Some functional limit theorems in number theory

E. Kowalski

ETH Zürich

November 2016

Introduction

Many objects in number theory exhibit apparently unpredictable individual behavior, but have more regular average properties.

Introduction

Many objects in number theory exhibit apparently unpredictable individual behavior, but have more regular average properties. For instance, for a positive integer $n \geq 1$, the number $\omega(n)$ of prime divisors of n fluctuates "randomly" as n increases. But on average, we have

$$\frac{1}{N} \sum_{n \leq N} \omega(n) \sim \log\log(N)$$

as $N \to \infty$.

This regularity often leads (conjecturally or provably) to convergence in law results on arithmetic invariants.

Examples

To state this in general, we package the set $\mathcal{X}$ of arithmetic objects in "finite" subsets Ω_N, give them some probability measure $\mathbf{P}_N$, and investigate the limits of sequences of random variables defined on Ω_N.

Examples

To state this in general, we package the set $\mathcal{X}$ of arithmetic objects in "finite" subsets Ω_N, give them some probability measure $\mathbf{P}_N$, and investigate the limits of sequences of random variables defined on Ω_N.

The Erdős-Kac Theorem. Here $\mathcal{X} = \{n \geq 1\}$, $\Omega_N = \{1, \ldots, N\}$ with uniform probability $\mathbf{P}_N$ and we consider $X_N \colon n \mapsto \omega(n)$ as random variables. Then

$$\frac{X_N - \log\log N}{\sqrt{\log\log N}} \Rightarrow \mathcal{N}(0, 1).$$

Examples

To state this in general, we package the set $\mathcal{X}$ of arithmetic objects in "finite" subsets Ω_N, give them some probability measure $\mathbf{P}_N$, and investigate the limits of sequences of random variables defined on Ω_N.

The Erdős-Kac Theorem. Here $\mathcal{X} = \{n \geq 1\}$, $\Omega_N = \{1, \ldots, N\}$ with uniform probability $\mathbf{P}_N$ and we consider $X_N \colon n \mapsto \omega(n)$ as random variables. Then

$$\frac{X_N - \log\log N}{\sqrt{\log\log N}} \Rightarrow \mathcal{N}(0,1).$$

Selberg's Theorem. Let $\mathcal{X} = \mathbf{R}$, $\Omega_N = [-N, N]$ with normalized Lebesgue measure and consider $X_N \colon t \mapsto \log|\zeta(1/2 + it)|$ as random variables. Then

$$\frac{X_N}{\sqrt{\frac{1}{2}\log\log N}} \Rightarrow \mathcal{N}(0,1).$$

Functional limit theorems

The Erdős-Kac Theorem revisited (Billingsley). On Ω_N as in the first example, define *processes* $(X_N(t))_{0\leq t\leq 1}$ by counting prime divisors

$$p \leq \exp((\log N)^t)$$

of n for $0 \leq t \leq 1$. Then a normalized version of $(X_N(t))$ converges in law to Brownian Motion on $[0,1]$.

Functional limit theorems

The Erdős-Kac Theorem revisited (Billingsley). On Ω_N as in the first example, define *processes* $(X_N(t))_{0\leq t\leq 1}$ by counting prime divisors

$$p \leq \exp((\log N)^t)$$

of n for $0 \leq t \leq 1$. Then a normalized version of $(X_N(t))$ converges in law to Brownian Motion on $[0,1]$.

We will present examples that are (maybe...) more natural, because they involve arithmetic objects that are themselves *functions*, and not just integers or real numbers. We then naturally want to have "functional" limit theorems that reflect this feature.

Part I: The distribution of values of L-functions

The most famous functions in number theory are the L-functions. A typical L-function is a function of a complex variable $s = \sigma + it$ given for $\mathrm{Re}(s)$ large enough by a Dirichlet series and an Euler product

$$L(s) = \sum_{n \geq 1} \lambda(n) n^{-s} = \prod_{p} L_p(p^{-s})^{-1},$$

that extends to a holomorphic function on $\mathbf{C}$ with a possible pole at $s = 1$.

Part I: The distribution of values of L-functions

The most famous functions in number theory are the L-functions. A typical L-function is a function of a complex variable $s = \sigma + it$ given for $\mathrm{Re}(s)$ large enough by a Dirichlet series and an Euler product

$$L(s) = \sum_{n \geq 1} \lambda(n) n^{-s} = \prod_{p} L_p(p^{-s})^{-1},$$

that extends to a holomorphic function on $\mathbf{C}$ with a possible pole at $s = 1$.

The Riemann zeta function. For $\mathrm{Re}(s) > 1$, we have

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_{p} (1 - p^{-s})^{-1}.$$

Part I: The distribution of values of L-functions

The most famous functions in number theory are the L-functions. A typical L-function is a function of a complex variable $s = \sigma + it$ given for $\mathrm{Re}(s)$ large enough by a Dirichlet series and an Euler product

$$L(s) = \sum_{n \geq 1} \lambda(n) n^{-s} = \prod_p L_p(p^{-s})^{-1},$$

that extends to a holomorphic function on $\mathbf{C}$ with a possible pole at $s = 1$.

