Mod-poisson convergence in probability and number theory

Kowalski, E ; Nikeghbali, A

Abstract: Building on earlier work introducing the notion of "mod-Gaussian" convergence of sequences of random variables, which arises naturally in Random Matrix Theory and number theory, we discuss the analogue notion of "mod-Poisson" convergence. We show in particular how it occurs naturally in analytic number theory in the classical Erdős– Kac Theorem. In fact, this case reveals deep connections and analogies with conjectures concerning the distribution of L functions on the critical line, which belong to the mod-Gaussian framework, and with analogues over finite fields, where it can be seen as a zero-dimensional version of the Katz–Sarnak philosophy in the "large conductor" limit.

DOI: https://doi.org/10.1093/imrn/rnq019

MOD-POISSON CONVERGENCE IN PROBABILITY AND NUMBER THEORY

E. KOWALSKI AND A. NIKEGHBALI

Abstract. Building on earlier work introducing the notion of "mod-Gaussian" convergence of sequences of random variables, which arises naturally in Random Matrix Theory and number theory, we discuss the analogue notion of "mod-Poisson" convergence. We show in particular how it occurs naturally in analytic number theory in the classical Erdős-Kac Theorem. In fact, this case reveals deep connections and analogies with conjectures concerning the distribution of L-functions on the critical line, which belong to the mod-Gaussian framework, and with analogues over finite fields, where it can be seen as a zero-dimensional version of the Katz-Sarnak philosophy in the "large conductor" limit.

1. Introduction

In our earlier paper [12] with J. Jacod,[1] motivated by results from Random Matrix Theory and probability, we have introduced the notion of mod-Gaussian convergence of a sequence of random variables (Z_N). This occurs when the sequence does not (typically) converge in distribution, so the sequence of characteristic functions does not converge pointwise to a limit characteristic function, but nevertheless, the characteristic functions decay precisely like a suitable Gaussian, i.e., the limits

$$\lim_{N\to+\infty} \exp(-iu\beta_N + u^2\gamma_N/2)\,\mathbf{E}(e^{iuZ_N}) \tag{1.1}$$

exist, locally uniformly for $u \in \mathbf{R}$, for some parameters $(\beta_N, \gamma_N) \in \mathbf{R} \times [0, +\infty[$.

Besides giving natural and fairly general instances of such behavior in probability theory, we investigated arithmetic instances of it. In that respect, we noticed that the limits (1.1) can not exist if the random variables Z_N are integer-valued, since the characteristic functions $\mathbf{E}(e^{iuZ_N})$ are then 2π-periodic, and we discussed briefly the possibility of introducing "mod-Poisson convergence", that may be applicable to such situations. Indeed,

2000 *Mathematics Subject Classification.* 60F05, 60F15, 60E10, 11N25, 11T55, 14G10.

Key words and phrases. Poisson distribution, Poisson convergence, distribution of values of L-functions, random permutations, Erdős-Kac Theorem, Katz-Sarnak philosophy.

[1] Although this new paper is largely self-contained, it is likely to be most useful for readers who have at least looked at the introduction and the examples in [12], especially Section 4

we noticed that this can be seen to occur in number theory in one approach to the famous Erdős-Kac Theorem.

In the present paper, we look more deeply at mod-Poisson convergence. We first recall the definition and give basic facts about mod-Poisson convergence in Sections 2 and 3. Sections 4 and 5 consider number-theoretic situations related to the Erdős-Kac Theorem. We show that the nature of the mod-Poisson convergence parallels closely the structure of conjectures for the moments of zeta functions on the critical line. This becomes especially clear over finite fields, leading to very precise analogies with the Katz-Sarnak philosophy and conjectures. In fact, in Section 6, we prove a version of the mod-Poisson convergence for the number of irreducible factors of a polynomial in $\mathbf{F}_q[X]$, as the degree increases, which is a zero-dimensional case of the large conductor limit for L-functions (see Remark 5.1 and Theorem 6.4). Our proof convincingly explains the probabilistic features of the limiting function, involving both local models of primes and large random permutations.

Notation. 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.

For any integer $d \geqslant 1$, we denote by $\mathfrak{S}_d$ the symmetric group on d letters and by $\mathfrak{S}_d^\sharp$ the set of its conjugacy classes. Recall these can be identified with partitions of d, where the partition

$$n = 1 \cdot r_1 + \cdots + d \cdot r_d, \qquad r_i \geqslant 0,$$

corresponds to permutations with r_1 fixed points, r_2 disjoint 2-cycles, ..., r_d disjoint d-cycles. For $\sigma \in \mathfrak{S}_d$, we write $\sigma^\sharp$ for its conjugacy class. We denote by $\varpi(\sigma)$ the number of disjoint cycles occurring in σ.

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.

Acknowledgments. We thank P-O. Dehaye and A.D. Barbour for interesting discussions related to this paper, and P. Bourgade for pointing out a computational mistake in an earlier draft. Thanks also to the referee for a careful reading of the manuscript.

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

2. General properties of mod-Poisson convergence

Recall that a Poisson random variable P_λ with parameter $\lambda > 0$ is one taking (almost surely) integer values $k \geqslant 0$ with

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

Its characteristic function is then given by

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

Definition 2.1. We say that a sequence of random variables (Z_N) converges in the mod-Poisson sense with parameters λ_N if the following limits

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

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

Example 2.2. (1) The simplest case of mod-Poisson convergence (which justifies partly the name) is given by

$$Z_N = P_{\lambda_N} + Z \tag{2.1}$$

where P_{λ_N} is a Poisson variable with parameter λ_N, while Z is an arbitrary random variable independent of all P_{λ_N}. In that case, the limiting function is the characteristic function $\mathbf{E}(e^{iuZ})$ of Z.

(2) Often, and in particular in the cases of interest in the arithmetic part of this paper, Z_N is (almost surely) integer-valued; in that case, its characteristic function is 2π-periodic, and it follows that if the convergence is locally uniform, then it is in fact uniform for $u \in \mathbf{R}$. However, this is not always the case, as shown by examples like (2.1) if the fixed random variable Z is not itself integer-valued.

(3) A.D. Barbour pointed out to us the paper [11] of H-K. Hwang. Hwang introduces an analytic assumption [11, (1), p. 451] on the *probability generating functions* of integer-valued random variables (X_N), i.e., on the power series

$$\sum_{n\geqslant 1} \mathbf{P}(X_N = n)z^n = \mathbf{E}(z^{X_N}),$$

which is very closely related to mod-Poisson convergence. This assumption is used as a basis to deduce results on Poisson approximation of the sequence (see Proposition 2.5 below for a simple example). Hwang also gives many additional examples where his assumption holds.

If we have mod-Poisson convergence with parameters (λ_N) which converge, then (Z_N) converges in law. Such a situation arises for instance in the so-called Poisson convergence (see, e.g.,[4, p. 188]), which we recall:

Proposition 2.3. *Let $(X_k^{(n)})$ be an array of independent random variables, identically distributed in each row, according to a Bernoulli distribution with parameter x_n:*

$$\mathbf{P}(X_i^{(n)} = 1) = x_n \text{ and } \mathbf{P}(X_i^{(n)} = 0) = 1 - x_n \quad \text{for } 1 \leqslant i \leqslant n.$$

Set $S_n = X_1^{(n)} + \ldots + X_n^{(n)}$. Then, S_n converges in distribution if and only if $nx_n \to \lambda > 0$, when $n \to \infty$. The limit random variable S is a Poisson random variable with parameter λ.

We will state an analogue of Poisson convergence in the mod-Poisson setting in the next section, but first we discuss some basic consequences. The link with mod-Gaussian convergence in the last part of the next result is quite intriguing.

Proposition 2.4. *Let (Z_N) be a sequence of random variables which converges in the mod-Poisson sense, with parameters λ_N, such that*

$$\lim_{N\to\infty} \lambda_N = \infty.$$

Then the following hold:

(1) *The re-scaled variables Z_N/λ_N converge in probability to 1, that is, for any $\varepsilon > 0$,*

$$\lim_{N\to\infty} \mathbf{P}\Big(\Big|\frac{Z_N}{\lambda_N} - 1\Big| > \varepsilon\Big) = 0.$$

(2) *We have the normal convergence*

$$\frac{Z_N - \lambda_N}{\sqrt{\lambda_N}} \overset{\text{law}}{\Rightarrow} \mathcal{N}(0,1), \tag{2.2}$$

where $\mathcal{N}$ is a standard Gaussian random variable.

(3) *The random variables*

$$Y_N = \frac{Z_N - \lambda_N}{\lambda_N^{1/3}}$$

converge in the mod-Gaussian sense (1.1) *with parameters $(0, \lambda_N^{1/3})$ and universal limiting function*

$$\Phi_u(t) = \exp(-it^3/6).$$

Proof. This is a very standard probabilistic argument, but we give details for completeness.

(1) For $u \in \mathbf{R}$, we write

$$s = \frac{u}{\lambda_N}$$

(note that s depends on N and $s \to 0$ when $N \to +\infty$). By the definition of mod-Poisson convergence (in particular the uniform convergence with respect to u), we have

$$\lim_{N\to+\infty} \exp(\lambda_N(1 - e^{is}))\, \mathbf{E}(e^{isZ_N}) = \Phi(0) = 1.$$

The fact that

$$\exp(\lambda_N(e^{is} - 1)) = \exp((is + O(s^2))\lambda_N),$$

yields

$$\lim_{N\to+\infty} \mathbf{E}(e^{iuZ_N/\lambda_N}) = e^{iu}.$$

Consequently, (Z_N/λ_N) converges in distribution to 1 and hence converges in probability since the limiting random variable is constant.

