the original sequences (ν_N) and (κ_N), and we are done. $\qquad\square$

We now state as a corollary a weak limit theorem for variables satisfying the assumptions of Theorem 3.10. Of course, (1) below is a classical result.

Corollary 3.11. *Let Z_N be a sequence of infinitely divisible random variables satisfying one of the equivalent conditions of Theorem 3.10, with generating triplets $(0, 0, \nu_N)$. Then we have:*

(1) If $\nu_N(h^2) \to \widetilde{\sigma} \in [0, +\infty[$, then the sequence (Z_N) converges in law to a limit random variable Z, which is necessarily infinitely divisible, with generating triplet $(0, \sigma, \nu)$ with ν as in (3.19), but in this case $x^2 \wedge 1$ is integrable with respect to ν, and $\sigma = \widetilde{\sigma} - \nu(h^2)$.

(2) If $\nu_N(h^2) \to +\infty$, then $Z_N / \sqrt{\nu_N(h^2)}$ converges in law to the standard Gaussian random variable $\mathcal{N}(0, 1)$.

Proof. The results follow from the fact that under our assumptions, we have

$$e^{u^2 \nu_N(h^2)/2}\, \mathbb{E}[e^{iuZ_N}] \;\to\; \Phi(u)$$

locally uniformly for $u \in \mathbb{R}$. $\qquad\square$

4. Some examples of mod-Gaussian convergence in arithmetic

In this section, which is largely independent of the previous one, we give two examples of (unconditional) instances of mod-Gaussian convergence in analytic number theory. The first is quite elementary and formal. For the second (involving function fields), we again summarize briefly the required information to understand the statements, this time for probabilist readers. In addition, Section 4.3 explains how to interpret the Erdős-Kác theorem in terms of mod-Poisson convergence.

4.1. The arithmetic factor in the moment conjecture for $\zeta(1/2+it)$.

We come back to the moment conjecture (1.2) for the Riemann zeta function, which we recall: we should have

$$\lim_{T\to+\infty} \frac{1}{T(\log T)^{\lambda^2}} \int_0^T |\zeta(\tfrac{1}{2}+it)|^{2\lambda} dt = A(\lambda)M(\lambda)$$

for any complex number λ such that $\mathrm{Re}(\lambda) > -1$, where

$$M(\lambda) = \frac{G(1+\lambda)^2}{G(1+2\lambda)}, \qquad G(z) \text{ the Barnes double-gamma function,} \quad (4.1)$$

$$A(\lambda) = \prod_p \Big(1-\frac{1}{p}\Big)^{\lambda^2} \Big\{ \sum_{m\geq 0} \Big(\frac{\Gamma(m+\lambda)}{m!\Gamma(\lambda)}\Big)^2 p^{-m} \Big\}. \qquad (4.2)$$

From (1.5), it follows that the random matrix factor $M(iu)$, for $u \in \mathbb{R}$, occurs as the limiting function for the mod-Gaussian convergence of some natural sequence of random variables (namely, characteristic polynomials of random unitary matrices of growing size distributed according to Haar measure). It is thus natural to wonder whether the arithmetic factor has the same property, since, if that were the case, the formal properties of mod-Gaussian convergence (specifically, (3) in Proposition 2.3) imply that there exists a sequence of random variables which converges in mod-Gaussian sense with limiting function $A(iu)M(iu)$. We will show that this is the case (indeed with strong mod-Gaussian convergence); we believe this structure of the moments has arithmetic significance, although the computation we do now (though enlightening) does not yet explain this.

Proposition 4.1. *There exists a sequence (Z_N) of positive real-valued random variables and positive real numbers $\gamma_N > 0$ such that*

$$e^{u^2\gamma_N/2}\, \mathbb{E}(e^{iuZ_N}) \to A(iu)$$

locally uniformly for $u \in \mathbb{R}$.

Proof. We start by writing $A(iu)$ as a limit

$$A(iu) = \lim_{N\to+\infty} A_1(u,N)A_2(u,N)$$

where

$$A_1(u, N) = \prod_{p \leq N} (1 - p^{-1})^{-u^2}, \tag{4.3}$$

$$A_2(u, N) = \prod_{p \leq N} \sum_{m \geq 0} \left(\frac{\Gamma(m + iu)}{m! \Gamma(iu)} \right)^2 p^{-m} = \prod_{p \leq N} {}_2F_1(iu, iu; 1; p^{-1}), \tag{4.4}$$

by the definition of the Gauss hypergeometric function

$$_2F_1(a, b; c; z) = \sum_{k \geq 0} \frac{a(a+1)\cdots(a+k-1)b(b+1)\cdots(b+k-1)}{c(c+1)\cdots(c+k-1)} \frac{z^k}{k!}.$$

We now recall that

$$\prod_{p \leq N} (1 - p^{-1}) \sim e^{-\gamma} (\log N)^{-1}$$

as $N \to +\infty$, by the Mertens formula (see, e.g., [7, Th. 429]). Thus, it is natural to consider

$$\gamma_N = 2(\gamma + \log \log N) > 0, \qquad N \geq 2,$$

because we then have

$$\lim_{N \to +\infty} e^{u^2 \gamma_N / 2} A_2(u, N) = A(iu).$$

It is then enough to show that, for any $N \geq 2$, the factor $A_2(u, N)$ is the characteristic function $\mathbb{E}(e^{iuZ_N})$ of a random variable Z_N to deduce

$$\lim_{N \to +\infty} e^{u^2 \gamma_N / 2} \mathbb{E}(e^{iuZ_N}) = A(iu).$$

Furthermore, since $A_2(u, N)$ is defined as a product, it is enough to show that each hypergeometric factor ${}_2F_1(iu, iu; 1; p^{-1})$, p prime, is the characteristic function of a random variable X_p to obtain the desired result with Z_N the sum of independent variables distributed as X_p for $p \leq N$. Lemma 4.2 below, applied with $x = p$, checks that this is the case. Then, finally, the convergence is locally uniform because so is the convergence of the Euler product defining $A(iu)$. $\qquad\square$