The Riemann zeta function. For $\mathrm{Re}(s) > 1$, we have

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_p (1 - p^{-s})^{-1}.$$

Ramanujan's function. Here we define $(\lambda(n))_{n \geq 1}$ by the identity

$$q \prod_{n \geq 1} (1 - q^n)^{24} = \sum_{n \geq 1} n^{11/2} \lambda(n) q^n,$$

and for $\mathrm{Re}(s) > 1$ we have $\displaystyle\sum_{n \geq 1} \lambda(n) n^{-s} = \prod_p (1 - \lambda(p) p^{-s} + p^{-2s})^{-1}$.

Bagchi's Theorem

We are interested in the distribution of values of *L*-functions. Such questions go back to H. Bohr, Jessen, etc. But they considered "individual" values instead of viewing the *L*-function as a holomorphic function. Bagchi's Thesis gives the first statement of this second kind.

Bagchi's Theorem

We are interested in the distribution of values of L-functions. Such questions go back to H. Bohr, Jessen, etc. But they considered "individual" values instead of viewing the L-function as a holomorphic function. Bagchi's Thesis gives the first statement of this second kind.

Bagchi's Theorem

For $T > 0$, let $\Omega_T = [-T, T]$ with uniform measure. Let $\mathcal{C}$ be a relatively compact open subset of the strip $1/2 < \mathrm{Re}(s) < 1$, and $\mathcal{H}(\mathcal{C})$ the Banach space of holomorphic functions in $\mathcal{C}$, continuous on $\bar{\mathcal{C}}$. Let ζ_T be the random variable on Ω_T sending t to the element $s \mapsto \zeta(s + it)$ of $\mathcal{H}(\mathcal{C})$.
Then ζ_T converges in law, as $T \to +\infty$, to the random Euler product

$$\prod_p (1 - \mathrm{X}_p p^{-s})^{-1}$$

where $(\mathrm{X}_p)_p$ is a sequence of independent random variables identically uniformly distributed on the unit circle.

Bagchi's Theorem for modular forms

Many people (Laurinčikas, Matsumoto, and others) have extended Bagchi's Theorem to vertical shifts (or twists by Dirichlet characters) of other L-functions.
The following statement is the first genuinely "higher rank" version.

Bagchi's Theorem for modular forms

Many people (Laurinčikas, Matsumoto, and others) have extended Bagchi's Theorem to vertical shifts (or twists by Dirichlet characters) of other L-functions.
The following statement is the first genuinely "higher rank" version.

Bagchi's Theorem for modular forms (K.)

For $q \geq 17$ prime, let Ω_q be the finite set of primitive weight 2 cusp forms of level q with "harmonic" measure (think uniform...) Let L_q be the random variable on Ω_q sending f to the element $s \mapsto L(s, f)$ of $\mathcal{H}(\mathcal{C})$. Then L_q converges in law, as $q \to +\infty$, to the random Euler product

$$\prod_p \det(1 - p^{-s}\mathsf{Y}_p)^{-1}$$

where $(\mathsf{Y}_p)_p$ is a sequence of independent random variables on $\mathrm{SU}_2(\mathbf{C})^\sharp$ identically distributed according to the Haar measure, namely

$$\frac{2}{\pi}\sin^2(\theta)d\theta, \quad \text{for} \quad \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}, \quad \theta \in [0, \pi].$$

Sketch of the proof

For any $f \in \Omega_q$, it is known that for $\mathrm{Re}(s) > 1$, we have

$$L(f, s) = \prod_{p \neq q} (1 - \lambda_f(p) p^{-s} + p^{-2s})^{-1} (1 - \lambda_f(q) q^{-s})^{-1},$$

Sketch of the proof

For any $f \in \Omega_q$, it is known that for $\mathrm{Re}(s) > 1$, we have

$$L(f,s) = \prod_{p \neq q} (1 - \lambda_f(p) p^{-s} + p^{-2s})^{-1} (1 - \lambda_f(q) q^{-s})^{-1},$$

and that there exists $\theta_p(f) \in [0, \pi]$ such that for $p \neq q$, we have

$$1 - \lambda_f(p) p^{-s} + p^{-2s} = \det(1 - p^{-s} \mathrm{S}_p(f))$$

where

$$\mathrm{S}_p(f) = \begin{pmatrix} e^{i\theta_p(f)} & 0 \\ 0 & e^{-i\theta_p(f)} \end{pmatrix} \in \mathrm{SU}_2(\mathbf{C}).$$

Sketch of the proof, continued

The basic fact that makes the connection between number theory and probability is the:

Local spectral equidistribution [Hecke, Petersson]

As $q \to +\infty$, the sequence $(\mathsf{S}_p)_p$ converges in law to $(\mathsf{Y}_p)_p$.