(2) For $u \in \mathbf{R}$, we now write

$$t = \frac{u}{\sqrt{\lambda_N}}$$

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

Again, by the definition of mod-Poisson convergence (in particular the uniform convergence with respect to u), we have

$$\lim_{N\to+\infty} \exp(\lambda_N(1-e^{it}))\,\mathbf{E}(e^{itZ_N}) = \Phi(0) = 1. \tag{2.3}$$

Moreover, we have

$$\begin{aligned}\exp(\lambda_N(e^{it}-1)) &= \exp((it - t^2/2 + O(t^3))\lambda_N)\\ &= \exp\Big(iu\sqrt{\lambda_N} - \frac{u^2}{2} + O\Big(\frac{u^3}{\sqrt{\lambda_N}}\Big)\Big).\end{aligned} \tag{2.4}$$

Let

$$Y_N = \frac{Z_N - \lambda_N}{\sqrt{\lambda_N}}.$$

We have then

$$\mathbf{E}(e^{iuY_N}) = \exp(-iu\sqrt{\lambda_N})\,\mathbf{E}(e^{itZ_N}). \tag{2.5}$$

Writing (2.5) as

$$\exp(-iu\sqrt{\lambda_N}) \times \exp((e^{it}-1)\lambda_N) \times \exp((1-e^{it})\lambda_N)\,\mathbf{E}(e^{itZ_N}),$$

we see from (2.3) and (2.4) that this is

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

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

Part (3) is a similar straightforward computation, which we leave as an enlightening exercise. □

In stating the renormalized convergence to a Gaussian variable, there is a loss of information, since the "Poisson nature" of the sequence is lost. This is illustrated further by the following result which goes some way towards clarifying the probabilistic nature of mod-Poisson convergence. We recall that the Kolmogorov-Smirnov distance between real-valued random variables X and Y is defined by

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

Proposition 2.5. *Let (Z_N) be a sequence of random variables which are a.s. supported on positive integers, and which converges in the mod-Poisson sense for some parameters (λ_N), such that $\lambda_N \to \infty$ when $N \to \infty$. Assume further that the characteristic functions $\mathbf{E}(e^{iuZ_N})$ are of C^1 class and the convergence holds in C^1 topology.*

Then we have

$$\lim_{N\to+\infty} d_{KS}(Z_N, P_{\lambda_N}) = 0,$$

where P_{λ_N} is a Poisson random variable with parameter λ_N, and in fact

$$d_{KS}(Z_N, P_{\lambda_N}) \leqslant \|\Phi'\|_\infty \lambda_N^{-1/2},$$

for $N \geqslant 1$.

Proof. We recall the following well-known inequality, which is the ad-hoc tool (see, e.g. [15, p. 186, 5.10.2]): if X and Y are integer-valued random variables, then

$$d_{KS}(X, Y) \leqslant \frac{1}{4} \int_{-\pi}^{\pi} \left| \frac{\mathbf{E}(e^{iuX}) - \mathbf{E}(e^{iuY})}{u} \right| du.$$

Let

$$\psi_N(u) = \mathbf{E}(e^{iuP_{\lambda_N}}), \quad \Phi_N(u) = \psi_N(u)^{-1}\, \mathbf{E}(e^{iuZ_N}).$$

From the inequality, we obtain

$$\begin{aligned} d_{KS}(Z_N, P_{\lambda_N}) &\leqslant \frac{1}{4} \int_{-\pi}^{\pi} |\, \mathbf{E}(e^{iuZ_N}) - \psi_N(u)| \frac{du}{u} \\ &= \frac{1}{4} \int_{-\pi}^{\pi} \Big| \psi_N(u) \frac{\Phi_N(u) - 1}{u} \Big| du \end{aligned}$$

From our stronger assumption of mod-Poisson convergence with C^1 convergence, we have a uniform bound

$$\left| \frac{\Phi_N(u) - 1}{u} \right| \leqslant \|\Phi_N'\|_\infty,$$

for $N \geqslant 1$, hence since $|\Psi_N(u)| = \exp(\lambda_N(\cos u - 1))$, we have

$$d_{KS}(Z_N, P_{\lambda_N}) \leqslant \frac{\|\Phi'\|_\infty}{4} \int_{-\pi}^{\pi} e^{\lambda_N(\cos u - 1)} du.$$

It is well-known that the precise asymptotic of such an integral gives order of magnitude $\lambda_N^{-1/2}$ for $\lambda_N \to +\infty$. To see this quickly, note for instance that $\cos u - 1 \leqslant -u^2/5$ on $[-\pi, \pi]$, hence

$$\int_0^{\pi} e^{\lambda_N(\cos u - 1)} du \leqslant \int_{\pi}^{\pi} e^{-\lambda_N u^2/5} du \leqslant \int_{\mathbf{R}} e^{-\lambda_N u^2/5} du = \sqrt{\frac{5\pi}{\lambda_N}},$$

which gives the result since $\sqrt{5\pi}/4 \leqslant 1$. □

Remark 2.6. (1) Hwang [11, Th. 1] gives this and many other variants for other measures of approximation, under the assumption of his version of mod-Poisson convergence. In another work with A. Barbour, we consider various refinements and applications of this type of statement, including with approximation involving more general families of discrete random variables (see [3]).

(2) As a reference for number theorists, note that the existence of renormalized convergence as in (2.2) for an arbitrary sequence of integer-valued

random variables (Z_N), with $\mathbf{E}(Z_N) = \lambda_N$, does not imply that the Kolmogorov distance $d_{KS}(Z_N, P_{\lambda_N})$ converge to 0: indeed, consider

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

where the B_i are Bernoulli random variables with $\mathbf{P}(B_i = 1) = \mathbf{P}(B_i = 0) = \frac{1}{2}$. Then $\lambda_N = \frac{N}{2}$, and the normalized convergence in law (2.2) is the Central Limit Theorem. However, it is known that, for some constant $c > 0$, we have

$$d_{KS}(Z_N, P_{\lambda_N}) \geqslant c > 0$$

for all N (see, e.g., [2, Th. 2], for the analogue in total variation distance, which in that case is comparable to the Kolmogorov distance [18, Prop. 1]).

3. Limit theorems with mod-Poisson behavior

Now we give an analogue of the Poisson convergence in the mod-Poisson framework.

Proposition 3.1. *Let (x_n) of positive real numbers with*

$$\sum_{n\geqslant 1} x_n = +\infty, \qquad \sum_{n\geqslant 1} x_n^2 < +\infty, \tag{3.1}$$

and let (B_n) be a sequence of independent Bernoulli random variables with

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

Then

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

has mod-Poisson convergence with parameters

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

and with limiting function given by

$$\Phi(u) = \prod_{n\geqslant 1} (1 + x_n(e^{iu} - 1)) \exp(x_n(1 - e^{iu})),$$

a uniformly convergent infinite product.

Proof. This is again a quite simple computation. Indeed, by independence of the variables B_n, we have

$$\exp(\lambda_N(1 - e^{iu}))\, \mathbf{E}(e^{iuZ_N}) = \prod_{n=1}^{N} \exp(x_n(1 - e^{iu}))(1 + x_n(e^{iu} - 1)),$$

and since

$$\exp(x_n(1 - e^{iu}))(1 + x_n(e^{iu} - 1)) = 1 + O(x_n^2)$$

for $u \in \mathbf{R}$ and $n \geqslant 1$ (recall $x_n \to 0$), it follows from (3.1) that this product converges locally uniformly to $\Phi(u)$, which completes the proof. □

Remark 3.2. More generally, assume that $(X_k^{(n)})$ is a triangular array of independent random variables taking values in $\{0, a_1, \dots, a_r\}$, such that

$$\mathbf{P}[X_k^{(n)} = a_i] = x_n^{(i)}; \quad i = 1, \dots, r.$$

Assume that for any i, $\sum_{n\geqslant 1} x_n^{(i)} = \infty$ and $\sum_{n\geqslant 1}(x_n^{(i)})^2 < \infty$. Then $S_n = X_1^{(n)} + \dots + X_n^{(n)}$ converges in the mod-Poisson sense with parameter $\lambda_N = a_1 x_n^{(1)} + \dots + a_r x_n^{(r)}$.

4. Mod-Poisson convergence and the Erdős-Kac Theorem: a first analogy

In [12, §4.3], we gave the first example of mod-Poisson convergence as explaining (through the Central Limit of Proposition 2.4) the classical result of Erdős and Kac concerning the statistic behavior of the arithmetic function function $\omega(n)$, the number of (distinct) prime divisors of a positive integer $n \geqslant 1$:

$$\lim_{N\to+\infty} \frac{1}{N}|\{n \leqslant N \mid a < \frac{\omega(n) - \log\log N}{\sqrt{\log\log N}} < b\}| = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} dt \quad (4.1)$$

for any real numbers $a < b$.

More precisely, with

$$\omega'(n) = \omega(n) - 1, \qquad \text{for } n \geqslant 2,$$

we showed by a simple application of the Delange-Selberg method (see, e.g., [20, II.5, Theorem 3]) that for any $u \in \mathbf{R}$, we have

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

and the convergence is uniform, with

$$\Phi(u) = \frac{1}{\Gamma(e^{iu}+1)} \prod_p \Big(1 - \frac{1}{p}\Big)^{e^{iu}} \Big(1 + \frac{e^{iu}}{p-1}\Big), \quad (4.2)$$

where the Euler product is absolutely and uniformly convergent: this means mod-Poisson convergence with parameters $\lambda_N = \log\log N$. By Proposition 2.4, (2), this implies (4.1).[2] To illustrate what extra information is contained in mod-Poisson convergence we make two remarks: first, by putting $u = \pi$, for instance, we get

$$\sum_{1\leqslant n\leqslant N} (-1)^{\omega(n)} = o\Big(\frac{N}{(\log N)^2}\Big),$$

as $N \to +\infty$ (since $1/\Gamma(1+e^{i\pi}) = 0$), which is a statement well-known to be equivalent to the Prime Number Theorem. Secondly, more generally, we can apply results like Proposition 2.5 (which is easily checked to be applicable

[2] As we observed, this gives essentially the proof of the Erdős–Kac theorem due to Rényi and Turán [16]. For another recent simple proof, see [9].

here) to derive Poisson-approximation results for $\omega(n)$ which are much more precise than the renormalized Gaussian behavior (see also [11, §4] and [20, §6.1] for the discussion of the classical work of Sathé and Selberg).

We wish here to bring to light the very interesting, and very complete, analogy between the probabilistic structure of this mod-Poisson version of the Erdős-Kac Theorem and the mod-Gaussian conjecture for the distribution of the values L-functions, taking as basic example the conjecture for the distribution of $\log|\zeta(1/2+it)|$, which follows from the Keating-Snaith moment conjectures for the Riemann zeta function (see [12], [14]).