Lemma 4.2. *Let X be a complex-valued random variable uniformly distributed over the unit circle, and let x be a real number with $x > 1$. Then we have*

$$\mathbb{E}(e^{iu(\log|1 - x^{-1/2}X|^{-2})}) = \mathbb{E}\left(|1 - x^{-1/2}X|^{-2iu} \right) = {}_2F_1(iu, iu; 1; x^{-1}).$$

Proof. With X as described, we have

$$\left| 1 - \frac{X}{\sqrt{x}} \right|^2 = 1 + \frac{1}{x} - \frac{2\operatorname{Re}(X)}{\sqrt{x}},$$

which is always $\geq (1 - x^{-1/2})^2 > 0$. Since $\mathrm{Re}(X)$ is distributed like $\cos\Theta$, where Θ is uniformly distributed on $[0, 2\pi]$, we have

$$\mathbb{E}(e^{iu \log |1 - x^{-1/2}X|^{-2}}) = \frac{1}{2\pi} \int_0^{2\pi} (1 + x^{-1} - 2x^{-1/2} \cos\theta)^{-iu} d\theta.$$

Now it is enough to apply [6, 9.112] (with $n = 0$, $p = iu$, $z = x^{-1/2}$) to see that this expression is exactly $_2F_1(iu, iu; 1; x^{-1})$. □

Remark 4.3. In view of (1.2) and the Euler product (formal) expansion

$$|\zeta(\tfrac{1}{2} + it)|^2 \text{ “}=\text{ ” } \prod_p \left|1 - \frac{1}{p^{1/2+it}}\right|^{-2},$$

the mod-Gaussian convergence of the arithmetic factor is described concretely as follows: let (X_p) be a sequence of independent random variables identically and uniformly distributed on the unit circle. Then the sequence of random variables defined by

$$\sum_{p \leq N} \log\left|1 - \frac{X_p}{\sqrt{p}}\right|^{-2} = \log \prod_{p \leq N} \left|1 - \frac{X_p}{\sqrt{p}}\right|^{-2}$$

converges as $N \to +\infty$, in the mod-Gaussian sense, with limiting function given by the arithmetic factor for the moments of $|\zeta(\tfrac{1}{2} + it)|^2$ in (1.2), evaluated at iu, and parameters $(0, 2\log(e^\gamma \log N))$.

Remark 4.4. The computations above are implicit in some earlier work, for instance in the paper [4] of Conrey, Farmer, Keating, Rubinstein and Snaith on refined conjectures for moments of L-functions.

4.2. **Some families of L-functions over function fields.** In this section, we give an example of mod-Gaussian convergence in the setting of families of L-functions, as developed by Katz and Sarnak [9]. We do not try to summarize the most general context in which they operate, in order to keep prerequisites from algebraic geometry to a minimum, concentrating on one concrete example which is already of great interest and can be explained "from scratch". It is the family of hyperelliptic curves, which is described in [9, §10.1.18, 10.8].

The fundamental result linking families of L-functions and Random Matrix Theory is the equidistribution theorem of Deligne, which we phrase (in the special case under consideration) in more probabilistic language than usual to clarify its meaning for probabilists. Its content is then that some sequences of random variables, defined arithmetically and taking values in the *set of conjugacy classes* in compact Lie groups such as $U(N)$, converge in law to the image on the space of conjugacy classes of the probability Haar measure on the group. Consequently, the values of the characteristic polynomials of such random variables are approximately distributed like the variables Z_N in the Keating-Snaith limit formula (1.1) for suitable values of N (or their analogues for other groups).

Let p be an odd prime number and let $q = p^n$, $n \geq 1$, be a power of p. We denote by $\mathbb{F}_q$ a field with q elements, in particular $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Recall from the theory of finite fields that if we fix an algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$, then for every $n \geq 1$ there exists a unique subfield $\mathbb{F}_{q^n}$ of $\bar{\mathbb{F}}_q$ which has order q^n (i.e., it is a field extension of degree n of $\mathbb{F}_q$), which is characterized as the set of $x \in \bar{\mathbb{F}}_q$ such that $x^{q^n} = x$.

Let $g \geq 1$ be an integer, and let $f \in \mathbb{F}_q[T]$ be a monic polynomial of degree $2g + 1$ with no repeated roots (in an algebraic closure $\bar{\mathbb{F}}_q$ of $\mathbb{F}_q$). Then the set C_f of solutions, in $\bar{\mathbb{F}}_q^2$, of the polynomial equation

$$C_f \,:\, y^2 = f(x) = x^{2g+1} + a_{2g}x^{2g} + \cdots + a_1 x + a_0, \qquad \text{(say)}.$$

is called an *affine hyperelliptic curve of genus g*. Taking the associated homogeneous equation in projective coordinates $[x : y : z]$, one gets the projective curve

$$\tilde{C}_f \,:\, y^2 z^{2g-1} = f(xz^{-1})z^{2g+1} = x^{2g+1} + a_{2g}zx^{2g} + \cdots + a_1 z^{2g}x + a_0 z^{2g+1},$$

which is still smooth and corresponds to C_f with an added point at infinity with projective coordinates $[0 : 1 : 0]$.

For every $n \geq 1$, denote by $\tilde{C}_f(\mathbb{F}_{q^n})$ the set of points in $\tilde{C}_f$ which have coordinates in the subfield $\mathbb{F}_{q^n}$ of $\bar{\mathbb{F}}_q$ (note that $\tilde{C}_f(\mathbb{F}_{q^n}) \simeq C_f(\mathbb{F}_{q^n}) \cup \{[0 : 1 : 0]\}$). The L-function $P_f(T)$ of $\tilde{C}_f$ (sometimes called the L-function of C_f instead) is then defined as the numerator of the zeta function $Z(\tilde{C}_f)$ defined by the formal power series expansion

$$Z(\tilde{C}_f) = \exp\Big(\sum_{n \geq 1} \frac{|\tilde{C}_f(\mathbb{F}_{q^n})|}{n} T^n\Big) = \exp\Big(\sum_{n \geq 1} \frac{|C_f(\mathbb{F}_{q^n})| + 1}{n} T^n\Big),$$

which is known to represent a rational function of the form

$$Z(\tilde{C}_f) = \frac{P_f(T)}{(1 - T)(1 - qT)},$$

which determines uniquely the L-function P_f.