Sketch of the proof, continued

The basic fact that makes the connection between number theory and probability is the:

Local spectral equidistribution [Hecke, Petersson]

As $q \to +\infty$, the sequence $(\mathsf{S}_p)_p$ converges in law to $(\mathsf{Y}_p)_p$.

We should therefore expect that

$$\prod_p (1 - \lambda_f(p)p^{-s} + p^{-2s})^{-1} = \prod_p \det(1 - p^{-s}\mathsf{S}_p)^{-1}$$

$$\Longrightarrow \quad \prod_p \det(1 - p^{-s}\mathsf{Y}_p)^{-1}.$$

Sketch of the proof, continued

The basic fact that makes the connection between number theory and probability is the:

Local spectral equidistribution [Hecke, Petersson]

As $q \to +\infty$, the sequence $(\mathsf{S}_p)_p$ converges in law to $(\mathsf{Y}_p)_p$.

We should therefore expect that

$$\prod_p (1 - \lambda_f(p)p^{-s} + p^{-2s})^{-1} = \prod_p \det(1 - p^{-s}\mathsf{S}_p)^{-1}$$

$$\Longrightarrow \quad \prod_p \det(1 - p^{-s}\mathsf{Y}_p)^{-1}.$$

This works with no more ado for $\mathrm{Re}(s) > 1$ (absolute convergence). In the strip $1/2 < \mathrm{Re}(s) < 1$, one must be a bit more careful.

Sketch of the proof, continued

One uses instead the Dirichlet series expansions

$$\prod_{p} \det(1 - p^{-s} \mathrm{Y}_p)^{-1} = \sum_{n \geq 1} \mathrm{Y}_n n^{-s}, \qquad \sigma > 1,$$

and compactly supported smooth approximations

$$\sum_{n \geq 1} \varphi\Big(\frac{n}{N}\Big) \lambda_f(n) n^{-s}, \qquad \sum_{n \geq 1} \varphi\Big(\frac{n}{N}\Big) \mathrm{Y}_n n^{-s}.$$

Sketch of the proof, continued

One uses instead the Dirichlet series expansions

$$\prod_{p} \det(1 - p^{-s} \mathsf{Y}_p)^{-1} = \sum_{n \geq 1} \mathsf{Y}_n n^{-s}, \qquad \sigma > 1,$$

and compactly supported smooth approximations

$$\sum_{n \geq 1} \varphi\Big(\frac{n}{N}\Big) \lambda_f(n) n^{-s}, \qquad \sum_{n \geq 1} \varphi\Big(\frac{n}{N}\Big) \mathsf{Y}_n n^{-s}.$$

Since the sums are finite, local spectral equidistribution shows that the arithmetic sums converge in law to the random ones (for fixed N).

Sketch of the proof, concluded

Another arithmetic ingredient is needed:

First moment estimate (K.– Michel)

If $1/2 < \sigma_0$, then there exists $A > 0$ such that, uniformly for $\mathrm{Re}(s) \geq \sigma_0$, we have

$$\mathbf{E}_q(|L(f,s)|) \ll (1+|s|)^A.$$

Sketch of the proof, concluded

Another arithmetic ingredient is needed:

First moment estimate (K.– Michel)

If $1/2 < \sigma_0$, then there exists $A > 0$ such that, uniformly for $\mathrm{Re}(s) \geq \sigma_0$, we have

$$\mathbf{E}_q(|L(f,s)|) \ll (1+|s|)^A.$$

Using this (resp. the easier analogue statement for the random Dirichlet series), one proves

$$\mathbf{E}_q\Bigl(\Bigl\|L(f,s) - \sum_n \varphi\Bigl(\frac{n}{N}\Bigr)\lambda_f(n)n^{-s}\Bigr\|_\infty\Bigr) \ll N^{-\delta}$$

for some $\delta > 0$ (resp. the probabilistic analogue) using contour integration.

Sketch of the proof, concluded

Another arithmetic ingredient is needed:

First moment estimate (K.– Michel)

If $1/2 < \sigma_0$, then there exists $A > 0$ such that, uniformly for $\mathrm{Re}(s) \geq \sigma_0$, we have

$$\mathbf{E}_q(|L(f,s)|) \ll (1+|s|)^A.$$

Using this (resp. the easier analogue statement for the random Dirichlet series), one proves

$$\mathbf{E}_q\Bigl(\Bigl\|L(f,s) - \sum_n \varphi\Bigl(\frac{n}{N}\Bigr)\lambda_f(n)n^{-s}\Bigr\|_\infty\Bigr) \ll N^{-\delta}$$

for some $\delta > 0$ (resp. the probabilistic analogue) using contour integration.

The convergence in law then follows easily using the fact that it can be tested with Lipschitz functions $\mathcal{H}(\mathcal{C}) \to \mathbf{C}$.

Conclusion

Note that the limit is non-generic, and contains arithmetic information (since it is a Dirichlet series and an Euler product).

Conclusion

Note that the limit is non-generic, and contains arithmetic information (since it is a Dirichlet series and an Euler product).