We start with the observation, following from (4.2), that the limiting function $\Phi(u)$ in the Erdős-Kac Theorem takes the form of a product $\Phi(u) = \Phi_1(u)\Phi_2(u)$ with

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

We compare this with the Moment Conjecture in the mod-Gaussian form, namely, if U is uniformly distributed on $[0,T]$, it is expected that

$$\lim_{T\to+\infty} e^{u^2\log\log T}\,\mathbf{E}(e^{iu\log|\zeta(1/2+iU)|^2}) = \Psi_1(u)\Psi_2(u), \tag{4.3}$$

for all $u\in\mathbf{R}$ (locally uniformly) where

$$\Psi_1(u) = \frac{G(1+iu)^2}{G(1+2iu)}, \tag{4.4}$$

($G(z)$ is the Barnes double-gamma function, see e.g. [21, Ch. XII, Misc. Ex. 48]), and

$$\Psi_2(u) = \prod_p \Big(1-\frac{1}{p}\Big)^{-u^2}\Big\{\sum_{m\geqslant 0}\Big(\frac{\Gamma(m+iu)}{m!\Gamma(\lambda)}\Big)^2 p^{-m}\Big\}. \tag{4.5}$$

Here also, the limiting function splits as a product of two terms, and each appears individually as limit in a distinct mod-Gaussian convergence. Indeed, we first have

$$\Psi_1(u) = \lim_{N\to+\infty} e^{u^2(\log N)}\,\mathbf{E}(e^{iu\log|\det(1-X_N)|^2}),$$

where X_N is a Haar-distributed $U(N)$-valued random variable. Secondly (see [12, 4.1]), we have

$$\Psi_2(u) = \lim_{N\to+\infty} e^{u^2(\log(e^\gamma\log N))}\,\mathbf{E}(e^{iuL_N})$$

where

$$L_N = \sum_{p\leqslant N}\log\Big|1-\frac{e^{i\theta_p}}{\sqrt{p}}\Big|^2,$$

for any sequence $(\theta_p)_{p\leqslant N}$ of independent random variables, uniformly distributed on $[0,1]$.

Remark 4.1. Note in passing that for fixed p, the p-th component of the Euler product of $\zeta(1/2+iU)$, for U uniformly distributed on $[0,T]$, converges in law to $(1-e^{i\theta_p}p^{-1/2})^{-1}$ as $T\to+\infty$.

We now prove that the Euler product Φ_2 (like Ψ_2) corresponds to mod-Poisson convergence for a natural asymptotic probabilistic model of primes, and that Φ_1 (like Ψ_1) comes from a model of group-theoretic origin.[3]

We start with the Euler product, where the computation was already described in [12, §4.3]: we have

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

and by isolating the first term, it follows that

$$\begin{aligned}\Phi_2(u)&=\lim_{y\to+\infty}\exp((1-e^{iu})\lambda_y)\prod_{p\leqslant y}\Big(1-\frac{1}{p}+\frac{1}{p}e^{iu}\Big)\\&=\lim_{y\to+\infty}\mathbf{E}(e^{iuP_{\lambda_y}})^{-1}\,\mathbf{E}(e^{iuZ'_y})\end{aligned}$$

where

$$\lambda_y=\sum_{p\leqslant y}\log\Big(\frac{1}{1-p^{-1}}\Big)=\sum_{\substack{p\leqslant y\\k\geqslant 1}}\frac{1}{kp^k}=\log\log y+\kappa+o(1),$$

as $y\to+\infty$, for some real constant κ (see, e.g., [10, §22.8]), and

$$Z'_y=\sum_{p\leqslant y}B'_p \tag{4.6}$$

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

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

We note that this is a particular case of Proposition 3.1, and that (as expected) the parameters of these Bernoulli laws correspond exactly to the "intuitive" probability that an integer n be divisible by p, or equivalently, the Bernoulli variable B'_p is the limit in law as $N\to+\infty$ of the random variables defined as the indicator of a uniformly chosen integer $n\leqslant N$ being divisible by p; the independence of the B'_p corresponds for instance to the formal (algebraic) independence of the divisibility by distinct primes given, e.g., by the Chinese Remainder Theorem.

As in the case of the Riemann zeta function, we also note that the independent model fails to capture the truth on the distribution of $\omega(n)$, the

[3] Since a product of two limiting functions for mod-Poisson convergence is clearly another such limiting function, we also recover without arithmetic the fact that the limiting function $\Phi(u)$ arises from mod-Poisson convergence.

extent of this failure being measured, in some sense, by the factor $\Phi_1(u)$. Because

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

this discrepancy between the independent model and the arithmetic truth is invisible at the level of the normalized convergence in distribution (as it is for $\log|\zeta(1/2+it)|$, by Selberg's Central Limit Theorem, hiding the Random Matrix Model).

Now we consider the first factor $\Phi_1(u) = \Gamma(e^{iu}+1)^{-1}$. Again, in [12, §4.3], we appealed to the formula

$$\frac{1}{\Gamma(e^{iu}+1)} = \prod_{k\geqslant 1}\Big(1+\frac{e^{iu}}{k}\Big)\Big(1+\frac{1}{k}\Big)^{-e^{iu}}$$

for $u \in \mathbf{R}$ (see [21, 12.11]) to compute

$$\begin{aligned}\Phi_1(u) &= \lim_{N\to+\infty}\prod_{k\leqslant N}\Big(1+\frac{1}{k}\Big)^{1-e^{iu}}\Big(1+\frac{1}{k}\Big)^{-1}\Big(1+\frac{e^{iu}}{k}\Big)\\ &= \lim_{N\to+\infty}\exp(\lambda_N(1-e^{iu}))\prod_{k\leqslant N}\Big(1+\frac{1}{k}\Big)^{-1}\Big(1+\frac{e^{iu}}{k}\Big)\\ &= \lim_{N\to+\infty}\exp(\lambda_N(1-e^{iu}))\,\mathbf{E}(e^{iuZ_N}),\end{aligned}$$

where

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

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

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

The group-theoretic interpretation of this distribution is very suggestive: indeed, it is the distribution of the random variable $\varpi(\sigma_{N+1})-1$, where $\sigma_{N+1}\in\mathfrak{S}_{N+1}$ is distributed according to the uniform measure on the symmetric group, and we recall that $\varpi(\sigma)$ is the number of cycles of a permutation. In other words, we have

$$\mathbf{E}(e^{iu\varpi(\sigma_N)}) = \prod_{1\leqslant j\leqslant N}\Big(1-\frac{1}{j}+\frac{e^{iu}}{j}\Big), \tag{4.7}$$

as proved, e.g., in [1, §4.6]; note that this is not obvious, and the decomposition as a sum of independent random variables is due to Feller, and is explained in [1, p. 16].

So we see – and this gives another example of natural mod-Poisson convergence – that these random variables have mod-Poisson convergence with parameters $\log N$, and limiting function $1/\Gamma(e^{iu})$:

$$\lim_{N\to+\infty} \exp((\log N)(1-e^{iu}))\,\mathbf{E}(e^{iu\varpi(\sigma_N)}) = \frac{1}{\Gamma(e^{iu})}. \tag{4.8}$$

For further reference, we state a more precise version, which follows from (4.7):

$$\mathbf{E}(e^{iu\varpi(\sigma_N)}) = \frac{1}{\Gamma(e^{iu})}\exp((\log N)(e^{iu}-1))\Big(1+O\Big(\frac{1}{N}\Big)\Big), \tag{4.9}$$

locally uniformly for $u \in \mathbf{R}$. Note that this includes the special case $u = (2k+1)\pi$ where

$$\mathbf{E}(e^{iu\varpi(\sigma_N)}) = \frac{1}{\Gamma(e^{iu})} = 0.$$

This explanation of the "transcendental" factor $1/\Gamma(e^{iu}+1)$ is particularly convincing because of well-known and well-studied analogies between the cycle structure of random permutations and the factorization of integers (see, e.g., the discussion in [1, §1.2] or the entertaining survey [8]). Its origin in [12, 4.3] is, however, not very enlightening: the Gamma function appears universally in the Delange-Selberg method in a way which may seem to be coincidental and unrelated to any group-theoretic structure (see, e.g., [20, §5.2] where it originates in a representation of $1/\Gamma(z)$ as a contour integral of Hankel type).

5. The analogy deepens

The discussion of the previous section is already interesting, but it becomes (to our mind) even more intriguing after one notes how the analogy can be extended by including consideration of function field situations, as in the work of Katz-Sarnak [13].

Let $\mathbf{F}_q$ be a finite field with $q = p^n$ elements, with $n \geqslant 1$ and p prime. For a polynomial $f \in \mathbf{F}_q[X]$, let

$$\omega(f) = \omega_q(f) = |\{\pi \in \mathbf{F}_q[X] \mid \pi \text{ is irreducible monic and divides } f\}|$$

be the analogue of the number of prime factors of an integer (we will usually drop the subscript q).

We consider the statistic behavior of this function under two types of limits: (i) either q is replaced by q^m, $m \to +\infty$, and f is assumed to range over monic polynomials of fixed degree $d \geqslant 1$ in $\mathbf{F}_{q^m}[X]$; or (ii) q is fixed, and f is assumed to range over monic polynomials of degree $d \to +\infty$ in $\mathbf{F}_q[X]$.

The first limit, of fixed degree and increasing base field, is similar to the one considered by Katz and Sarnak for the distribution of zeros of families of L-functions over finite fields [13]. And the parallel is quite precise as far as the group-theoretic situation goes. Indeed, recall that the crucial ingredient in their work is that the Frobenius automorphism provides in a natural way

a "random matrix" for a given L-function, the characteristic polynomial of which provides a spectral interpretation of the zeros (see, e.g., [12, §4.2] for a partial, down-to-earth, summary).

In our case, let us assume first that $f \in \mathbf{F}_q[X]$ is squarefree. Let K_f denote the splitting field of f, i.e., the extension field of $\mathbf{F}_q$ generated by the d roots of f, and let F_f denote the Frobenius automorphism $x \mapsto x^q$ of K_f. This automorphism permutes the roots of f, which all lie in K_f, and after enumerating them, leads to an element of $\mathfrak{S}_d$, denoted F_f. This depends on the enumeration of the roots, but the conjugacy class $F_f^\sharp \in \mathfrak{S}_d^\sharp$ is well-defined.

Now, by the very definition, we have

$$\omega(f) = \varpi(F_f^\sharp), \tag{5.1}$$

which can be seen as the (very simple) analogue of the spectral interpretation of an L-function as the characteristic polynomial of the Frobenius endomorphism.

