6

The Shape of Exponential Sums

Probability tools	Arithmetic tools
Definition of convergence in law (§ B.3)	Kloosterman sums (§ C.6)
Kolmogorov's Theorem for random series (th. B.10.1)	Riemann Hypothesis over finite fields (th. C.6.4)
Convergence of finite distributions (def. B.11.2)	Average Sato–Tate Theorem
Kolmogorov's Criterion for tightness (prop. B.11.10)	Weyl criterion (§ B.6)
Fourier coefficients criterion (prop. B.11.8)	Deligne's Equidistribution Theorem
Sub-Gaussian random variables (§ B.8)	
Talagrand's inequality (th. B.11.12)	
Support of a random series (prop. B.10.8)	

6.1 Introduction

We consider in this chapter a rather different type of arithmetic objects: exponential sums and their partial sums. Although the ideas that we will present apply to very general situations, we consider as usual only an important special case: the partial sums of *Kloosterman sums* modulo primes. In Section C.6, we give some motivation for the type of sums (and questions) discussed in this chapter.

Thus let p be a prime number. For any pair (a, b) of invertible elements in the finite field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, the (normalized) Kloosterman sum $\mathrm{Kl}(a, b; p)$ is defined by the formula

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

$$\mathrm{Kl}(a,b;p) = \frac{1}{\sqrt{p}} \sum_{x \in \mathbf{F}_p^\times} e\left(\frac{ax + b\bar{x}}{p}\right),$$

where we recall that we denote by $e(z)$ the 1-periodic function defined by $e(z) = e^{2i\pi z}$, and that $\bar{x}$ is the inverse of x modulo p.

These are finite sums, and they are of great importance in many areas of number theory, especially in relation with automorphic and modular forms and with analytic number theory (see [66] for a survey of the origin of these sums and of their applications, due to Poincaré, Kloosterman, Linnik, Iwaniec, and others). Among their remarkable properties is the following estimate for the modulus of $\mathrm{Kl}(a,b;p)$, due to A. Weil: for any $(a,b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$, we have

$$|\mathrm{Kl}(a,b;p)| \leqslant 2. \tag{6.1}$$

This is a very strong result if one considers that $\mathrm{Kl}(a,b;p)$ is, up to dividing by $\sqrt{p}$, the sum of $p-1$ roots of unity, so that the "trivial" estimate is that $|\mathrm{Kl}(a,b;p)| \leqslant (p-1)/\sqrt{p}$. What this reveals is that the arguments of the summands $e((ax+b\bar{x})/p)$ in $\mathbf{C}$ vary in a very complicated manner that leads to this remarkable cancellation property. This is due essentially to the very "random" behavior of the map $x \mapsto \bar{x}$ when seen at the level of representatives of x and $\bar{x}$ in the interval $\{0,\dots,p-1\}$.

From a probabilistic point of view, the order of magnitude $\sqrt{p}$ of the sum (before normalization) is not unexpected. If we simply heuristically model an exponential sum as above by a random walk with independent summands uniformly distributed on the unit circle, say,

$$\mathrm{S_N} = \mathrm{X}_1 + \cdots + \mathrm{X_N},$$

where the random variables (X_n) are independent and uniform on the unit circle, then the Central Limit Theorem implies a convergence in law of $\mathrm{X_N}/\sqrt{\mathrm{N}}$ to a standard complex Gaussian random variable, which shows that $\sqrt{\mathrm{N}}$ is the "right" order of magnitude. Note however that probabilistic analogies of this type would also suggest that $\mathrm{S_N}$ is sometimes (although rarely) larger than $\sqrt{\mathrm{N}}$ (the law of the iterated logarithm suggests that it should almost surely reach values as large as $\sqrt{\mathrm{N}}(\log\log \mathrm{N})$; see, e.g., [9, Th. 9.5]). Hence Weil's bound (6.1) indicates that the summands defining the Kloosterman sum have very special properties.