As corollaries, one gets:

1. For suitable domains $\mathcal{C}$, "universality" theorems, by computing the support of the random limit (this is still an arithmetic problem);
2. Convergence in law of $L(f, s_0)$ for fixed s_0 with $1/2 < \mathrm{Re}(s_0) < 1$; in particular, the set of values $L(f, s_0)$ as f runs over the union of Ω_q is dense in $\mathbf{C}$.

Conclusion

Note that the limit is non-generic, and contains arithmetic information (since it is a Dirichlet series and an Euler product).

As corollaries, one gets:

1. For suitable domains $\mathcal{C}$, "universality" theorems, by computing the support of the random limit (this is still an arithmetic problem);
2. Convergence in law of $L(f, s_0)$ for fixed s_0 with $1/2 < \mathrm{Re}(s_0) < 1$; in particular, the set of values $L(f, s_0)$ as f runs over the union of Ω_q is dense in $\mathbf{C}$.

This proof is robust and extends formally to any family of L-functions satisfying:

1. Some local spectral equidistribution, which dictates what the limit is; this is known in great generality.
2. A first moment estimate; this is much more restrictive.

Part II: The shape of exponential sums

Let p be a prime number. For $(a, b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$, define

$$K(a, b; p) = \sum_{x \in \mathbf{F}_p^\times} e\Big(\frac{ax + b\bar{x}}{p}\Big),$$

where $e(z) = e^{2i\pi z}$, and $\bar{x}$ is the inverse of x modulo p.

Part II: The shape of exponential sums

Let p be a prime number. For $(a,b)\in\mathbf{F}_p^\times\times\mathbf{F}_p^\times$, define

$$K(a,b;p)=\sum_{x\in\mathbf{F}_p^\times} e\Big(\frac{ax+b\bar{x}}{p}\Big),$$

where $e(z)=e^{2i\pi z}$, and $\bar{x}$ is the inverse of x modulo p.

These are the classical *Kloosterman sums*; they are among the most important examples of exponential sums over finite fields and appear in many parts of analytic number theory (modular forms, diophantine problems, arithmetic functions in arithmetic progressions, etc.)

The shape of exponential sums

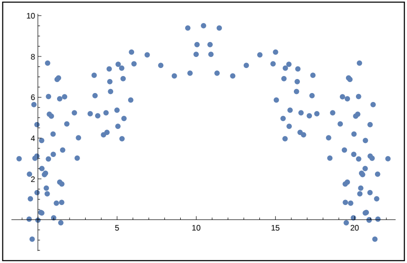
We play the following game.

The shape of exponential sums

We play the following game. Given a prime p and parameters $(a, b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$, plot in the complex plane the successive *partial sums*

$$\sum_{1 \le x \le j} e\Big(\frac{ax + b\bar{x}}{p}\Big)$$

for $0 \le j \le p - 1$,

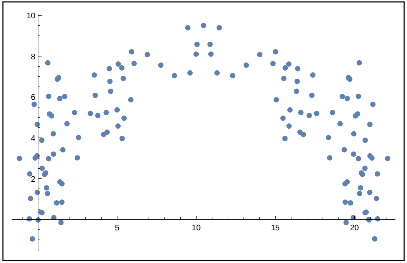


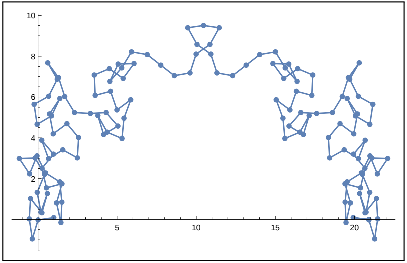
The shape of exponential sums

We play the following game. Given a prime p and parameters $(a, b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$, plot in the complex plane the successive *partial sums*

$$\sum_{1 \leq x \leq j} e\Big(\frac{ax + b\bar{x}}{p}\Big)$$

for $0 \leq j \leq p - 1$, and join these points by line segments, to obtain a polygonal curve in the plane.





What kinds of curves do we obtain when a and b vary?

Normalization

Weil proved that for all primes p and $(a, b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$, we have

$$|K(a, b; p)| \leq 2\sqrt{p}.$$

("square-root cancellation philosophy").

Normalization

Weil proved that for all primes p and $(a, b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$, we have

$$|K(a, b; p)| \leq 2\sqrt{p}.$$

("square-root cancellation philosophy").

So the summands

$$e\Big(\frac{ax + b\bar{x}}{p}\Big)$$

of the Kloosterman sums behave extremely randomly as x varies over $\mathbf{F}_p^\times$,

Normalization

Weil proved that for all primes p and $(a, b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$, we have

$$|K(a, b; p)| \leq 2\sqrt{p}.$$

("square-root cancellation philosophy").

So the summands

$$e\Big(\frac{ax + b\bar{x}}{p}\Big)$$

of the Kloosterman sums behave extremely randomly as x varies over $\mathbf{F}_p^\times$, but the randomness is quite subtle since

$$\frac{1}{\sqrt{p}} K(a, b; p)$$

always lies in $[-2, 2]$, instead of being (rarely) unbounded, as the Central Limit Theorem might naively suggest.