The following properties of P_f were all proved by 1945, in particular thanks to the work of A. Weil on the Riemann Hypothesis for curves over finite fields:
– P_f is a polynomial with integer coefficients of degree $2g$, with $P_f(0) = 1$.
– [Functional equation (F.K. Schmidt)] We have the polynomial identity

$$q^g T^{2g} P_f\Big(\frac{1}{qT}\Big) = P_f(T).$$

– [Riemann Hypothesis (A. Weil)] If we write

$$P_f(T) = \prod_{1 \leq j \leq 2g} (1 - \alpha_{f,j}T), \qquad \alpha_{f,j} \in \mathbb{C}, \qquad (4.5)$$

then all the inverse roots $\alpha_{f,j}$ satisfy $|\alpha_{f,j}| = \sqrt{q}$.

The following property, which Weil could already prove in some form, is much better understood in the framework of algebraic geometry as developed in the 1960's by the Grothendieck school:

– [Spectral interpretation] There exists a well-defined conjugacy class F_f in the set $U(2g, \mathbb{C})^\sharp$ of conjugacy classes in the compact unitary group $U(2g, \mathbb{C})$ such that

$$P_f(T) = \det(1 - q^{1/2} T F_f) \qquad (4.6)$$

(this conjugacy class is the unitarized geometric Frobenius conjugacy class of $\tilde{C}_f$). Moreover, there exists a non-degenerate alternating form $\langle \cdot, \cdot \rangle$ on $\mathbb{C}^{2g}$ such that F_f is a conjugacy class in $USp(2g, \langle \cdot, \cdot \rangle)$, the unitary symplectic group of matrices which leave the alternating form invariant. Because any two non-degenerate alternating forms are conjugate over $\mathbb{C}$, we can (and will) see F_f as a well-defined conjugacy class in $USp(2g, \mathbb{C})$, the unitary symplectic group for the standard symplectic form.

Remark 4.5. If one makes the substitution $T = q^{-s}$, $s \in \mathbb{C}$, to define a complex-variable L-function

$$L(f, s) = P_f(q^{-s}), \qquad (4.7)$$

the functional equation and Riemann Hypothesis become exact analogues of the corresponding property and conjecture for the Riemann zeta function and its zeros, namely

$$L(f, s) = q^{2g(1/2 - s)} L(f, 1 - s),$$

and all zeros of $L(f, s)$ have real part equal to $\frac{1}{2}$.

The spectral interpretation, on the other hand, which implies that zeros of the L-function are eigenvalues of a unitary matrix (defined only up to conjugation), is much more mysterious for the Riemann zeta function. Note that the fact that F_f is in fact a symplectic conjugacy class implies the functional equation, by simple linear algebra.

Here is now one particular case of the Deligne Equidistribution Theorem.

Theorem 4.6 (Katz-Sarnak). *Fix an integer $g \geq 1$. For every power q of an odd prime p, let $\mathcal{H}_{g,q}$ be the set of monic polynomials in $\mathbb{F}_q[T]$ of degree $2g+1$ which have no multiple roots. Let $H_{g,q}$ be random variables with values in $USp(2g, \mathbb{C})^\sharp$ and with distributions given by*

$$\mathbb{P}(H_{g,q} = C) = \frac{1}{|\mathcal{H}_{g,q}|} |\{f \in \mathcal{H}_{g,q} \mid F_f = C\}| \qquad (4.8)$$

for any conjugacy class $C \in USp(2g, \mathbb{C})^\sharp$.

Then, as $q \to +\infty$, among odd powers of primes, the random variables $H_{g,q}$ converge in law to a random variable H_g distributed according to

$$\mathbb{P}(H_g \in A) = \mu_g(A), \qquad (4.9)$$

for any conjugacy-invariant measurable set A in $USp(2g, \mathbb{C})$, where μ_g is the probability Haar measure on $USp(2g, \mathbb{C})$. In other words, H_g is distributed

according to the image on the space of conjugacy classes of the probability Haar measure on $USp(2g, \mathbb{C})$.

Proof. This is exactly Theorem 10.8.2 of Katz and Sarnak [9],[2] taking the choice of α_k to be $\sqrt{|k|}$ so that the conjugacy class denoted $\vartheta(k, \alpha_k, C_f/k)$ is the same as the class F_f for $f \in \mathcal{H}_{g,|k|}$ (see the discussion in 10.7.2 of [9]), and the distribution (4.8) of $H_{g,q}$ is the same as the measure $\mu(hyp, 2g + 1, g, \mathbb{F}_q, \sqrt{q})$ as defined in 10.8.1 of [9]. $\qquad\square$

Remark 4.7. This result is derived by an application of Deligne's Equidistribution Theorem. Deligne's theorem is much more general: in fact, for *any* "algebraic" family of L-functions (a much more general notion that what we have described) there is always an equidistribution theorem which can be interpreted as convergence in law of random variables defined similarly to (4.8) for some conjugacy classes associated with the family, to a random variable distributed according to the image of the probability Haar measure on a group which can be interpreted as "the smallest group for which equidistribution may conceivably hold" (see [9, §9.2, 9.3, 9.7] for detailed discussions of various versions). Much of the work in applying Deligne's Equidistribution Theorem is concentrated in the determination of this group (often called the geometric monodromy group of the family). For the case of the family given by the $\mathcal{H}_{g,q}$ in Theorem 4.6, the content of the result is that this monodromy group is the whole symplectic group $Sp(2g)$, and this is proved in [9, Th. 10.1.18.3].

The following proposition is then immediate.