Remark 5.1. We can come even closer to the Katz-Sarnak setting of families of L-functions. Consider, in scheme-theoretic language,[4] the (very simple!) family of zeta functions of the zero-dimensional schemes $X_f = \mathrm{Spec}(\mathbf{F}_q[X]/(f))$, i.e., the varieties over $\mathbf{F}_q$ with equation $f(x) = 0$. These zeta functions are defined by either of the following two formulas:

$$Z(X_f) = \prod_{x \in |X_f|} (1 - T^{\deg(x)})^{-1} = \exp\Big(\sum_{m \geqslant 1} \frac{|X_f(\mathbf{F}_{q^m})| T^m}{m}\Big),$$

where $|X_f|$ is the set of closed points of X_f. Since these correspond naturally to irreducible factors of f (without multiplicity), it follows that

$$Z(X_f) = \prod_{\pi | f} (1 - T^{\deg(\pi)})^{-1},$$

and hence, if f is squarefree, a higher-level version of (5.1) is the "spectral interpretation"

$$Z(X_f) = \det(1 - F_f T | H_c^0(\bar{X}_f, \mathbf{Q}_\ell))^{-1} = \det(1 - \rho(F_f)T)^{-1} \tag{5.2}$$

where F_f is still the Frobenius automorphism, $H_c^0(\bar{X}_f, \mathbf{Q}_\ell)$ is simply isomorphic with $\mathbf{Q}_\ell^{\deg(f)}$ (the variety over the algebraic closure has $\deg(f)$ connected components, which are points), and ρ is the natural faithful representation of $\mathfrak{S}_{\deg(f)}$ in $U(\deg(f), \mathbf{C})$ by permutation matrices, since this is quite clearly how F_f acts on the étale cohomology space.

Looking at the order of the pole of $Z(X_f)$ at $T = 1$, we recover (5.1). In particular, the generalizations of the Erdős-Kac Theorem that we will prove in the next section can be interpreted as describing the limiting statistical behavior, in mod-Poisson sense, of the order of the pole of those zeta

[4] Readers unfamiliar with this language can skip this remark, which will not be used, except to state Theorem 6.4 below.

functions as the degree $\deg(f)$ tends to infinity (see Theorem 6.4). It is truly a zero-dimensional version of the Katz-Sarnak problematic for growing conductor. (Note that this interpretation also suggests to look at other distribution statistics of these zeta functions, and we hope to come back to this).

The relation (5.1) (or (5.2)) explains the existence of a link between the number of irreducible factors of polynomials and the number of cycles of permutations. Indeed, the other essential number-theoretic ingredient for Katz and Sarnak is Deligne's Equidistribution Theorem, which shows that the matrices given by the Frobenius, *in the limit under consideration* where q is replaced by q^m, $m \to +\infty$, become equidistributed in a certain monodromy group. Here we have, exactly similarly, the following well-known:

Fact. In the limit of fixed d and $m \to +\infty$, for f uniformly chosen among monic squarefree polynomials of degree d in $\mathbf{F}_{q^m}[X]$, the conjugacy classes $F_f^\sharp$ become uniformly distributed in $\mathfrak{S}_d^\sharp$ for the natural (Haar) measure.

This fact is easily proved from the well-known Gauss-Dedekind formula

$$\Pi_q(d) = \sum_{\deg(\pi)=d} 1 = \frac{1}{d}\sum_{\delta|d} \mu(\delta) q^{d/\delta} = \frac{q^d}{d} + O(q^{d/2})$$

for the number of irreducible monic polynomials of degree d with coefficients in $\mathbf{F}_q$, and it is a "baby" analogue of Deligne's Equidistribution Theorem.[5] Hence, we obtain

$$\omega(f) \overset{\text{law}}{\Rightarrow} \varpi(\sigma_d),$$

as $m \to +\infty$, where f is distributed uniformly among monic polynomials of degree d in $\mathbf{F}_{q^m}[X]$, and σ_d is distributed uniformly among $\mathfrak{S}_d$.

The second limit, where the base field $\mathbf{F}_q$ is fixed and the degree d grows, is analogue of the problematic situation of families of curves of increasing genus over a fixed finite field (see the discussion in [13, p. 12]), and – for our purposes – of the distribution of the number of prime divisors of integers, which we discussed in the previous section. In the next section, we prove a mod-Poisson form of the Erdős-Kac theorem in $\mathbf{F}_q[X]$ (the Central Limit version being a standard result, essentially due to M. Car, and apparently stated first by Flajolet and Soria [6, §3, Cor. 1]; see also the recent quick derivation by R. Rhoades [17]).

Remark 5.2. One may extend the conjugacy class $F_f^\sharp \in \mathfrak{S}_d^\sharp$ to all $f \in \mathbf{F}_q[X]$ of degree d, in the following directly combinatorial way (which hides the Frobenius aspect): $F_f^\sharp$ is the conjugacy class of permutations with as many disjoint j-cycles, $1 \leqslant j \leqslant d$, as there are irreducible factors of f of degree j. However, the relation $\omega(f) = \varpi(F_f^\sharp)$ does *not* extend to this case, since

[5] Indeed, it could be proved using the Chebotarev density theorem, which is a special case of Deligne's theorem.

multiple factors are not counted by ω. However, we have $\Omega(f) = \varpi(F_f^\sharp)$, where $\Omega(f)$ is the number of irreducible factors counted with multiplicity.

6. Mod-Poisson convergence for the number of irreducible factors of a polynomial

In this section, we state and prove the mod-Poisson form of the analogue of the Erdős-Kac Theorem for polynomials over finite fields, trying to bring to the fore the probabilistic structure suggested in the previous section.

Theorem 6.1. *Let $q \neq 1$ be a power of a prime p, and let $\omega(f)$ denote as before the number of monic irreducible polynomials dividing $f \in \mathbf{F}_q[X]$. Write $|g| = q^{\deg(g)} = |\mathbf{F}_q[X]/(g)|$ for any non-zero $g \in \mathbf{F}_q[X]$.*

For any $u \in \mathbf{R}$, we have

$$\lim_{d\to+\infty} \frac{\exp((1-e^{iu})\log d)}{q^d} \sum_{\deg(f)=d} e^{iu(\omega(f)-1)} = \tilde{\Phi}_1(u)\tilde{\Phi}_2(u), \tag{6.1}$$

where

$$\tilde{\Phi}_1(u) = \frac{1}{\Gamma(e^{iu}+1)} \tag{6.2}$$

and

$$\tilde{\Phi}_2(u) = \prod_{\pi} \Big(1-\frac{1}{|\pi|}\Big)^{e^{iu}} \Big(1+\frac{e^{iu}}{|\pi|-1}\Big), \tag{6.3}$$

the product running over all monic irreducible polynomials $\pi \in \mathbf{F}_q[X]$ and the sum over all monic polynomials $f \in \mathbf{F}_q[X]$ with degree $\deg(f) = d$. Moreover, the convergence is uniform.

Remark 6.2. Note the similarity of the shape of the limiting function with that in (4.2) and the conjecture for $\zeta(1/2+it)$, in particular the fact that the group-theoretic term is the same as for $\omega(n)$, while the Euler product is a direct transcription in $\mathbf{F}_q[X]$ of the earlier Φ_2.

Remark 6.3. This can be rephrased, according to Remark 5.1, in the following manner which illustrates the analogy with the Katz-Sarnak philosophy:

Theorem 6.4. *Let $q \neq 1$ be a power of a prime. For any $f \in \mathbf{F}_q[X]$, monic of degree $\geqslant 1$, let X_f be the zero-dimensional scheme $\mathrm{Spec}(\mathbf{F}_q[X]/(f))$, let $Z(X_f) \in \mathbf{Q}(T)$ denote its zeta function and let $r(X_f) \geqslant 0$ denote the order of the pole of $Z(X_f)$ at $T = 1$. Then for any $u \in \mathbf{R}$, we have*

$$\lim_{d\to+\infty} \frac{\exp((1-e^{iu})\log d)}{q^d} \sum_{\deg(f)=d} e^{iur(f)} = e^{-iu}\tilde{\Phi}_1(-u)\tilde{\Phi}_2(-u),$$

with notation as before.

The only thing to note here is that if f is not squarefree, the scheme X_f is not reduced; the induced reduced scheme is $X_{f^\flat}$, where $f^\flat$ is the

(squarefree) product of the distinct monic irreducible factors dividing f. Then $Z(X_f) = Z(X_{f^\flat})$, and we have

$$-r(f) = \mathrm{ord}_{T=1} Z(X_f) = \mathrm{ord}_{T=1} Z(X_{f^\flat}) = -r(f^\flat) = \omega(f^\flat) = \omega(f),$$

so the two theorems are indeed equivalent.

Remark 6.5. One can also prove by the same method the following two variants, where we restrict attention to squarefree polynomials, or we consider irreducible factors with multiplicity. First, we have

$$\frac{e^{(1-e^{iu})\log d}}{q^d} \sum_{\deg(f)=d}^{\flat} e^{iu(\omega(f)-1)} \to \frac{1}{\Gamma(1+e^{iu})} \prod_{\pi} \Big(1-\frac{1}{|\pi|}\Big)^{e^{iu}} \Big(1+\frac{e^{iu}}{|\pi|}\Big),$$

where the sum $\sum^{\flat}$ runs over all squarefree monic polynomials $f \in \mathbf{F}_q[X]$ with degree $\deg(f) = d$. Next, we have

$$\frac{e^{(1-e^{iu})\log d}}{q^d} \sum_{\deg(f)=d}^{\flat} e^{iu(\Omega(f)-1)} \to \frac{1}{\Gamma(1+e^{iu})} \prod_{\pi} \frac{(1-|\pi|^{-1})^{e^{iu}}}{1-e^{iu}/|\pi|}.$$

We now come to the proof. The idea we want to highlight – the source of the splitting of the limiting function in two parts of distinct probabilistic origin – is to first separate the irreducible factors of "small" degree and those of "large" degree (which is fairly classical), and then observe that an equidistribution theorem allows us to perform a transfer of the contribution of large factors to the corresponding average over random permutations, conditioned to not have small cycle lengths. This will explain the factor $\tilde{\Phi}_1$ corresponding to the cycle length of random permutations. Note that shorter arguments are definitely available, using analogues of the Delange-Selberg method used in [12] (see [6, §2, Th. 1]), but this hides again the mixture of probabilistic models involved.

Interestingly, the small and larger irreducible factors are *not* exactly independent. But the dependency is (essentially) perfectly compensated by the effect of the conditioning at the level of random permutations. Why this is so may be the last little mystery in the computation, which is otherwise very enlightening.

We set up some notation first: for $f \in \mathbf{F}_q[X]$, we let $d^+(f)$ (resp. $d^-(f)$) denote the largest (resp., smallest) degree of an irreducible factor $\pi \mid f$; correspondingly, for a permutation $\sigma \in \mathfrak{S}_d$, we denote by $\ell^+(\sigma)$ (resp. $\ell^-(\sigma)$) the largest (resp. smallest) length of a cycle occurring in the decomposition of σ.