Kloosterman paths as random variables

For p prime and $(a, b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$, let

$$\mathcal{K}\ell_p(a,b) \,:\, [0,1] \longrightarrow \mathbf{C}$$

be the continuous function obtained by linear interpolation between the normalized partial sums

$$\frac{1}{\sqrt{p}} \sum_{1 \leq x \leq j} e\Big(\frac{ax + b\bar{x}}{p}\Big).$$

Kloosterman paths as random variables

For p prime and $(a, b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$, let

$$\mathcal{K}\ell_p(a, b) \,:\, [0, 1] \longrightarrow \mathbf{C}$$

be the continuous function obtained by linear interpolation between the normalized partial sums

$$\frac{1}{\sqrt{p}} \sum_{1 \leq x \leq j} e\Big(\frac{ax + b\bar{x}}{p}\Big).$$

So the path $t \mapsto \mathcal{K}\ell_p(a, b)(t)$ is the (rescaled) polygonal curve described above.

Kloosterman paths as random variables

For p prime and $(a, b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$, let

$$\mathcal{K}\ell_p(a, b) \,:\, [0, 1] \longrightarrow \mathbf{C}$$

be the continuous function obtained by linear interpolation between the normalized partial sums

$$\frac{1}{\sqrt{p}} \sum_{1 \leq x \leq j} e\Big(\frac{ax + b\bar{x}}{p}\Big).$$

So the path $t \mapsto \mathcal{K}\ell_p(a, b)(t)$ is the (rescaled) polygonal curve described above.

We consider, as $p \to +\infty$, the distribution properties of these functions in the space $C([0, 1])$ of continuous functions on $[0, 1]$, or in other words the limit of the sequence of $C([0, 1])$-valued random variables $\mathcal{K}\ell_p$ defined on the probability space $\Omega_p = \mathbf{F}_p^\times \times \mathbf{F}_p^\times$, with uniform probability measure.

The functional limit theorem

The shape of Kloosterman paths [K.–Sawin]

As $p \to +\infty$, the sequence of random functions $(\mathcal{K}\ell_p)_p$ converges in law to a $C([0,1])$-valued random variable V. This limit is the random Fourier series

$$V(t) = \sum_{h \in \mathbf{Z}} \frac{e(ht) - 1}{2i\pi h} \mathrm{ST}_h,$$

where $(\mathrm{ST}_h)_{h \in \mathbf{Z}}$ are independent random variables, all Sato-Tate distributed, and the term $h = 0$ should be interpreted as $t\mathrm{ST}_0$.

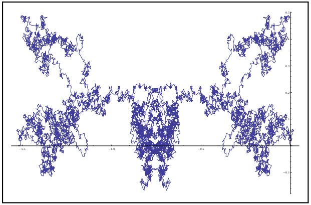
The functional limit theorem

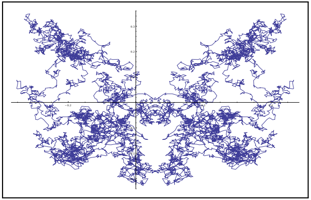
The shape of Kloosterman paths [K.–Sawin]

As $p \to +\infty$, the sequence of random functions $(\mathcal{K}\ell_p)_p$ converges in law to a $C([0,1])$-valued random variable V. This limit is the random Fourier series

$$V(t) = \sum_{h \in \mathbf{Z}} \frac{e(ht) - 1}{2i\pi h} \mathrm{ST}_h,$$

where $(\mathrm{ST}_h)_{h \in \mathbf{Z}}$ are independent random variables, all Sato-Tate distributed, and the term $h = 0$ should be interpreted as $t\mathrm{ST}_0$.





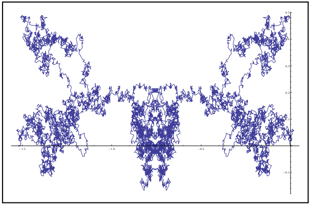
The functional limit theorem

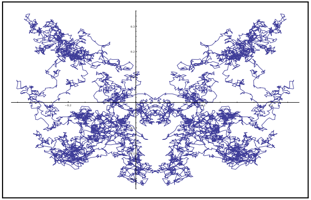
The shape of Kloosterman paths [K.–Sawin]

As $p \to +\infty$, the sequence of random functions $(\mathcal{K}\ell_p)_p$ converges in law to a $C([0,1])$-valued random variable V. This limit is the random Fourier series

$$V(t) = \sum_{h \in \mathbf{Z}} \frac{e(ht) - 1}{2i\pi h} \mathrm{ST}_h,$$

where $(\mathrm{ST}_h)_{h \in \mathbf{Z}}$ are independent random variables, all Sato-Tate distributed, and the term $h = 0$ should be interpreted as $t\mathrm{ST}_0$.