This probabilistic analogy and the study of random walks (or sheer curiosity) suggests to look at the partial sums of Kloosterman sums, and the way they move in the complex plane. This requires some ordering of the sum defining

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

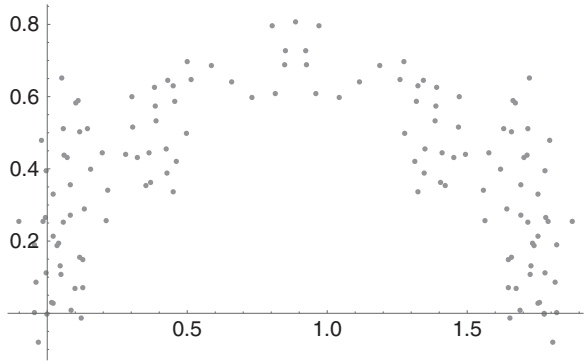

Figure 6.1 The partial sums of $\mathrm{Kl}(1,1;139)$.

$\mathrm{Kl}(a,b;p)$, which we simply achieve by summing over $1 \leqslant x \leqslant p-1$ in increasing order. Thus we will consider the $p-1$ points

$$z_j = \frac{1}{\sqrt{p}} \sum_{1 \leqslant x \leqslant j} e\left(\frac{ax + b\bar{x}}{p}\right)$$

for $1 \leqslant j \leqslant p-1$. We illustrate this for the sum $\mathrm{Kl}(1,1;139)$ in Figure 6.1.

Because this cloud of points is not particularly enlightening, we refine the construction by joining the successive points with line segments. This gives the result in Figure 6.2 for $\mathrm{Kl}(1,1;139)$. If we change the values of a and b, we observe that the figures change in apparently random and unpredictable way, although some basic features remain (the final point is on the real axis, which reflects the easily proven fact that $\mathrm{Kl}(a,b;p) \in \mathbf{R}$, and there is a reflection symmetry with respect to the line $x = \frac{1}{2}\mathrm{Kl}(a,b;p)$). For instance, Figure 6.3 shows the curves corresponding to $\mathrm{Kl}(2,1;139)$, $\mathrm{Kl}(3,1;139)$ and $\mathrm{Kl}(4,1;139)$; see [71] for many more pictures.

We then ask whether there is a definite statistical behavior for these *Kloosterman paths* as $p \to +\infty$, when we pick $(a,b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$ uniformly at random. As we will see, this is indeed the case!

To state the precise result, we introduce some further notation. Thus, for p prime and $(a,b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$, we denote by $\mathsf{K}_p(a,b)$ the function

$$[0,1] \longrightarrow \mathbf{C}$$

such that, for $0 \leqslant j \leqslant p-2$, the value at a real number t such that

$$\frac{j}{p-1} \leqslant t < \frac{j+1}{p-1}$$

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

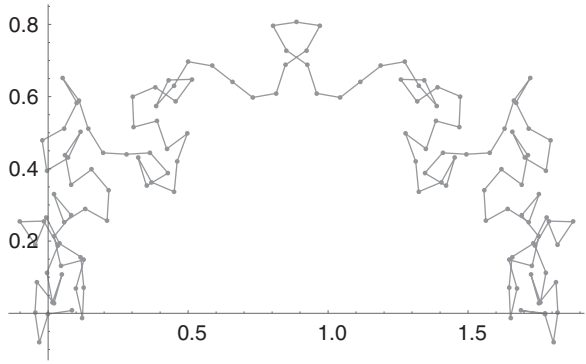

Figure 6.2 The partial sums of $\mathrm{Kl}(1,1;139)$, joined by line segments.