Henceforth, by convention, any sum involving polynomials f, g, h, etc, is assumed to restrict to monic polynomials, and any sum or product involving π is restricted to monic irreducible polynomials.

The next lemma summarizes some simple properties, and the important equidistribution property we need.

Lemma 6.6. *With notation as above, we have:*

(1) *For all $d \geqslant 1$, we have*

$$\frac{1}{q^d} \sum_{\deg(\pi)=d} 1 = \frac{1}{d} + O(q^{-d/2}).$$

(2) *For all $d \geqslant 1$, we have*

$$\prod_{\deg(\pi)\leqslant d} \Big(1 + \frac{1}{|\pi|-1}\Big) \ll d, \tag{6.4}$$

$$\prod_{\deg(\pi)\leqslant d} \Big(1 - \frac{1}{|\pi|}\Big) = \exp\Big(-\sum_{1\leqslant j\leqslant d} \frac{1}{j}\Big)\Big(1 + O\Big(\frac{1}{d}\Big)\Big). \tag{6.5}$$

(3) *For any $d \geqslant 1$ and any fixed permutation $\sigma \in \mathfrak{S}_d$, we have*

$$\frac{1}{q^d} \sum_{\substack{\deg(f)=d \\ F_f^\sharp = \sigma^\sharp}}^{\flat} 1 = \mathbf{P}(\sigma_d = \sigma)\Big(1 + O\Big(\frac{d}{q^{\ell^-(\sigma)/2}}\Big)\Big), \tag{6.6}$$

where the conjugacy class $F_f^\sharp \in \mathfrak{S}_d^\sharp$ is defined in the previous section, σ_d is a uniformly chosen random permutation in $\mathfrak{S}_d$ and $\sum^\flat$ restricts the sum to squarefree polynomials.

In all estimates, the last under the assumption $q^{\ell^-(\sigma)/2} \geqslant d$, the implied constants are absolute, except that in (6.4)*, the implied constant may depend on q.*

Proof. The first statement has already been recalled. For (6.4), we have

$$\begin{aligned}\prod_{\deg(\pi)\leqslant d} \Big(1 + \frac{1}{|\pi|-1}\Big) &\leqslant \exp\Big(\sum_{1\leqslant j\leqslant d} \frac{\Pi_q(j)}{q^j-1}\Big) \\ &= \exp\Big(\sum_{2\leqslant j\leqslant d} \frac{1}{j} + O\Big(\sum_{1\leqslant j\leqslant d} \frac{q^{j/2}}{q^j-1}\Big)\Big) \ll d,\end{aligned}$$

for $d \geqslant 1$, with an implied constant depending on q.

For (6.5), which is the analogue for $\mathbf{F}_q[T]$ of the classical Mertens estimate, we refer, e.g., to [19], where it is proved in the form

$$\prod_{\deg(\pi)\leqslant d} \Big(1 - \frac{1}{|\pi|}\Big) = \frac{e^{-\gamma}}{d}\Big(1 + O\Big(\frac{1}{d}\Big)\Big)$$

for $d \geqslant 1$, γ being the Euler constant; since

$$\sum_{1\leqslant j\leqslant d} \frac{1}{j} = \log d + \gamma + O\Big(\frac{1}{d}\Big),$$

we get the stated result. We emphasize the fact that the asymptotic of the product in (6.5) is independent of q (and is the same as for the usual Mertens formula for prime numbers), since this may seem surprising at first sight.

This is explained by the relation with random permutations, and in fact, in Remark 6.10 below, we explain how our argument leads to a much sharper estimate (6.20) for the error term in (6.5).

Finally, for the third statement, if σ is a product of r_j disjoint j-cycles for $1 \leqslant j \leqslant d$, we first recall the standard formula that

$$\mathbf{P}(\sigma_d = \sigma) = \prod_{1\leqslant j\leqslant d} \frac{1}{j^{r_j} r_j!}, \tag{6.7}$$

and we observe that the product can be made to range over $\ell^-(\sigma) \leqslant j \leqslant d$, since the terms $j < \ell^-(\sigma)$ have $r_j = 0$ by definition. Using this observation, we have by simple counting

$$\sum_{\substack{\deg(f)=d\\ F_f^\sharp=\sigma^\sharp}}{}^{\flat} 1 = \prod_{\ell^-(\sigma)\leqslant j\leqslant d} \binom{\Pi_q(j)}{r_j}.$$

Furthermore, for any r and $j \geqslant 1$ such that $r < q^{j/2}$ and $j \leqslant r$, we have

$$\begin{aligned}\binom{\Pi_q(j)}{r} &= \frac{1}{r!}\Pi_q(j)(\Pi_q(j)-1)\cdots(\Pi_q(j)-r+1)\\ &= \frac{1}{r!}\Big(\frac{q^j}{j}+O(q^{-j/2})\Big)^r = \frac{q^{jr}}{j^r r!}(1+O(rq^{-j/2}))^r,\end{aligned}$$

by the first part of the lemma. Combining the two formulas, we get

$$\begin{aligned}\frac{1}{q^d}\sum_{\substack{\deg(f)=d\\ F_f^\sharp=\sigma^\sharp}}{}^{\flat} 1 &= q^{-d}\prod_{\ell^-(\sigma)\leqslant j\leqslant d}\frac{q^{jr_j}}{j^{r_j}r_j!}(1+O(dq^{-j/2}))^{r_j}\\ &= \prod_{\ell^-(\sigma)\leqslant j\leqslant d}\frac{1}{r_j!j^{r_j}}\Big(1+O(dq^{-j/2})\Big)^{r_j}\\ &= \mathbf{P}(\sigma_d=\sigma)\prod_{\ell^-(\sigma)\leqslant j\leqslant d}\Big(1+O(dq^{-j/2})\Big)^{r_j}\end{aligned}$$

and this immediately gives the conclusion since the implied constant in the formula for $\Pi_q(j)$ is at most 1. □

Part (3) of this lemma means that, as long as we consider permutations $\sigma \in \mathfrak{S}_d$ with no short cycle, so that

$$d = o(q^{\ell^-(\sigma)/2}),$$

there is strong quantitative equidistribution of the conjugacy class $F_f^\sharp$ among all conjugacy classes in $\mathfrak{S}_d$.

Thus, to compare the distribution of polynomials and that of permutations, it is natural to introduce a parameter b, $0 \leqslant b \leqslant d$, to be specified

later, and to first write any monic polynomial f of degree d as $f = gh$, where the monic polynomials g and h are uniquely determined by

$$d^+(g) \leqslant b, \qquad d^-(h) > b \tag{6.8}$$

(i.e., g contains the small factors, and h the large ones; they correspond to "friable" and "sifted" integers in classical analytic number theory). One can expect, by the above, that if b is such that $q^{b/2}$ is large enough compared with d, the distribution of h will reflect that of permutations without cycles of length $\leqslant b$. And the contribution of small factors should (and will) be comparable with the independent model for divisibility of polynomials by irreducible ones.

We now start the proof of Theorem 6.1 along these lines, trying to evaluate

$$\frac{1}{q^d} \sum_{\deg(f)=d} e^{iu\omega(f)}$$

Writing $f = gh$, where g and h satisfy (6.8) as above, we have $\omega(f) = \omega(g) + \omega(h)$ since g and h are coprime, and hence

$$\frac{1}{q^d} \sum_{\deg(f)=d} e^{iu\omega(f)} = \sum_{\substack{\deg(g)\leqslant d \\ d^+(g)\leqslant b}} \frac{e^{iu\omega(g)}}{|g|} T(d-\deg(g), b),$$

where we define

$$T(d,b) = \frac{1}{q^d} \sum_{\substack{\deg(f)=d \\ d^-(f)>b}} e^{iu\omega(f)}.$$

Denote further

$$R(d,b) = \sum_{\substack{\deg(g)>d \\ d^+(g)\leqslant b}} \frac{1}{|g|}, \qquad S(d,b) = \sum_{\substack{\deg(g)\leqslant d \\ d^+(g)\leqslant b}}{}^{\flat} \frac{1}{|g|}.$$

Noting that $|T(d,b)| \leqslant 1$ for all b and d, and splitting the sum over g according as to whether $\deg(g) \leqslant \sqrt{d}$ or $\deg(g) > \sqrt{d}$, we get

$$\begin{aligned} \frac{1}{q^d} \sum_{\deg(f)=d} e^{iu\omega(f)} &= \sum_{\substack{\deg(g)\leqslant \sqrt{d} \\ d^+(g)\leqslant b}} \frac{e^{iu\omega(g)}}{|g|} T(d-\deg(g), b) + O(R(\sqrt{d}, b)) \\ &= S_1 + O(R(\sqrt{d}, b)), \text{ say.} \end{aligned} \tag{6.9}$$

The next step, which is were random permutations will come into play, will be to evaluate $T(d,b)$ asymptotically in suitable ranges.