Proposition 4.8. *Let $g \geq 1$ be an integer. Let $H_{g,q}$ be random variables as in Theorem 4.6. For any $\lambda \in \mathbb{C}$ with $\mathrm{Re}(\lambda) > 0$, we have*

$$\lim_{g \to +\infty} \lim_{q \to +\infty} \frac{1}{g^{(\lambda^2+\lambda)/2}} \mathbb{E}(\det(1 - H_{g,q})^\lambda) = M_{Sp}(\lambda),$$

where

$$M_{Sp}(\lambda) = 2^{-\lambda^2/2} \left(\frac{\pi}{2}\right)^{\lambda/2} \frac{G(3/2)}{G(3/2 + \lambda)}$$

In particular, for any integer $k \geq 1$, we have

$$\lim_{g \to +\infty} \lim_{q \to +\infty} \frac{1}{g^{(k^2+k)/2}} \mathbb{E}(\det(1 - H_{g,q})^k) = \prod_{j=1}^{k} \frac{1}{(2j-1)!!}.$$

Proof. For $\mathrm{Re}(\lambda) > 0$, the function

$$x \mapsto \det(1 - x)^\lambda$$

---

[2] Except that there is a typo in their statement, namely in the right-hand side of line 13, $\mu(intrin, g, k_i, \alpha_{k_i})$ should be replaced by $\mu(hyp, d, g, k_i, \alpha_{k_i})$ and line 14 can be deleted.

is continuous and bounded on $USp(2g, \mathbb{C})^\sharp$; this is because, in terms of the eigenvalues $e^{i\theta_j}$ of $x \in USp(2g, \mathbb{C})$ arranged in pairs so that $\theta_{2g+1-j} = -\theta_j$, we have[3]

$$\det(1 - x) = \prod_{1 \leq j \leq g} |(1 - e^{i\theta_j})|^2 \geq 0.$$

Keating and Snaith [11, eq. (26) & (32)] have shown that

$$\lim_{g \to +\infty} g^{-(\lambda^2 + \lambda)/2} \, \mathbb{E}(\det(1 - H_g)^\lambda) = 2^{\lambda^2/2} \frac{G(1 + \lambda)\sqrt{\Gamma(1 + \lambda)}}{\sqrt{G(1 + 2\lambda)\Gamma(1 + 2\lambda)}} \quad (4.10)$$

for any complex number λ with $\mathrm{Re}(\lambda) > -1$, and therefore the statement is a direct consequence of convergence in law of $H_{g,q}$ to H_g once we prove that our expression for $M_{Sp}(\lambda)$ coincides with this value. This, however, is easy to check: using the duplication formula for $G(z)$ in the form

$$G(\tfrac{1}{2})^2 G(2z) = (2\pi)^{-z} 2^{2z^2 - 2z + 1} \Gamma(z) (G(z)G(z + \tfrac{1}{2}))^2$$

one can rewrite the function in the square-root of the denominator of the Keating-Snaith expression as

$$\Gamma(1 + 2\lambda)G(1 + 2\lambda) = G(2(1 + \lambda)) = (2\pi)^{-(\lambda+1)} 2^{2(\lambda+1)^2 - 2(\lambda+1)+1}$$
$$\Gamma(1 + \lambda)\Big(\frac{G(1 + \lambda)G(3/2 + \lambda)}{G(\tfrac{1}{2})} \Big)^2,$$

and deduce the result after a short computation.

The last expression for $M_{Sp}(k)$ is equation (34) in [11] and follows also from the definition of $M_{Sp}(\lambda)$ using $G(z + 1) = \Gamma(z)G(z)$ and the formula

$$\Gamma(k + \tfrac{1}{2}) = \frac{(2k - 1)!!}{2^k}\sqrt{\pi},$$

for $k \geq 0$ integer. $\square$

We can not argue quite so quickly to derive a mod-Gaussian convergence result because the random variables $\log \det(1 - H_{g,q})$ are not defined whenever $H_{g,q}$ has an eigenvalue 1, and this can occur with positive probability. Indeed, by (4.6) and (4.5), we have

$$\det(1 - F_f) = P_f(q^{-1/2}) = \prod_{1 \leq j \leq 2g} (1 - q^{-1/2}\alpha_{f,j})$$

for any $f \in \mathcal{H}_{g,q}$, and so the issue is whether $\sqrt{q}$ is a zero of $Z(C_f)$ (equivalently, whether $L(f, 1/2) = 0$), and this may well happen (e.g., if $q = p^2$ with $p \equiv 3 \,(\mathrm{mod}\, 4)$, for the curve $E : y^2 = x^3 - x$, it is well-known, and easy to show, that $P_E(T) = (1 - pT)^2$).

Nevertheless, it is not too hard to prove the following:

---

[3] This is an analogue of the non-negativity of the central special value $L(f, 1/2)$ for any self-dual L-function, which is implied by the Riemann Hypothesis.

Proposition 4.9. *Let $g \geq 1$ be an integer. For any power $q \neq 1$ of an odd prime p, let $\tilde{\mathcal{H}}_{g,q}$ be the subset of those $f \in \mathcal{H}_{g,q}$ such that $L(f, 1/2) = P_f(q^{-1/2}) \neq 0$.*

(1) Let $I_{g,q}$ be random variables with values in $USp(2g, \mathbb{C})^{\sharp}$ such that

$$\mathbb{P}(I_{g,q} = C) = \frac{1}{|\tilde{\mathcal{H}}_{g,q}|} |\{f \in \tilde{\mathcal{H}}_{g,q} \mid F_f = C\}|$$

for any $C \in USp(2g, \mathbb{C})^{\sharp}$. Then $I_{g,q}$ converges in law to H_g as $q \to +\infty$.

(2) Let $L_{g,q} = \log \det(I - I_{g,q})$ which is a well-defined real-valued random variable. We have the mod-Gaussian convergence

$$\lim_{g \to +\infty} \lim_{q \to +\infty} g^{-iu/2 + u^2/2} \, \mathbb{E}(e^{iuL_{g,q}}) = M_{Sp}(iu),$$

for any $u \in \mathbb{R}$.

Note that we have here mod-Gaussian convergence with parameters given by $(\frac{1}{2} \log g, \log g)$.