Note that the limit here is non-generic, but not "arithmetic".

Sketch of the proof

Recall that the Sato-Tate measure is the measure supported on $[-2, 2]$ given by

$$\mu_{ST} = \frac{1}{\pi}\sqrt{1 - x^2/4}.$$

Sketch of the proof

Recall that the Sato-Tate measure is the measure supported on $[-2, 2]$ given by

$$\mu_{ST} = \frac{1}{\pi}\sqrt{1 - x^2/4}.$$

It is also the direct image of the Haar measure on $\mathrm{SU}_2(\mathbf{C})$ under the trace. It appears here primarily because Weil's proof proceeds by showing that there exists $\Theta_p(a, b) \in \mathrm{SU}_2(\mathbf{C})^\sharp$ such that

$$\frac{1}{\sqrt{p}} \sum_{x \in \mathbf{F}_p^\times} e\Big(\frac{ax + b\bar{x}}{p}\Big) = \mathrm{Tr}(\Theta_p(a, b)).$$

Sketch of the proof

Recall that the Sato-Tate measure is the measure supported on $[-2, 2]$ given by

$$\mu_{ST} = \frac{1}{\pi}\sqrt{1 - x^2/4}.$$

It is also the direct image of the Haar measure on $\mathrm{SU}_2(\mathbf{C})$ under the trace. It appears here primarily because Weil's proof proceeds by showing that there exists $\Theta_p(a, b) \in \mathrm{SU}_2(\mathbf{C})^\sharp$ such that

$$\frac{1}{\sqrt{p}} \sum_{x \in \mathbf{F}_p^\times} e\Big(\frac{ax + b\bar{x}}{p}\Big) = \mathrm{Tr}(\Theta_p(a, b)).$$

Averate Sato-Tate equidistribution [Katz]

For $p \to +\infty$, the conjugacy classes $\Theta_p(a, b)$ are equidistributed in $\mathrm{SU}_2(\mathbf{C})^\sharp$, hence the normalized Kloosterman sums become equidistributed with respect to the Sato-Tate measure.

Heuristic argument

We make a discrete Fourier expansion of a partial sum:

$$\frac{1}{\sqrt{p}} \sum_{1 \le x \le (p-1)t} e\Big(\frac{ax + b\bar{x}}{p}\Big)$$

Heuristic argument

We make a discrete Fourier expansion of a partial sum:

$$\frac{1}{\sqrt{p}} \sum_{1\leq x\leq (p-1)t} e\Big(\frac{ax+b\bar{x}}{p}\Big) = \frac{1}{\sqrt{p}} \sum_{x\in \mathbf{F}_p} \Big(\sum_{h\in \mathbf{F}_p} \alpha_p(h;t) e\Big(-\frac{hx}{p}\Big)\Big) e\Big(\frac{ax+b\bar{x}}{p}\Big)$$

where

$$\alpha_p(h;t) = \frac{1}{p} \sum_{1\leq x\leq (p-1)t} e\Big(\frac{hx}{p}\Big).$$

Heuristic argument

We make a discrete Fourier expansion of a partial sum:

$$\frac{1}{\sqrt{p}} \sum_{1\leq x\leq (p-1)t} e\Big(\frac{ax+b\bar{x}}{p}\Big) = \frac{1}{\sqrt{p}} \sum_{x\in \mathbf{F}_p} \Big(\sum_{h\in \mathbf{F}_p} \alpha_p(h;t) e\Big(-\frac{hx}{p}\Big)\Big) e\Big(\frac{ax+b\bar{x}}{p}\Big)$$
$$= \sum_{|h|<p/2} \alpha_p(h,t) \mathrm{Kl}(a-h,b;p)$$

where

$$\alpha_p(h;t) = \frac{1}{p} \sum_{1\leq x\leq (p-1)t} e\Big(\frac{hx}{p}\Big).$$

Heuristic argument

On one side we have

$$\sum_{h\in\mathbf{Z}}\beta_p(h,t)\mathrm{ST}_h$$

On the other side we have

$$\sum_{|h|<p/2}\alpha_p(h,t)\mathrm{Kl}(a-h,b;p)$$

Heuristic argument

On one side we have

$$\sum_{h\in\mathbf{Z}} \beta_p(h,t)\mathrm{ST}_h$$

with

$$\beta_p(h,t) = \frac{e(ht)-1}{2i\pi h},$$

On the other side we have

$$\sum_{|h|<p/2} \alpha_p(h,t)\mathrm{Kl}(a-h,b;p)$$

where

$$\alpha_p(h;t) \to \int_0^t e(hx)dx = \frac{e(ht)-1}{2i\pi h},$$

Heuristic argument

On one side we have

$$\sum_{h\in\mathbf{Z}} \beta_p(h,t)\mathrm{ST}_h$$

with

$$\beta_p(h,t) = \frac{e(ht)-1}{2i\pi h},$$

and each ST_h is μ_{ST}-distributed.