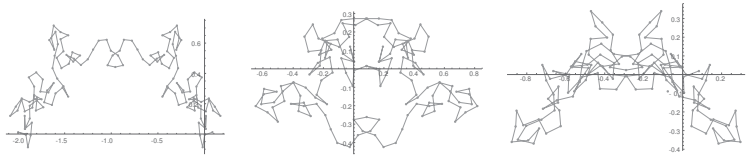

Figure 6.3 The partial sums of $\mathrm{Kl}(a,1;139)$ for $a = 2,3,4$.

is obtained by interpolating linearly between the consecutive partial sums

$$z_j = \frac{1}{\sqrt{p}} \sum_{1 \leqslant x \leqslant j} e\left(\frac{ax + b\bar{x}}{p}\right) \quad \text{and} \quad z_{j+1} = \frac{1}{\sqrt{p}} \sum_{1 \leqslant x \leqslant j+1} e\left(\frac{ax + b\bar{x}}{p}\right).$$

The path $t \mapsto \mathsf{K}_p(a,b)(t)$ is the polygonal path described above; for $t = 0$, we have $\mathsf{K}_p(a,b)(0) = 0$, and for $t = 1$, we obtain $\mathsf{K}_p(a,b)(1) = \mathrm{Kl}(a,b;p)$.

Let $\Omega_p = \mathbf{F}_p^\times \times \mathbf{F}_p^\times$. We view K_p as a random variable

$$\Omega_p \longrightarrow \mathrm{C}([0,1]),$$

where $\mathrm{C}([0,1])$ is the Banach space of continuous functions $\varphi\colon [0,1] \to \mathbf{C}$ with the supremum norm $\|\varphi\|_\infty = \sup |\varphi(t)|$. Alternatively, we may think of the *family* of random variables $(\mathsf{K}_p(t))_{t\in[0,1]}$ such that

$$(a,b) \mapsto \mathsf{K}_p(a,b)(t)$$

and view it as a "stochastic process" with t playing the role of "time."

Here is the theorem that gives the limiting behavior of these arithmetically defined random variables, proved by Kowalski and Sawin in [79].

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

Theorem 6.1.1 *Let* $(\mathrm{ST}_h)_{h\in\mathbf{Z}}$ *be a sequence of independent random variables, all distributed according to the Sato–Tate measure*

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

on $[-2,2]$.

(1) *The random Fourier series*

$$\mathrm{K}(t) = t\mathrm{ST}_0 + \sum_{\substack{h\in\mathbf{Z}\\ h\neq 0}} \frac{e(ht)-1}{2i\pi h}\mathrm{ST}_h$$

defined for $t\in[0,1]$ *converges uniformly almost surely, in the sense of symmetric partial sums*

$$\mathrm{K}(t) = t\mathrm{ST}_0 + \lim_{\mathrm{H}\to+\infty} \sum_{\substack{h\in\mathbf{Z}\\ 1\leqslant|h|<\mathrm{H}}} \frac{e(ht)-1}{2i\pi h}\mathrm{ST}_h.$$

This random Fourier series defines a $\mathrm{C}([0,1])$*-valued random variable* K.

(2) *As* $p\to+\infty$*, the random variables* K_p *converge in law to* K*, in the sense of* $\mathrm{C}([0,1])$*-valued variables.*

The Sato–Tate measure is better known in probability as a semi-circle law, but its appearance in Theorem 6.1.1 is really due to the group-theoretic interpretation that often arises in number theory, and reflects the choice of name. Namely, we recall (see Example B.6.1 (3)) that μ_{ST} is the direct image under the trace map of the probability Haar measure on the compact group $\mathrm{SU}_2(\mathbf{C})$.

Note in particular that the theorem implies, by taking $t=1$, that the Kloosterman sums $\mathrm{Kl}(a,b;p)=\mathsf{K}_p(a,b)(1)$, viewed as random variables on Ω_p, become asymptotically distributed like $\mathrm{K}(1)=\mathrm{ST}_0$, that is, that Kloosterman sums are Sato–Tate distributed in the sense that for any real numbers $-2\leqslant\alpha<\beta\leqslant 2$, we have

$$\frac{1}{(p-1)^2}|\{(a,b)\in\mathbf{F}_p^\times\times\mathbf{F}_p^\times \mid \alpha<\mathrm{Kl}(a,b;p)<\beta\}| \longrightarrow \int_\alpha^\beta d\mu_{\mathrm{ST}}(t).$$

This result is a famous theorem of N. Katz [61]. In some sense, Theorem 6.1.1 is a "functional" extension of this equidistribution theorem. In fact, the key arithmetic ingredient in the proof is an extension of the results and methods developed by Katz to prove many similar statements.