Proof. (1) If φ is a bounded continuous function on $USp(2g, \mathbb{C})^{\sharp}$, we have

$$|\mathbb{E}(\varphi(I_{g,q})) - \mathbb{E}(\varphi(H_{g,q}))| \leq \|\varphi\|_{\infty} \, \mathbb{P}(\det(1 - H_{g,q}) = 0) = \|\varphi\|_{\infty} \, \mathbb{P}(H_{g,q} \in A_g),$$

where $A_g = \{x \in USp(2g, \mathbb{C})^{\sharp} \mid \det(1 - x) = 0\}$. This set A_g is a closed set with empty interior, hence boundary equal to A_g, which has Haar measure zero. By Theorem 4.6 and the standard properties of convergence in law, we have

$$\lim_{q \to +\infty} \mathbb{P}(H_{g,q} \in A_g) = \mathbb{P}(H_g \in A_g) = 0,$$

and it follows then that

$$\lim_{q \to +\infty} \mathbb{E}(\varphi(I_{g,q})) = \mathbb{E}(\varphi(H_{g,q})),$$

which justifies the convergence in law of $I_{g,q}$.

(2) For $f \in \tilde{\mathcal{H}}_{g,q}$, we have $\det(1 - F_f) > 0$, and therefore the definition of the law of $I_{g,q}$ shows that $L_{g,q}$ is well-defined. Because of the Keating-Snaith limit formula (4.10), valid for all complex numbers with $\mathrm{Re}(\lambda) > -1$, it is enough to show that, for all $u \in \mathbb{R}$, we have

$$\lim_{q \to +\infty} \mathbb{E}(e^{iuL_{g,q}}) = \mathbb{E}(\det(1 - H_g)^{iu}).$$

The function φ on $USp(2g, \mathbb{C})^{\sharp}$ defined by

$$x \mapsto \begin{cases} 0, & \text{if } \det(1 - x) = 0 \\ \det(1 - x)^{iu}, & \text{otherwise,} \end{cases}$$

is bounded and its set of points of discontinuity is the set A_g of Haar-measure 0. By a fairly standard result on convergence in law, this and the convergence in law of $I_{g,q}$ to H_g suffice to ensure that

$$\lim_{q \to +\infty} \mathbb{E}(\varphi(I_{g,q})) = \mathbb{E}(\varphi(H_g))$$

(see, e.g., [2, Ch. 4, §5, n°12, Prop. 22], properly translated, or one can of course do the necessary ε management by hand). By definition, the left-hand side is $\mathbb{E}(e^{iuL_{g,q}})$, while the right-hand side is $\mathbb{E}(\det(1 - H_g)^{iu})$ (since A_g has measure zero, once more). $\square$

Remark 4.10. Although we used the example of the family $\mathcal{H}_{g,q}$ in this section, it is clear from the proofs that the argument goes through with no change for any family with symplectic monodromy, and that suitable analogues will hold for families with unitary or (with a bit more care because of the issue of forced vanishing at the critical point) with orthogonal symmetry.

Remark 4.11. In terms of L-functions as defined in (4.7), we can rephrase the last limit as follows:

$$\lim_{g\to+\infty} \lim_{q\to+\infty} \frac{g^{u^2/2}}{|\tilde{\mathcal{H}}_{g,q}|} \sum_{f\in\tilde{\mathcal{H}}_{g,q}} \Big(\frac{L(f,1/2)}{\sqrt{g}} \Big)^{iu} = M_{Sp}(iu).$$

It remains a big problem to obtain results of this type without the inner limit over q, which already transforms the arithmetic to a pure "random matrix" problem by the magic of Deligne's equidistribution theorem (see the comments and conjectures in [9, p. 12, 13], in particular Example (2), p. 13). However, Faifman and Rudnick [5] and Kurlberg and Rudnick [13] have recently given examples of problems where it is possible to understand the limit $g \to +\infty$ for fixed q.

In this situation, by analogy with Section 4.1, one may expect to have a mod-Gaussian limit theorem with an extra "arithmetic" factor. More precisely, one can make the following conjecture:

Conjecture 4.12. *For fixed odd q, we have*

$$\lim_{g\to+\infty} \frac{g^{u^2/2-iu/2}}{|\tilde{\mathcal{H}}_{g,q}|} \sum_{f\in\tilde{\mathcal{H}}_{g,q}} |L(f,1/2)|^{iu} = M_{Sp}(iu)A_h(iu)$$

locally uniformly for $u \in \mathbb{R}$ and also

$$\lim_{g\to+\infty} \frac{g^{-\lambda(\lambda+1)/2}}{|\tilde{\mathcal{H}}_{g,q}|} \sum_{f\in\tilde{\mathcal{H}}_{g,q}} |L(f,1/2)|^{\lambda} = M_{Sp}(\lambda)A_h(\lambda)$$

for all real $\lambda > 0$, where

$$A_h(\lambda) = \prod_{\pi} \Big(1 - \frac{1}{|\pi|} \Big)^{\lambda(\lambda+1)/2} \times$$
$$\Big(1 + \frac{1}{2}\frac{1}{1+|\pi|^{-1}} \Big\{ \Big(1 - \frac{1}{\sqrt{|\pi|}}\Big)^{-\lambda} - 1 + \Big(1 + \frac{1}{\sqrt{|\pi|}}\Big)^{-\lambda} - 1 \Big\} \Big),$$

the product extending over all irreducible monic polynomials $\pi \in \mathbb{F}_q[T]$, and $|\pi| = q^{\deg(\pi)}$ denoting the norm of π.

The shape of arithmetic factors is motivated by the fact (essentially observed by Kurlberg and Rudnick) that for a fixed π, the π-factor of the Euler product representing $L(f, \frac{1}{2})$ converges in law to

$$(1 - T_\pi |\pi|^{-1/2})^{-1}$$

where T_π is a trinomial random variable taking value 0 with probability $\frac{1}{1+|\pi|}$ and values ± 1 with equal probability $\frac{1}{2}\left(1 - \frac{1}{|\pi|+1}\right)$; the inner parenthesis on the right of the arithmetic factor is, of course, equal to $\mathbb{E}((1 - T_\pi |\pi|^{-1/2})^{-\lambda})$ (as one sees after rearrangement of the latter).