On the other side we have

$$\sum_{|h|<p/2} \alpha_p(h,t)\mathrm{Kl}(a-h,b;p)$$

where

$$\alpha_p(h;t) \to \int_0^t e(hx)dx = \frac{e(ht)-1}{2i\pi h},$$

and for each h, the sums $\mathrm{Kl}(a-h,b;p)$ become μ_{ST}-equidistributed.

Heuristic argument

The summands (ST_h) in the random Fourier series are also independent. So the analogy becomes very clear from the following generalization of Katz's result:

Shifted equidistribution

For any $k \geq 1$, and any k-tuple $\boldsymbol{h} \in (\mathbf{F}_p^\times)^k$ with distinct coordinates, the k-tuples

$$(\mathrm{Kl}(a - h_1, b; p), \ldots, \mathrm{Kl}(a - h_k, b; p))$$

for $(a, b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$ become equidistributed in $[-2, 2]^k$ with respect to $\mu_{ST}^{\otimes k}$.

Heuristic argument

The summands (ST_h) in the random Fourier series are also independent. So the analogy becomes very clear from the following generalization of Katz's result:

Shifted equidistribution

For any $k \geq 1$, and any k-tuple $\boldsymbol{h} \in (\mathbf{F}_p^\times)^k$ with distinct coordinates, the k-tuples

$$(\mathrm{Kl}(a - h_1, b; p), \ldots, \mathrm{Kl}(a - h_k, b; p))$$

for $(a, b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$ become equidistributed in $[-2, 2]^k$ with respect to $\mu_{ST}^{\otimes k}$.

This is proved by generalizing Katz's argument, and relies essentially on the deepest form of Deligne's Riemann Hypothesis over finite fields.

Implementing the proof

To transform this heuristic into a proof, we use a standard strategy in probability. There are two separate parts:

Implementing the proof

To transform this heuristic into a proof, we use a standard strategy in probability. There are two separate parts:

Step 1 (Convergence of finite distributions). For any $k \geq 1$, and any real numbers

$$0 \leq t_1 < t_2 < \cdots < t_k \leq 1,$$

the random vectors

$$(a, b) \mapsto (\mathcal{K}\ell_p(a, b)(t_1), \ldots, \mathcal{K}\ell_p(a, b)(t_k))$$

converge in law to $(V(t_1), \ldots, V(t_k))$ as $p \to +\infty$.

Implementing the proof

To transform this heuristic into a proof, we use a standard strategy in probability. There are two separate parts:

Step 1 (Convergence of finite distributions). For any $k \geq 1$, and any real numbers

$$0 \leq t_1 < t_2 < \cdots < t_k \leq 1,$$

the random vectors

$$(a, b) \mapsto (\mathcal{K}\ell_p(a, b)(t_1), \ldots, \mathcal{K}\ell_p(a, b)(t_k))$$

converge in law to $(V(t_1), \ldots, V(t_k))$ as $p \to +\infty$.

This is proved essentially by elaborating the heuristic argument above (or by the method of moments).

Tightness

Step 2 (Tightness). The sequence $(\mathcal{K}\ell_p)_p$ of $C([0,1)$-valued random variables is tight.

Tightness

Step 2 (Tightness). The sequence $(\mathcal{K}\ell_p)_p$ of $C([0,1)$-valued random variables is tight.

We use Kolmogorov's Criterion: it is enough to prove the existence of constants

$$C \geq 0, \quad \alpha > 0, \quad \delta > 0,$$

such that for any $0 \leq s \leq t \leq 1$, we have

$$\frac{1}{(p-1)^2} \sum_{(a,b)\in \mathbf{F}_p^\times \times \mathbf{F}_p^\times} \Big| \mathcal{K}\ell_p(a,b)(t) - \mathcal{K}\ell_p(a,b)(s) \Big|^\alpha \leq C|t-s|^{1+\delta}.$$

Tightness

Step 2 (Tightness). The sequence $(\mathcal{K}\ell_p)_p$ of $C([0,1)$-valued random variables is tight.

We use Kolmogorov's Criterion: it is enough to prove the existence of constants

$$C \geq 0, \quad \alpha > 0, \quad \delta > 0,$$

such that for any $0 \leq s \leq t \leq 1$, we have

$$\frac{1}{(p-1)^2} \sum_{(a,b)\in \mathbf{F}_p^\times \times \mathbf{F}_p^\times} \Big|\mathcal{K}\ell_p(a,b)(t) - \mathcal{K}\ell_p(a,b)(s)\Big|^\alpha \leq C|t-s|^{1+\delta}.$$

We write $|t-s| = p^{-\gamma}$ where $\gamma \geq 0$. Depending on γ, we use different tools (linear interpolation, trivial bounds, Kloosterman's fourth moment method).

Tightness

Step 2 (Tightness). The sequence $(\mathcal{K}\ell_p)_p$ of $C([0,1)$-valued random variables is tight.