Remark 6.1.2 Although we do not require this, we mention a few regularity properties of the random series $\mathrm{K}(t)$: it is almost surely nowhere differentiable,

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

but almost surely Hölder-continuous of order α for any $\alpha < 1/2$ (see the references in [79, Prop. 2.1]; these follow from general results of Kahane).

6.2 Proof of the Distribution Theorem

We will explain the proof of the theorem. We use a slightly different approach than the original article, bypassing the method of moments, and exploiting some simplifications that arise from the consideration of this single example.

The proof will be complete from a probabilistic point of view, but it relies on an extremely deep arithmetic result that we will only be able to view as a black box in this book. The crucial underlying result is the very general form of the Riemann Hypothesis over finite fields, and the formalism that is attached to it. This is due to Deligne, and the particular application we use relies extensively on the additional work of Katz. All of this builds on the algebraic-geometric foundations of Grothendieck and his school (see [59, Ch. 11] for an introduction).

In outline, the proof has three steps:

- **Step 1**: Show that the random Fourier series K exists, as a $\mathrm{C}([0,1])$-valued random variable.
- **Step 2**: Prove that (a small variant of) the sequence of Fourier coefficients of K_p converges in law to the sequence of Fourier coefficients of K.
- **Step 3**: Prove that the sequence $(\mathsf{K}_p)_p$ is tight (Definition B.3.6), using Kolmogorov's Tightness Criterion (Proposition B.11.10).

Once this is done, a simple probabilistic statement (Proposition B.11.8, which is a variant of Prokhorov's Theorem, B.11.4) shows that the combination of (2) and (3) implies that K_p converges to K. Both steps (2) and (3) involve nontrivial arithmetic information; indeed, the main input in (2) is exceptionally deep, as we will explain soon.

We denote by $\mathbf{P}_p$ and $\mathbf{E}_p$ the probability and expectation with respect to the uniform measure on $\Omega_p = \mathbf{F}_p^\times \times \mathbf{F}_p^\times$. Before we begin the proof in earnest, it is useful to see *why* the limit arises, and why it is precisely this random Fourier series. The idea is to use discrete Fourier analysis to represent the partial sums of Kloosterman sums.

Lemma 6.2.1 *Let $p \geqslant 3$ be a prime and $a, b \in \mathbf{F}_p^\times$. Let $t \in [0,1]$. Then we have*

$$\frac{1}{\sqrt{p}} \sum_{1 \leqslant n \leqslant (p-1)t} e\left(\frac{an + b\bar{n}}{p}\right) = \sum_{|h|<p/2} \alpha_p(h,t)\,\mathrm{Kl}(a-h,b;p), \qquad (6.2)$$

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

where

$$\alpha_p(h,t) = \frac{1}{p} \sum_{1 \leqslant n \leqslant (p-1)t} e\left(\frac{nh}{p}\right).$$

Proof This is a case of the discrete Plancherel formula, applied to the characteristic (indicator) function of the discrete interval of summation; to check it quickly, insert the definitions of $\alpha_p(h,t)$ and of $\mathrm{Kl}(a-h,b;p)$ in the right-hand side of (6.2). This shows that it is equal to

$$\begin{aligned}
&\sum_{|h|<p/2} \alpha_p(h,t)\,\mathrm{Kl}(a-h,b;p) \\
&= \frac{1}{p^{3/2}} \sum_{|h|<p/2} \sum_{1 \leqslant n \leqslant (p-1)t} \sum_{m \in \mathbf{F}_p} e\left(\frac{nh}{p}\right) e\left(\frac{(a-h)m + b\bar{m}}{p}\right) \\
&= \frac{1}{\sqrt{p}} \sum_{1 \leqslant n \leqslant (p-1)t} \sum_{m \in \mathbf{F}_p} e\left(\frac{am + b\bar{m}}{p}\right) \frac{1}{p} \sum_{h \in \mathbf{F}_p} e\left(\frac{h(n-m)}{p}\right) \\
&= \frac{1}{\sqrt{p}} \sum_{1 \leqslant n \leqslant (p-1)t} e\left(\frac{an + b\bar{n}}{p}\right),
\end{aligned}$$