Proposition 6.7. *With notation as before, we have*

$$T(d,b) = \exp\Big(-e^{iu}\sum_{j=1}^{b}\frac{1}{j}\Big)\,\mathbf{E}(e^{iu\varpi(\sigma_d)})+ O\Big(|\,\mathbf{E}(e^{iu\varpi(\sigma_d)})|b^2d^{-1}+dq^{-b/2}+b^3(\log d)^{1/2}d^{-2}\Big), \quad (6.10)$$

with an absolute implied constant, in the range

$$q^{b/2}\geqslant d, \quad b\leqslant d. \quad (6.11)$$

Proof. Before introducting permutations, we separate the contribution of squarefree and non-squarefree polynomials in $T(d,b)$ (the intuition being that non-squarefree ones should be much sparser than for all polynomials because of the imposed divisibility only by large factors):

$$T(d,b) = T^\flat(d,b) + T^\sharp(d,b)$$

where

$$T^\flat(d,b) = \frac{1}{q^d}\sideset{}{^\flat}\sum_{\substack{\deg(f)=d\\ d^-(f)>b}} e^{iu\omega(f)},$$

and $T^\sharp(d,b)$ is the complementary term. We then estimate the latter by

$$\begin{aligned}|T^\sharp(d,b)| &\leqslant \sum_{b\leqslant\deg(g)\leqslant d/2}\frac{1}{q^d}\sum_{\substack{\deg(f)=d\\ g^2|f}} 1\\ &= \sum_{b\leqslant\deg(g)\leqslant d/2}\frac{1}{q^d}\sum_{\deg(f)=d-2\deg(g)} 1\\ &\leqslant \sum_{\deg(g)\geqslant b}\frac{1}{q^{2\deg(g)}} \ll \frac{1}{q^b}.\end{aligned}$$

We can now introduce permutations through the association $f\mapsto F_f^\sharp$ sending a squarefree polynomial to its associated cycle type. Using (5.1), we obtain

$$T^\flat(d,b) = \sum_{\substack{\sigma\in\mathfrak{S}_d\\ \ell^-(\sigma)>b}} e^{iu\varpi(\sigma)}\frac{1}{q^d}\sideset{}{^\flat}\sum_{\substack{\deg(f)=d\\ F_f^\sharp=\sigma^\sharp}} 1,$$

which is now a sum over permutations without small cycles. Using the third statement of Lemma 6.6, we derive

$$\begin{aligned}T^\flat(d,b) &= \sum_{\substack{\sigma\in\mathfrak{S}_d\\ \ell^-(\sigma)>b}} e^{iu\varpi(\sigma)}\,\mathbf{P}(\sigma_d=\sigma)\Big(1+O\Big(\frac{d}{q^{b/2}}\Big)\Big)\\ &= \mathbf{E}(e^{iu\varpi(\sigma_d)}\mathbf{1}_{\ell^-(\sigma_d)>b}) + O\Big(\mathbf{P}(\ell^-(\sigma_d)>b)dq^{-b/2}\Big),\end{aligned}$$

with an absolute implied constant if $q^{b/2} \geqslant d$.

Thus the problem is reduced to one about random permutations. Using Proposition 6.8 below with $\varepsilon = 1$, the proof is finished. □

Now recall that the characteristic function $\mathbf{E}(e^{iu\varpi(\sigma_d)})$ is explicitly known from (4.7). This formula, or (4.9), implies in particular that we have

$$\mathbf{E}(e^{iu\varpi(\sigma_{d-j})}) = \mathbf{E}(e^{iu\varpi(\sigma_d)})\Big(1 + O\Big(\frac{j}{d}\Big)\Big). \tag{6.12}$$

Then, inserting the formula of Proposition 6.7 in the first term S_1 of (6.9), and using this formula, we obtain in the range of validity (6.11) that

$$S_1 = \exp\Big(-e^{iu}\sum_{j=1}^{b}\frac{1}{j}\Big)\,\mathbf{E}(e^{iu\varpi(\sigma_d)})\sum_{\substack{\deg(g)\leqslant\sqrt{d}\\ d^+(g)\leqslant b}}\frac{e^{iu\omega(g)}}{|g|} + R$$

where, after some computations, we find that

$$R \ll (|\,\mathbf{E}(e^{iu\varpi(\sigma_d)})|b^2d^{-1} + dq^{-b/2} + b^3(\log d)^{1/2}d^{-2})S(\sqrt{d}, b),$$

with an absolute implied constant.

Extending the sum in the main term, we get

$$S_1 = M + R_1,$$

where

$$M = \mathbf{E}(e^{iu\varpi(\sigma_d)})\exp\Big(-e^{iu}\sum_{j=1}^{b}\frac{1}{j}\Big)\sum_{d^+(g)\leqslant b}\frac{e^{iu\omega(g)}}{|g|},$$

$$R_1 \ll bR(\sqrt{d}, b) + \Big(|\,\mathbf{E}(e^{iu\varpi(\sigma_d)})|\frac{b^2}{d} + \frac{d}{q^{b/2}} + \frac{b^3(\log d)^{1/2}}{d^2}\Big)S(\sqrt{d}, b).$$

Now, we can finally apply (6.5) and multiplicativity in the sum over g in M, to see that

$$M = \mathbf{E}(e^{iu\varpi(\sigma_d)})\prod_{\deg(\pi)\leqslant b}\Big(1 - \frac{1}{|\pi|}\Big)^{e^{iu}}\Big(1 + \frac{e^{iu}}{|\pi| - 1}\Big)\Big(1 + O\Big(\frac{1}{b}\Big)\Big)$$

and hence, by the mod-Poisson convergence of $\varpi(\sigma_d)$ and the absolute convergence of the Euler product extended to infinity, we have

$$\lim_{d,b\to+\infty}\exp((\log d)(1 - e^{iu}))M = \tilde{\Phi}_1(u)\tilde{\Phi}_2(u),$$

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

There remain to consider the error terms to conclude the proof of Theorem 6.1. We select $b = (\log d)^2 \to +\infty$; then (6.11) holds for all $d \geqslant d_0(q)$, and hence the previous estimates are valid and we must now show that

$$\exp((\log d)(1 - e^{iu}))R(\sqrt{d}, b) \to 0, \quad \exp((\log d)(1 - e^{iu}))R_1 \to 0$$

(the first desideratum coming from (6.9)).

Note that $|\exp((\log d)(1-e^{iu}))| \leqslant d^2$. Now we claim that

$$R(d,b) \ll b^C e^{-d/b} \tag{6.13}$$

$$S(d,b) \ll b, \tag{6.14}$$

for $1 \leqslant b \leqslant d$ and absolute constant $C > 0$, with absolute implied constants for the first, and an implied constant depending only on q for the second.

Granting this, we have

$$d^2 R(\sqrt{d}, (\log d)^2) \ll \exp\Big(2\log d + 2C\log\log d - \frac{\sqrt{d}}{(\log d)^2}\Big) \longrightarrow 0,$$

and all terms in R_1 are similarly trivially estimated, except for

$$\exp((\log d)(1-e^{iu}))|\,\mathbf{E}(e^{iu\varpi(\sigma_d)})|b^2 d^{-1} S(\sqrt{d}, b) \ll b^3 d^{-1} \longrightarrow 0,$$

using again the mod-Poisson convergence of $\varpi(\sigma_d)$.

We now justify (6.14) and (6.13): for the former, by (6.4), we have

$$|S(\sqrt{d}, b)| \leqslant \prod_{\deg(\pi)\leqslant b} \Big(1 + \frac{1}{|\pi|-1}\Big) \ll b,$$

and for the latter, we need only a simple application of the well-known Rankin trick: for any $\sigma \geqslant 0$, $d \geqslant 1$ and $g \in \mathbf{F}_q[X]$, we have

$$\mathbf{1}_{\deg(g)>d} \leqslant q^{\sigma(\deg(g)-d)},$$

and hence, by multiplicativity, we get

$$R(d,b) \leqslant q^{-\sigma d} \sum_{d^+(g)\leqslant b} q^{(\sigma-1)\deg(g)} = q^{-\sigma d} \prod_{\deg(\pi)\leqslant b} (1-|\pi|^{\sigma-1})^{-1},$$

which we estimate further for σ using

$$\begin{aligned}\prod_{\deg(\pi)\leqslant b} (1-|\pi|^{\sigma-1})^{-1} &= \exp\Big(\sum_{\deg(\pi)\leqslant b}\sum_{k\geqslant 1} \frac{|\pi|^{k(\sigma-1)}}{k}\Big)\\ &\leqslant \exp\Big(C\sum_{j=1}^{b} \frac{q^{j\sigma}}{j}\Big) \leqslant \exp(C' q^{\sigma b}\log b)\end{aligned}$$

for some absolute constants $C, C' > 0$. Taking $\sigma = 1/(b\log q)$ leads immediately to (6.13).

Finally, here is the computation of the characteristic function of the cycle count of permutations without small parts that we used in the proof of Proposition 6.7.

Proposition 6.8. *For all $d \geqslant 2$ and $b \geqslant 0$ such that $b \leqslant d$, we have*

$$\begin{aligned}\mathbf{E}(e^{iu\varpi(\sigma_d)}\mathbf{1}_{\ell^-(\sigma_d)>b}) &= \exp\Big(-e^{iu}\sum_{j=1}^{b}\frac{1}{j}\Big)\,\mathbf{E}(e^{iu\varpi(\sigma_d)})\\ &\quad + O(|\,\mathbf{E}(e^{iu\varpi(\sigma_d)})|b^{1+\varepsilon}d^{-1} + b^3(\log d)^{1/2}d^{-2}),\end{aligned} \tag{6.15}$$

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

Proof. This is essentially a sieve (or inclusion-exclusion) argument, which may well be already known (although we didn't find it explicitly in our survey of the literature). To simplify the notation, we will prove the statement by induction on b, although this may not be necessary; taking care of the error terms is then slightly more complicated, and readers should probably first disregard them to see the main flow of the argument.

We denote

$$\Phi_{d,b}(u) = \mathbf{E}(e^{iu\varpi(\sigma_d)}\mathbf{1}_{\ell^-(\sigma_d)>b}), \quad \Phi_d(u) = \Phi_{d,0}(u), \quad h_b = \sum_{j=1}^{b} \frac{1}{j}.$$

We will write

$$\Phi_{d,b} = \exp(-e^{iu}h_b)\Phi_d + |\Phi_d|E_{d,b} + F_{d,b}, \tag{6.16}$$

where $E_{d,b}$, $F_{d,b} \geqslant 0$; such an expression holds for $b = 0$, with $E_{d,0} = F_{d,0} = 0$, and we will proceed inductively to obtain an expression for $\Phi_{d,b}$ from that of $\Phi_{d',b-1}$, $d' \leqslant d$, from which we will derive estimates for $E_{d,b}$ and $F_{d,b}$ in general. Note that we can assume that d is large enough (i.e., larger than any fixed constant), since smaller values of d (and b) are automatically incorporated by making the right-most implied constant large enough in (6.15). Also, we can always write such a formula with $|F_{d,b}| \ll b$, for some absolute constant, since the characteristic functions $\Phi_{d,b}$ are bounded by 1 and $\exp(-e^{iu}h_b) \ll b$.