4.3. **The number of prime divisors of an integer.** A classical result of Erdős and Kác states (as a particular case) that the arithmetic function $\omega(n)$, the number of (distinct) prime divisors of a positive integer $n \geq 1$, behaves for large n like a Gaussian random variable with mean $\log \log n$ and variance $\log \log n$, in the sense that

$$\lim_{N \to +\infty} \frac{1}{N} |\{n \leq N \mid a < \frac{\omega(n) - \log \log N}{\sqrt{\log \log N}} < b\}| = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} dt \quad (4.11)$$

for any real numbers $a < b$.

This phenomenon where increasing variance is observed suggests, in the context of this paper, to look at the behavior of $\omega(n)$ over $n \leq N$ without normalizing. However, mod-Gaussian behavior is excluded here because of the following easy remark:

Proposition 4.13. *Let (Z_N) be a sequence of* integer valued *random variables. Then (Z_N) does not converges in the mod-Gaussian sense with respect to any unbounded parameters (γ_N).*

Proof. The point is that the characteristic functions

$$\mathbb{E}(e^{iuZ_N})$$

are 2π-periodic for all N if the Z_N take only integral values. If $u = 2\pi$ (or any other non-zero integral multiple of 2π) then the limit (1.6) implies

$$\lim_{N \to +\infty} e^{\gamma_N/2} = |\Phi(1)|,$$

and (since $\gamma_N \geq 0$) the existence of this limit implies that γ_N converges to $\gamma \geq 0$. $\qquad\square$

However, it turns out that there is mod-Poisson convergence, in the sense sketched in Section 2.2. For this, it seems slightly more appropriate to consider

$$\omega'(n) = \omega(n) - 1 \quad (4.12)$$

for $n \geq 2$, because Poisson random variables takes all integral values ≥ 0, whereas $\omega(n) \geq 1$ for any $n \geq 2$ (of course, (4.11) is valid for $\omega'(n)$ also).

To state the result precisely, recall that a Poisson random variable P_λ with parameter $\lambda > 0$ is one taking (almost surely) integer values $k \geq 0$ with

$$\mathbb{P}(P_\lambda = k) = \frac{\lambda^k}{k!} e^{-\lambda}.$$

The characteristic function is then given by

$$\mathbb{E}(e^{iuP_\lambda}) = \exp(\lambda(e^{iu} - 1)),$$

and strong mod-Poisson convergence of a sequence Z_N of random variables with parameters λ_N means that the limit

$$\lim_{N \to +\infty} \exp(\lambda_N(1 - e^{iu})) \, \mathbb{E}(e^{iuZ_N}) = \Phi(u)$$

exists for every $u \in \mathbb{R}$, and the convergence is locally uniform. The *limiting function* Φ is then continuous and $\Phi(0) = 1$.

Proposition 4.14. *For $u \in \mathbb{R}$, let*

$$\Phi(u) = \frac{1}{\Gamma(e^{iu} + 1)} \prod_p \left(1 - \frac{1}{p}\right)^{e^{iu}} \left(1 + \frac{e^{iu}}{p - 1}\right). \tag{4.13}$$

This Euler product is absolutely and locally uniformly convergent. Moreover, for any $u \in \mathbb{R}$, we have

$$\lim_{N \to +\infty} \frac{(\log N)^{(1 - e^{iu})}}{N} \sum_{2 \leq n \leq N} e^{iu\omega'(n)} = \Phi(u),$$

and the convergence is locally uniform.

Proof. Since

$$\frac{1}{N - 1} \sum_{2 \leq n \leq N} e^{iu\omega'(n)} = e^{-iu} \times \frac{1}{N} \sum_{1 \leq n \leq N} e^{iu\omega(n)} + O(1),$$

for $N \geq 2$, this is in fact a simple reinterpretation of a direct application of the Delange-Selberg method (see, e.g., [18, II.5, Theorem 3]) to the multiplicative function $n \mapsto e^{iu\omega(n)}$. The details are explained in [18, II.6, Theorem 1] (take $N = 0$, $z = e^{iu}$, $A = 1$ there, and apply $\lambda_0(z) = 1$ to get the formula

$$\frac{1}{\Gamma(e^{iu})} G_1(1; e^{iu}) = \frac{1}{\Gamma(e^{iu})} \prod_p \left(1 - \frac{1}{p}\right)^{e^{iu}} \left(1 + \frac{e^{iu}}{p - 1}\right)$$

for the limit, which is in the notation of loc. cit., with $G_1(s; z)$ defined on the last line of p. 201 of [18], its analytic continuation to $\mathrm{Re}(s) > 1/2$ being described on p. 202). Multiplying by e^{-iu}, we obtain the stated result using $e^{iu}\Gamma(e^{iu}) = \Gamma(e^{iu} + 1)$. $\qquad\square$

Corollary 4.15. *Consider random variables M_N, for $N \geq 2$, such that*

$$\mathbb{P}(M_N = n) = \frac{1}{N - 1}, \qquad 2 \leq n \leq N,$$

and let $Z_N = \omega'(M_N)$. Then the sequence (Z_N) converges strongly in the mod-Poisson sense with limiting function Φ given by (4.13) and parameters $\lambda_N = \log \log N$.

Proof. This follows directly from the proposition and the definition of strong mod-Poisson convergence, since we have $\mathbb{E}(e^{iuP_{\lambda_N}})^{-1} = (\log N)^{(1-e^{iu})}$. $\square$

The analogue of Corollary 3.3 is then the theorem of Erdős and Kác:

Corollary 4.16. *The Gaussian limit (4.11) holds.*

Proof. With notation as in Corollary 4.15, we must show that

$$Y_N = \frac{\omega(M_N) - \log \log N}{\sqrt{\log \log N}}$$

converges in law to a standard Gaussian variable (with a shift from N to $N + 1$ which is immaterial). The argument is again quite standard, but we spell it out in detail.

Let $u \in \mathbb{R}$ be fixed; the characteristic function of Y_N is

$$\mathbb{E}(e^{iuY_N}) = \exp(-iu\sqrt{\log \log N})\,\mathbb{E}(e^{it\omega(M_N)})$$
$$= \exp(-iu\sqrt{\log \log N} + it)\,\mathbb{E}(e^{it\omega'(M_N)}) \qquad (4.14)$$

where

$$t = \frac{u}{\sqrt{\log \log N}}$$

(note that t depends on N and $t \to 0$ when $N \to +\infty$).