We use Kolmogorov's Criterion: it is enough to prove the existence of constants

$$C \geq 0, \quad \alpha > 0, \quad \delta > 0,$$

such that for any $0 \leq s \leq t \leq 1$, we have

$$\frac{1}{(p-1)^2} \sum_{(a,b)\in \mathbf{F}_p^\times \times \mathbf{F}_p^\times} \Big|\mathcal{K}\ell_p(a,b)(t) - \mathcal{K}\ell_p(a,b)(s)\Big|^\alpha \leq C|t-s|^{1+\delta}.$$

We write $|t-s| = p^{-\gamma}$ where $\gamma \geq 0$. Depending on γ, we use different tools (linear interpolation, trivial bounds, Kloosterman's fourth moment method). The critical range is when γ is close to $1/2$; this is a very "non-generic" range.

A first application

Composing with the (continuous!) norm map $T(\varphi) = \|\varphi\|_\infty$ on $C([0,1])$, we deduce that there exists a limiting probability distribution ν for

$$\|\mathcal{K}\ell_p(a,b)\|_\infty = \max_{1\leq j\leq p-1} \frac{1}{\sqrt{p}}\Big|\sum_{1\leq x\leq j} e\Big(\frac{ax+b\bar{x}}{p}\Big)\Big|.$$

A first application

Composing with the (continuous!) norm map $T(\varphi) = \|\varphi\|_\infty$ on $C([0,1])$, we deduce that there exists a limiting probability distribution ν for

$$\|\mathcal{K}\ell_p(a,b)\|_\infty = \max_{1\leq j\leq p-1} \frac{1}{\sqrt{p}}\Big|\sum_{1\leq x\leq j} e\Big(\frac{ax+b\bar{x}}{p}\Big)\Big|.$$

Using results of probability in Banach spaces (Talagrand, Montgomery-Smith), we prove tail bounds for ν: there exists $c > 0$ such that

$$c^{-1}\exp(-\exp(ct)) \leq \nu([t,+\infty[) \leq c\exp(-\exp(c^{-1}t))$$

A first application

Composing with the (continuous!) norm map $T(\varphi) = \|\varphi\|_\infty$ on $C([0,1])$, we deduce that there exists a limiting probability distribution ν for

$$\|\mathcal{K}\ell_p(a,b)\|_\infty = \max_{1\leq j\leq p-1} \frac{1}{\sqrt{p}}\Big|\sum_{1\leq x\leq j} e\Big(\frac{ax+b\bar{x}}{p}\Big)\Big|.$$

Using results of probability in Banach spaces (Talagrand, Montgomery-Smith), we prove tail bounds for ν: there exists $c>0$ such that

$$c^{-1}\exp(-\exp(ct)) \leq \nu([t,+\infty[) \leq c\exp(-\exp(c^{-1}t))$$

In particular, the partial sums

$$\frac{1}{\sqrt{p}}\sum_{1\leq x\leq j} e\Big(\frac{ax+b\bar{x}}{p}\Big)$$

are not bounded as (p,j,a,b) all vary with $1\leq j\leq p$, but "large" values are extremely rare.

Some similar results

1. The method extends to many exponential sums with “large” monodromy groups (instead of $\mathrm{SU}_2(\mathbf{C})$);

Some similar results

1. The method extends to many exponential sums with “large” monodromy groups (instead of $\mathrm{SU}_2(\mathbf{C})$);
2. Ricotta–Royer: similar result for Kloosterman sums modulo p^k, $k \geq 2$ fixed (different limiting series);

Some similar results

1. The method extends to many exponential sums with “large” monodromy groups (instead of $\mathrm{SU}_2(\mathbf{C})$);
2. Ricotta–Royer: similar result for Kloosterman sums modulo p^k, $k \geq 2$ fixed (different limiting series);
3. Bober, Goldmakher, Granville, Koukoulopoulos, Soundararajan: “classical” character sums
$$S_N(\chi) = \frac{1}{\sqrt{p}} \sum_{1 \leq N} \chi(n)$$
for $\chi \neq 1$ multiplicative character modulo p, with very different limiting random Fourier series, and a lot of work on tail bounds;

Some similar results

1. The method extends to many exponential sums with "large" monodromy groups (instead of $\mathrm{SU}_2(\mathbf{C})$);
2. Ricotta–Royer: similar result for Kloosterman sums modulo p^k, $k \geq 2$ fixed (different limiting series);
3. Bober, Goldmakher, Granville, Koukoulopoulos, Soundararajan: "classical" character sums
$$S_N(\chi) = \frac{1}{\sqrt{p}} \sum_{1 \leq N} \chi(n)$$
for $\chi \neq 1$ multiplicative character modulo p, with very different limiting random Fourier series, and a lot of work on tail bounds;
4. Jurkat and van Horne; Marklof, Akarsu, Cellarosi: quadratic Gauss sums
$$S_N(x) = \frac{1}{\sqrt{N}} \sum_{n \leq N} e(\tfrac{1}{2} n^2 x + n\alpha)$$
with arbitrary real coefficients (functional limit theorem, again very different limiting process).