Now, with these preliminaries settled, let I be the set of b-cycles in $\mathfrak{S}_d$; we write $\tau \mid \sigma$ (resp. $\tau \nmid \sigma$) to indicate that $\tau \in I$ occurs (resp. does not occur) in the decomposition of σ in cycles. Then we have

$$\begin{aligned}\Phi_{d,b}(u) &= \mathbf{E}(e^{iu\varpi(\sigma_d)}\mathbf{1}_{\ell^-(\sigma_d)>b}) \\ &= \frac{1}{d!}\sum_{\substack{\ell^-(\sigma)>b-1 \\ \tau\in I\Rightarrow\tau\nmid\sigma}} e^{iu\varpi(\sigma)} = \frac{1}{d!}\sum_{\ell^-(\sigma)>b-1} e^{iu\varpi(\sigma)}\prod_{\tau\in I}(1-\mathbf{1}_{\tau|\sigma}).\end{aligned}$$

We expand the product as a sum over subsets $J \subset I$, and exchange the two sums, getting

$$\Phi_{d,b}(u) = \frac{1}{d!}\sum_{J\subset I}(-1)^{|J|}\sum_{\substack{\ell^-(\sigma)>b-1 \\ \tau\in J\Rightarrow\tau|\sigma}} e^{iu\varpi(\sigma)}.$$

Now fix a $J \subset I$ such that the inner sum is *not empty*. This implies of course that the support of the cycles in J are disjoint, in particular that those cycles contribute $|J|$ to $\varpi(\sigma)$. Moreover, if we call A the complement of the union of the support of the cycles in J, we have $|A| = d - |J|b$, and any σ in the inner sum maps A to itself. Thus, by enumerating the elements of A, we can map injectively those σ to permutations in $\mathfrak{S}_{d-|J|b}$, and the image

of this map is exactly the set of those $\sigma_1 \in \mathfrak{S}_{d-|J|b}$ for which $\ell^-(\sigma_1) > b-1$. Moreover, if σ maps to σ_1, we have

$$\varpi(\sigma) = |J| + \varpi(\sigma_1),$$

and thus we get

$$\sum_{\substack{\ell^-(\sigma)>b-1\\ \tau\in J\Rightarrow\tau|\sigma}} e^{iu\varpi(\sigma)} = e^{iu|J|} \sum_{\substack{\sigma\in\mathfrak{S}_{d-|J|b}\\ \ell^-(\sigma)>b-1}} e^{iu\varpi(\sigma)},$$

and then

$$\begin{aligned}\Phi_{d,b}(u) &= \sum_{J\subset I} \frac{(d-|J|b)!}{d!}(-e^{iu})^{|J|}\,\mathbf{E}(e^{iu\varpi(\sigma_{d-|J|b})}\mathbf{1}_{\ell^-(\sigma_{d-|J|b})>b-1}),\\ &= \sum_{J\subset I} \frac{(d-|J|b)!}{d!}(-e^{iu})^{|J|}\Phi_{d-|J|b,b-1}(u),\end{aligned}$$

the sum over J being implicitly restricted to those subsets of I for which there is at least one permutation in $\mathfrak{S}_d$ where all cycles in J occur.

In particular, we have $|J| \leqslant d/b$ (so there is enough room to find that many disjoint b-cycles), and if we denote by $S(k,b)$ the number of possible such subsets of I with $|J| = k$, we can write

$$\Phi_{d,b}(u) = \sum_{k=0}^{d/b} S(k,b)\frac{(d-kb)!}{d!}(-e^{iu})^k\Phi_{d-kb,b-1}(u)$$

Now we claim that

$$S(k,b) = \binom{d}{d-kb} \times \frac{(kb)!}{b^k k!} = \frac{d!}{(d-kb)!b^k k!}.$$

Indeed, to construct the subsets J with $|J| = k$, we can first select arbitrarily a subset A of size $d-kb$ in $\{1,\dots,d\}$, and then select, independently, an arbitrary set of k disjoint b-cycles supported outside A. The choice of A corresponds to the binomial factor above, and the second factor is clearly equal to the number of permutations $\sigma \in \mathfrak{S}_{kb}$ which are a product of k disjoint b-cycles. Those are all conjugate in $\mathfrak{S}_{kb}$, and their cardinality is given by (6.7), applied with d replaced by kb and all $r_j = 0$ except for $r_b = k$.

Consequently, we obtain the basic induction relation

$$\Phi_{d,b}(u) = \sum_{k=0}^{d/b} \Big(\frac{-e^{iu}}{b}\Big)^k \frac{1}{k!}\Phi_{d-kb,b-1}(u).$$

Before applying the induction assumption (6.16), we shorten the sum over k so that $\Phi_{d-kb,b-1}$ will remain close to $\Phi_{d,b-1}$. For this, we use the inequality

$$\Big|\sum_{k=0}^{m}\frac{z^k}{k!} - e^z\Big| \leqslant \frac{1}{m!},$$

for $|z| \leqslant 1$, $m \geqslant 0$, as well as $|\Phi_{d-kb}(u)| \leqslant 1$, and deduce that

$$\Phi_{d,b}(u) = \sum_{k=0}^{m} \Big(\frac{-e^{iu}}{b}\Big)^k \frac{1}{k!} \Phi_{d-kb,b-1}(u) + O\Big(\frac{1}{m!}\Big), \tag{6.17}$$

for some m to be specified later, subject for the moment only to the condition $m < d/2b$, and an implied constant which is at most 1.

By (6.16), we have

$$\Phi_{d-kb,b-1}(u) = \exp(-e^{iu}h_{b-1})\Phi_{d-kb}(u) + |\Phi_{d-kb}(u)|E_{d-kb,b-1} + F_{d-kb,b-1}.$$

Moreover, by (6.12), we also know that for $k \leqslant m$, we have

$$\Phi_{d-kb}(u) = \mathbf{E}(e^{iu\varpi(\sigma_d)})\Big(1 + O\Big(\frac{kb}{d}\Big)\Big) = \Phi_d(u)\Big(1 + O\Big(\frac{kb}{d}\Big)\Big), \tag{6.18}$$

with an absolute implied constant. Hence, we obtain

$$\Phi_{d,b}(u) = \exp(-e^{iu}h_{b-1})\Phi_d(u)M + R + S$$

where

$$\begin{aligned}
M &= \sum_{k=0}^{m} \Big(\frac{-e^{iu}}{b}\Big)^k \frac{1}{k!}\Big(1 + O\Big(\frac{bk}{d}\Big)\Big)\\
|R| &\leqslant \sum_{k=0}^{m} \frac{1}{b^k k!} E_{d-kb,b-1}|\Phi_{d-kb}(u)|\\
&= |\Phi_d(u)| \sum_{k=0}^{m} \frac{1}{b^k k!} E_{d-kb,b-1}\Big(1 + O\Big(\frac{kb}{d}\Big)\Big)\\
|S| &\leqslant \sum_{k=0}^{m} \frac{1}{b^k k!} F_{d-kb,b-1} + \frac{1}{m!}.
\end{aligned}$$

We next write

$$M = \exp\Big(-\frac{e^{iu}}{b}\Big) + O\Big(\frac{1}{d}\sum_{k=1}^{m} \frac{1}{b^{k-1}(k-1)!}\Big) + O\Big(\frac{1}{m!}\Big),$$

where the implied constants are absolute, and deduce that

$$\Phi_{d,b}(u) = \exp(-e^{iu}h_b)\Phi_d(u) + |\Phi_d(u)|M_1 + R + S,$$

with

$$|M_1| \ll \frac{1}{m!} + d^{-1}e^{1/b},$$

where the implied constant is absolute. The desired shape of the main term is now visible, and it remains to verify that (for a suitable m) the other terms are bounded as stated in the proposition.

First, comparing with (6.16), with the terms in R_1 and R contributing to $E_{d,b}$, while those in S contribute to $F_{d,b}$, we see that we have

$$F_{d,b} \leqslant \sum_{k=0}^{m} \frac{1}{b^k k!} F_{d-kb,b-1} + \frac{1}{m!}.$$

We now select $m = \lfloor \log d \rfloor$. Then, together with $F_{d,0} = 0$, we claim that this inductive inequality implies

$$F_{d,b} \leqslant Cb^3 (\log d)^{1/2} d^{-2}, \tag{6.19}$$

for $b \leqslant d$ and some absolute implied constant $C \geqslant 1$. For a large enough value of C, note that this is already true for all $d \leqslant d_0$, where d_0 can be any fixed integer. We select d_0 so that

$$\frac{1}{m!} \leqslant \frac{1}{d^2},$$

for $d \geqslant d_0$, and we can thus assume that $d > d_0$ from now on.

The desired bound holds, of course, for $b = 0$. It is also trivial if $b(\log d) \geqslant d/24$ (say), because we have observed at the beginning that (6.16) can be obtained with $F_{d,b} \ll b$. If it is assumed to be true for all d and $b-1$, we have for $b(\log d) < d/24$ that

$$\begin{aligned} F_{d,b} &\leqslant \frac{1}{m!} + C \sum_{k=0}^{m} \frac{1}{b^k k!} F_{d-kb,b-1} \\ &\leqslant \frac{1}{m!} + \frac{C(\log d)^{1/2}(b-1)^3}{d^2} \sum_{k=0}^{m} \frac{1}{b^k k!} \Big(1 - \frac{kb}{d}\Big)^{-2}. \end{aligned}$$

We note the following simple inequalities

$$(1-x)^{-1} \leqslant e^{2x}, \quad \exp(x) \leqslant 1 + \frac{3x}{2}, \quad \text{for } 0 \leqslant x \leqslant 1/2,$$
$$(x-1)e^{1/x} \leqslant x, \qquad \text{for } 0 \leqslant x \leqslant 1,$$

and from them we deduce that if $b(\log d) < d/24$ (so that $kb/d \leqslant 1/2$ for the values involved), we have

$$\sum_{k=0}^{m} \frac{1}{b^k k!} \Big(1 - \frac{kb}{d}\Big)^{-2} \leqslant \sum_{k=0}^{m} \frac{1}{k!} \Big(\frac{\exp(4b/d)}{b}\Big)^k \leqslant \exp\Big(\frac{1}{b} + \frac{6}{d}\Big)$$

and, hence (from the same simple inequalities) we get

$$\begin{aligned} (b-1)^3 \sum_{k=0}^{m} \frac{1}{b^k k!} \Big(1 - \frac{kb}{d}\Big)^{-2} &\leqslant (b-1)^{3/2} \times (b-1) \exp\Big(\frac{1}{b}\Big) \\ &\quad \times \Big((b-1)\exp\Big(\frac{1}{3d}\Big)\Big)^{1/2} \leqslant (b-1)^{3/2} b^{3/2}. \end{aligned}$$

By the choice of d_0, we deduce for $b \geqslant 1$ and $d > d_0$ that we have

$$F_{d,b} \leqslant d^{-2} (\log d)^{1/2} (1 + Cb^{3/2}(b-1)^{3/2}) \leqslant Cd^{-2} b^3,$$

(assuming again C large enough), completing the verification of (6.19) by induction.