By Proposition 4.14, in particular the uniform convergence with respect to u, we have

$$\lim_{N \to +\infty} (\log N)^{1-e^{it}}\,\mathbb{E}(e^{it\omega'(M_N)}) = \Phi(0) = 1. \qquad (4.15)$$

Moreover, we have for $N \geq 1$

$$(\log N)^{e^{it}-1} = \exp((e^{it} - 1)\log \log N)$$
$$= \exp((it - t^2/2 + O(t^3))\log \log N)$$
$$= \exp\Big(iu\sqrt{\log \log N} - \frac{u^2}{2} + O\Big(\frac{u^3}{\sqrt{\log \log N}}\Big)\Big). \qquad (4.16)$$

Writing (4.14) as

$$\exp(-iu\sqrt{\log \log N} + it) \times (\log N)^{e^{it}-1} \times (\log N)^{1-e^{it}}\,\mathbb{E}(e^{it\omega'(M_N)}),$$

we see from (4.15) and (4.16) that this is

$$\exp\Big(-\frac{u^2}{2} + O\Big(\frac{u^3}{\sqrt{\log \log N}}\Big)\Big)(1 + o(1)) \to \exp\Big(-\frac{u^2}{2}\Big), \quad \text{as} \quad N \to +\infty,$$

and by Lévy's criterion, this concludes the proof. $\square$

In fact, this proof is essentially the one of Rényi and Turán [16], who simply did not isolate Proposition 4.14 as a separate statement of interest (and proved directly the version of the Delange-Selberg needed in this case, see equation (1.31) in loc. cit.).

Remark 4.17. It is also natural to use Poisson variables because the asymptotic formula

$$\frac{1}{N}|\{n \leq N \mid \omega'(n) = k\}| \sim \frac{1}{\log N}\frac{(\log\log N)^k}{k!}$$

holds as $N \to +\infty$, for fixed $k \geq 0$ (the uniformity with respect to k, as shown first by Sathe and Selberg, is a quite delicate issue, see, e.g., [18, II.6, Theorem 4]), so that $\omega'(n)$ is again seen to be "approximately" Poisson with parameter $\log\log N$.

Our focus here is on arithmetic behavior, but it is interesting to note a phenomenon similar (though apparently simpler) to what happens for the Moment Conjecture for $\zeta(1/2 + it)$, namely, that the limiting function $\Phi(u)$ takes the form of a product

$$\Phi(u) = \Phi_1(u)\Phi_2(u)$$

with

$$\Phi_1(u) = \frac{1}{\Gamma(e^{iu} + 1)}, \qquad \Phi_2(u) = \prod_p \left(1 - \frac{1}{p}\right)^{e^{iu}-1}\left(1 - \frac{1}{p}\right)\left(1 + \frac{e^{iu}}{p-1}\right),$$

and we can see the Euler product Φ_2 as an instance of a natural asymptotic probabilistic model of primes, while Φ_1 comes from a seemingly unrelated model which has some group-theoretic origin.

Indeed, for the first factor $\Phi_1(u) = \Gamma(e^{iu}+1)^{-1}$, appealing to the classical formula

$$\frac{1}{\Gamma(e^{iu} + 1)} = \prod_{k \geq 1}\left(1 + \frac{e^{iu}}{k}\right)\left(1 + \frac{1}{k}\right)^{-e^{iu}}$$

for any $u \in \mathbb{R}$ (due to Euler; see [19, 12.11]), we can compute this as follows:

$$\Phi_1(u) = \lim_{N \to +\infty} \prod_{k \leq N}\left(1 + \frac{1}{k}\right)^{1-e^{iu}}\left(1 + \frac{1}{k}\right)^{-1}\left(1 + \frac{e^{iu}}{k}\right)$$

$$= \lim_{N \to +\infty} \exp(\lambda_N(1 - e^{iu}))\prod_{k \leq N}\left(1 + \frac{1}{k}\right)^{-1}\left(1 + \frac{e^{iu}}{k}\right)$$

$$= \lim_{N \to +\infty} \exp(\lambda_N(1 - e^{iu}))\,\mathbb{E}(e^{iuZ_N}),$$

where

$$\lambda_N = \sum_{1 \leq k \leq N}\log(1 + k^{-1}) = \log(N + 1),$$

and Z_N is the sum

$$Z_N = B_1 + B_2 + \cdots + B_N,$$

with B_k denoting independent Bernoulli random variables with distribution

$$\mathbb{P}(B_k = 1) = 1 - \frac{1}{1 + \frac{1}{k}} = \frac{1}{k+1}, \qquad \mathbb{P}(B_k = 0) = \frac{1}{1 + \frac{1}{k}} = \frac{k}{k+1}.$$

This distribution is also found, for instance, as the distribution of $K_{N+1} - 1$, where K_{N+1} is the number of cycles of a permutation $\sigma \in \mathfrak{S}_N$, distributed according to the uniform measure on the symmetric group (see, e.g., [1, §4.6]; we observe in particular that this gives another instance of natural mod-Poisson convergence explaining some type of normal limit). So here we see random permutations occuring as explaining the "transcendental" factor $\Phi_1(u)$; in [12], this phenomenon is explored in greater depth.