Finally, from (6.16) and the foregoing, we deduce similarly that

$$E_{d,b} \leqslant D\Big(\frac{1}{m!} + d^{-1}e^{1/b}\Big) + \sum_{k=0}^{m} \frac{1}{b^k k!} E_{d-kb,b-1}\Big(1 + O\Big(\frac{kb}{d}\Big)\Big),$$

for some absolute constant $D \geqslant 0$. Fix $\varepsilon > 0$, and consider the bound

$$E_{d,b} \leqslant Cb^{1+\varepsilon}d^{-1};$$

then if $C \geqslant 1$, assuming it for $b-1$, we obtain the inductive bound

$$\begin{aligned} E_{d,b} &\leqslant d^{-1}\Big\{D(1+e^{1/b}) + C(b-1)^{1+\varepsilon}\sum_{k=0}^{m}\frac{1}{b^k k!}\Big(1+\frac{\beta kb}{d}\Big)\Big(1-\frac{kb}{d}\Big)^{-1}\Big\} \\ &\leqslant d^{-1}\Big\{D(1+e^{1/b}) + C(b-1)^{1+\varepsilon}\exp\Big(\frac{1}{b}+\frac{3(\beta+2)}{2d}\Big)\Big\} \end{aligned}$$

(using again the elementary inequalities above). Then for $d \geqslant d_1(\varepsilon)$, provided $C \geqslant 1$, we obtain

$$E_{d,b} \leqslant Cb^{1+\varepsilon}d^{-1},$$

confirming the validity of this estimate. □

Remark 6.9. Proposition 6.8 can itself be seen as an instance of mod-Poisson convergence, for the cycle count of randomly, uniformly, chosen permutations in $\mathfrak{S}_d$ without small cycles.

Precisely, let $\mathfrak{S}_d^{(b)}$ denote the set of $\sigma \in \mathfrak{S}_d$ with $\ell^-(\sigma) > b$. We then find first (by putting $u = 0$ in Proposition 6.8) that

$$\frac{|\mathfrak{S}_d^{(b)}|}{|\mathfrak{S}_d|} \sim_{d,b\to+\infty} \exp\Big(-\sum_{j=1}^{b}\frac{1}{j}\Big) \sim \frac{e^{-\gamma}}{b},$$

provided b is restricted by $b \ll d^{1/2-\varepsilon}$ with $\varepsilon > 0$ arbitrarily small. Then, for arbitrary $u \in \mathbf{R}$ and b similarly restricted, we find that

$$\frac{1}{|\mathfrak{S}_d^{(b)}|}\sum_{\sigma\in\mathfrak{S}_d^{(b)}} e^{iu\varpi(\sigma)} \sim_{d,b\to+\infty} \exp\Big((1-e^{iu})\sum_{j=1}^{b}\frac{1}{j}\Big)\,\mathbf{E}(e^{iu\varpi(\sigma_d)}),$$

locally uniformly. Thus the mod-Poisson convergence (4.8) for $\varpi(\sigma_d)$ implies mod-Poisson convergence for the cycle count restricted to $\mathfrak{S}_d^{(b)}$ as long as $b \ll d^{1/2-\varepsilon}$, with limiting function $1/\Gamma(e^{iu})$ and parameters

$$\log d - \sum_{j=1}^{b}\frac{1}{j} \sim \log\frac{d}{b}.$$

It may be that the restriction of b with respect to d could be relaxed. However, in the opposite direction, note that for $b = d-1$, the number of d-cycles in $\mathfrak{S}_d$, i.e., $|\mathfrak{S}_d^{(d-1)}|$, is $(d-1)!$, so the ratio is $1/d$ which is obviously not asymptotic with $e^{-\gamma}/(d-1)$.

Remark 6.10. We come back to the asymptotic formula (6.5), to explain how it follows from Theorem 6.1 in the sharper form

$$\prod_{\deg(\pi)\leqslant d}\Big(1-\frac{1}{|\pi|}\Big)=\exp\Big(-\sum_{1\leqslant j\leqslant d}\frac{1}{j}\Big)\Big(1+O\Big(\frac{1}{q^{d/2}}\Big)\Big). \tag{6.20}$$

Namely, it is very easy to derive this asymptotic up to some constant:

$$\prod_{\deg(\pi)\leqslant d}\Big(1-\frac{1}{|\pi|}\Big)=\exp\Big(\gamma_q-\sum_{1\leqslant j\leqslant d}\frac{1}{j}\Big)\Big(1+O\Big(\frac{1}{q^{d/2}}\Big)\Big),$$

where γ_q is given by the awkward, yet absolutely convergent, expression

$$\gamma_q=\sum_{\pi}\Big(\log\Big(1-\frac{1}{|\pi|}\Big)+\frac{1}{|\pi|}\Big)+\sum_{j\geqslant 1}\Big(\frac{\Pi_q(j)}{q^j}-\frac{1}{j}\Big). \tag{6.21}$$

From this, the flow of the proof leads to the mod-Poisson limit (6.1), with an additional factor $\exp(-\gamma_q e^{iu})$ in the limit. But for $u=0$, both sides of (6.1) are equal to 1, so we must have $\exp(\gamma_q)=1$ for all q. (This is another interesting example of the information coming from mod-Poisson convergence, which is invisible at the level of the normal limit; note in particular that this is really a manifestation of the random permutations.)

7. Final comments and questions

Many natural questions arise out of this paper. The most obvious concern the general notion of mod-Poisson convergence, and its probabilistic significance and relation with other types of convergence and measures of approximation (and similarly for mod-Gaussian behavior). Already from [11], it is clear that mod-Poisson convergence should be a very general fact in the setting of "logarithmic combinatorial structures", as discussed in [1].

In the direction suggested by the Erdős-Kac Theorem, there is a very abundant literature concerning generalizations to additive functions and beyond (see, e.g., the discussion at the end of [9]), and again it would be interesting to know which of those Central Limit Theorems extend to mod-Poisson convergence, and maybe even more so, to know which *don't*.

In the direction of pursuing the analogy with distribution of L-functions, the first thing to do might be to construct a proof of the mod-Poisson Erdős-Kac Theorem for integers which parallels the one of the previous section. This does not seem out of the question, but our current attempts suffer from the fact that the associations of permutations in "$\mathfrak{S}_{\log N}$" to integers $n\leqslant N$ that we have considered are ad-hoc (though potentially useful), and do not carry the flavor of a generalization of the Frobenius. It is then difficult to envision a further natural analogue of a unitary matrix associated, say, with $\zeta(1/2+it)$. One can suggest a "made up" matrix U_t obtained by taking the zeros of $\zeta(s)$ close to t, and wrapping them around the unit circle after proper rescaling, but this also lacks a good a priori definition – though this was studied by Coram and Diaconis [5], who obtained extremely

good numerical agreement; this is also close to the "hybrid" model for the Riemann zeta function of Gonek, Hughes and Keating [7].

One may hope for more success in the case of finite fields in trying to understand (for instance) families of L-functions of algebraic curves in the limit of large genus, since the definition of a random matrix from Frobenius does not cause problem there (though recall it is really a *conjugacy class*). However, although we have Deligne's Equidistribution Theorem in the "vertical" direction $q \to +\infty$, and its proof is highly effective, it is not clear what a suitable analogue of the quantitative "diagonal" equidistribution (6.6) in Lemma 6.6 should be. More precisely, what condition should replace the restriction to polynomials without small irreducible factors? We do not have clear answers at the moment, but we hope to make progress in later work.

Finally, it should be clear that analogues of mod-Gaussian and mod-Poisson convergence exist, involving other families of probability distributions. Some cases related to discrete variables are discussed in [3, §5], and one may also define "mod-stable" convergence in an obvious way (though we do not have interesting examples of these to suggest at the moment). It may be interesting to investigate links between these various definitions; the last part of Proposition 2.4 suggests that there should exist interesting relations.

References

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

[2] A.D. Barbour and P. Hall: *On the rate of Poisson convergence*, Math. Proc. Camb. Phil. Soc. 95 (1984), 473–480.

[3] A.D. Barbour, E. Kowalski and A. Nikeghbali: *Mod-discrete expansions*, preprint (2009), `arXiv:0912.1886`

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

[5] M. Coram and P. Diaconis: *New tests of the correspondence between unitary eigenvalues and the zeros of Riemann's zeta function*, J. Phys. A. 36 (2000), 2883–2906.

[6] P. Flajolet and M. Soria: *Gaussian limiting distributions for the number of components in combinatorial structures*, J. Combin. Theory Ser. A 53 (1990), 165–182.

[7] S. Gonek, C. Hughes and J. Keating: *A hybrid Euler-Hadamard product for the Riemann zeta function*, Duke Math. J. 136 (2007), 507–549.

[8] A. Granville: *The anatomy of integers and permutations*, preprint (2008), `http://www.dms.umontreal.ca/~andrew/PDF/Anatomy.pdf`

[9] A. Granville and K. Soundararajan: *Sieving and the Erdős-Kac Theorem*, in "Equidistribution in Number Theory, An Introduction", edited by A. Granville and Z. Rudnick, Springer Verlag 2007.

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

[11] Hwang, H-K.: *Asymptotics of Poisson approximation to random discrete distributions: an analytic approach*, Adv. Appl. Prob. 31 (1999), 448–491.

[12] J. Jacod, E. Kowalski and A. Nikeghbali: *Mod-Gaussian convergence: new limit theorems in probability and number theory*, to appear in Forum Math; `arXiv:0807.4739`

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

[14] J.P. Keating and N.C. Snaith: *Random matrix theory and* $\zeta(1/2+it)$, Commun. Math. Phys. **214**, (2000), 57-89.
[15] V.V. Petrov: *Limit Theorems of Probability Theory*, Oxford University Press, Oxford, 1995.
[16] A. Rényi and P. Turán: *On a theorem of Erdős-Kac*, Acta Arith. 4 (1958), 71–84.
[17] R.C. Rhoades: *Statistics of prime divisors in function fields*, Internat. J. Number Theory 5 (2009), 141–152.
[18] B. Roos: *Sharp constants in the Poisson approximation*, Stat. Prob. Letters 52 (2001), 155–168.
[19] M. Rosen: *A generalization of Mertens' theorem*, J. Ramanujan Math. Soc. 14 (1999), 1–19.
[20] G. Tenenbaum: *Introduction to analytic and probabilistic number theory*, Cambridge Studies Adv. Math. **46**, Cambridge Univ. Press, 1995.
[21] E.T. Whittaker and G.N. Watson: *A course in modern analysis*, 4th Edition, Cambridge Math. Library, Cambridge Univ. Press, 1996.

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