For the arithmetic factor $\Phi_2(u)$, we argue (much as in Section 4.1) that

$$\Phi_2(u) = \lim_{y \to +\infty} \prod_{p \le y} \left(1 - \frac{1}{p}\right)^{e^{iu}-1} \left(1 - \frac{1}{p}\right)\left(1 + \frac{e^{iu}}{p-1}\right),$$

and by isolating the first term, it follows that

$$\Phi_2(u) = \lim_{y \to +\infty} \exp((1 - e^{iu})\lambda_y) \prod_{p \le y} \left(1 - \frac{1}{p} + \frac{1}{p}e^{iu}\right)$$
$$= \lim_{y \to +\infty} \mathbb{E}(e^{iuP_{\lambda_y}})^{-1} \, \mathbb{E}(e^{iuZ'_y})$$

where

$$\lambda_y = \sum_{p \le y} \log(1 - p^{-1})^{-1} = \sum_{\substack{p \le y \\ k \ge 1}} \frac{1}{kp^k} \sim \log\log y, \qquad \text{as } y \to +\infty,$$

and

$$Z'_y = \sum_{p \le y} B'_p \tag{4.17}$$

is a sum of independent Bernoulli random variables with parameter $1/p$:

$$\mathbb{P}(B'_p = 1) = \frac{1}{p}, \qquad \mathbb{P}(B'_p = 0) = 1 - \frac{1}{p}.$$

The parameters of these Bernoulli laws correspond exactly to the "intuitive" probability that an integer n be divisible by p, or in other words to the model limit

$$\lim_{x \to +\infty} \frac{1}{x} \sum_{\substack{n \le x \\ n \equiv 0 \,(\mathrm{mod}\, p)}} 1 = \frac{1}{p},$$

and the independence of the B'_p corresponds to the formal (algebraic) independence of the divisiblity by distinct primes given, e.g., by the Chinese Remainder Theorem.

Since the analogue of Proposition 2.3, (3), is trivially valid for mod-Poisson convergence, we also recover in this manner (without arithmetic) the fact that the limiting function $\Phi(u)$ arises from mod-Poisson convergence.

As in the case of the Riemann zeta function, we note that the independent model fails to capture the truth on the distribution of $\omega(n)$, the extent of this failure being given by the factor $\Phi_1(u)$. Because

$$\frac{Z'_y - \log\log y}{\sqrt{\log\log y}} \xrightarrow{law} \mathcal{N}(0,1)$$

(with the right-hand side being a standard normal random variable), this discrepancy between the independent model and the arithmetic truth is invisible at the level of the normalized convergence in distribution.

Remark 4.18. Computations similar to the above show that, for any sequence (x_n) of positive real numbers with

$$\sum_{n\geq 1} x_n = +\infty, \qquad \sum_{n\geq 1} x_n^2 < +\infty, \tag{4.18}$$

if we denote now by (B_n) a sequence of independent Bernoulli random variables with

$$\mathbb{P}(B_n = 1) = x_n, \qquad \mathbb{P}(B_n = 0) = 1 - x_n,$$

then the random variables

$$Z_N = B_1 + \cdots + B_N$$

have mod-Poisson convergence with parameters

$$\lambda_N = x_1 + \cdots + x_N,$$

and with limiting function given by

$$u \mapsto \prod_{n\geq 1}(1 + x_n(e^{iu} - 1))\exp(x_n(1 - e^{iu})) \ ;$$

the (uniform) convergence of this infinite product is ensured by the second condition in (4.18), after expanding in terms of x_n (which tends to 0 as $n \to +\infty$).

References

[1] R. Arratia, A.D. Barbour and S. Tavaré: *Logarithmic combinatorial structures: a probabilistic approach*, E.M.S. Monographs, 2003.

[2] N. Bourbaki: *Intégration*, Chapters 1, 2, 3, 4, 2nd edition, Hermann, 1965.

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

[4] J.B. Conrey, D. Farmer, J. Keating, M. Rubinstein and N. Snaith: *Integral moments of L-functions*, Proc. London Math. Soc. 91 (2005), 33–104.

[5] D. Faifman and Z. Rudnick: *Statistics of the zeros of zeta functions in families of hyperelliptic curves over a finite field*, Composition Math. 146 (2010), 81–101; arXiv:0803.3534.

[6] I.S. Gradshteyn and I.M. Ryzhik: *Table of integrals, series, and products*, 5th edition, Academic Press, 1994.

[7] G.H. Hardy and E.M. Wright: *An introduction to the theory of numbers*, 5th Edition, Oxford Univ. Press, 1979.

[8] J. Jacod and P. Protter: *Probability essentials*, Springer, 2nd Edition, 2003.

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

[10] J.P. KEATING AND N.C. SNAITH: *Random matrix theory and $\zeta(1/2 + it)$*, Commun. Math. Phys. **214**, (2000), 57-89.

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

[12] 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`.

[13] P. KURLBERG AND Z. RUDNICK: *The fluctuations in the number of points on a hyperelliptic curve over a finite field*, Journal Number Th. 129 (2009), 580–587; `arXiv:0804.0808`.

[14] F. MEZZADRI AND N.C. SNAITH (EDITORS): *Recent Perspectives in Random Matrix Theory and Number Theory*, LMS Lecture Notes **322**, Cambridge Univ. Press, 2005.

[15] A. NIKEGHBALI AND M. YOR: *The Barnes G function and its relations with sums and products of generalized Gamma variables*, Electron. Commun. Probab. 14 (2009), 396–411; `arXiv:0707.3187`.

[16] A. RÉNYI AND P. TURÁN: *On a theorem of Erdős-Kác*, Acta Arith. 4 (1958), 71–84.

[17] K. SATO: *Lévy processes and infinitely divisible distributions*, Cambridge Studies Adv. Math. **68**, Cambridge Univ. Press, 1999.

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

[19] E.T. WHITTAKER AND G.N. WATSON: *A course in modern analysis*, 4th Edition, Cambridge Math. Library, Cambridge Univ. Press, 1996.

[20] A. ZYGMUND: *Trigonometric series*, 2nd Edition, Vol. I, Cambridge Math. Library, Cambridge Univ. Press, 1988.

INSTITUT DE MATHÉMATIQUES DE JUSSIEU, UNIVERSITÉ PIERRE ET MARIE CURIE, ET C.N.R.S. UMR 7586, 175, RUE DU CHEVALERET, F-75013 PARIS, FRANCE
E-mail address: `jean.jacod@upmc.fr`

ETH ZÜRICH – D-MATH, RÄMISTRASSE 101, 8092 ZÜRICH, SWITZERLAND
E-mail address: `kowalski@math.ethz.ch`

INSTITUT FÜR MATHEMATIK, UNIVERSITÄT ZÜRICH, WINTERTHURERSTRASSE 190, CH-8057 ZÜRICH, SWITZERLAND
E-mail address: `ashkan.nikeghbali@math.uzh.ch`