as claimed, since by the orthogonality of characters we have

$$\frac{1}{p} \sum_{h \in \mathbf{F}_p} e\left(\frac{h(n-m)}{p}\right) = \delta(n,m)$$

for any n, $m \in \mathbf{F}_p$, where $\delta(n,m) = 1$ if $n = m$ modulo p, and otherwise $\delta(n,m) = 0$. □

If we observe that $\alpha_p(h,t)$ is essentially a Riemann sum for the integral

$$\int_0^t e(ht)dt = \frac{e(ht)-1}{2i\pi h}$$

for all $h \neq 0$, and that $\alpha_p(0,t) \to t$ as $p \to +\infty$, we see that the right-hand side of (6.2) looks like a Fourier series of the same type as $\mathrm{K}(t)$, with coefficients given by shifted Kloosterman sums $\mathrm{Kl}(a-h,b;p)$ instead of ST_h. Now the crucial arithmetic information is contained in the following very deep theorem:

Theorem 6.2.2 (Katz; Deligne) *Fix an integer $b \neq 0$. For p prime not dividing b, consider the random variable*

$$\mathsf{S}_p : a \mapsto (\mathrm{Kl}(a-h,b;p))_{h \in \mathbf{Z}}$$

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

on $\mathbf{F}_p^\times$ *with uniform probability measure, taking values in the compact topological space*

$$\hat{\mathrm{T}} = \prod_{h\in\mathbf{Z}} [-2,2].$$

Then S_p *converges in law to the product probability measure*

$$\bigotimes_{h\in\mathbf{Z}} \mu_{\mathrm{ST}}.$$

In other words, the sequence of random variables $a \mapsto \mathrm{Kl}(a-h,b;p)$ *converges in law to a sequence* $(\mathrm{ST}_h)_{h\in\mathbf{Z}}$ *of independent Sato–Tate distributed random variables.*

Because of this theorem, the formula (6.2) suggests that $\mathsf{K}_p(t)$ converges in law to the random series

$$t\mathrm{ST}_0 + \sum_{\substack{h\in\mathbf{Z}\\ h\neq 0}} \frac{e(ht)-1}{2i\pi h}\mathrm{ST}_h,$$

which is exactly $\mathrm{K}(t)$. We now proceed to the implementation of the three steps above, which will use this deep arithmetic ingredient.

Remark 6.2.3 There is a subtlety in the argument: although Theorem 6.2.2 holds for any fixed b, when averaging only over a, we cannot at the current time prove the analogue of Theorem 6.1.1 for fixed b, because the proof of tightness in the last step uses crucially both averages.

Step 1. (Existence and properties of the random Fourier series)
We can write the series $\mathrm{K}(t)$ as

$$\mathrm{K}(t) = t\mathrm{ST}_0 + \sum_{h\geqslant 1}\left(\frac{e(ht)-1}{2i\pi h}\mathrm{ST}_h - \frac{e(-ht)-1}{2i\pi h}\mathrm{ST}_{-h}\right).$$

The summands here, namely,

$$\mathrm{X}_h = \frac{e(ht)-1}{2i\pi h}\mathrm{ST}_h - \frac{e(-ht)-1}{2i\pi h}\mathrm{ST}_{-h}$$

for $h\geqslant 1$, are independent and have expectation 0 since $\mathbf{E}(\mathrm{ST}_h)=0$ (see (B.8)). Furthermore, since ST_h is independent of ST_{-h}, and they have variance 1, we have

$$\sum_{h\geqslant 1}\mathbf{V}(\mathrm{X}_h) = \sum_{h\geqslant 1}\left(\left|\frac{e(ht)-1}{2i\pi h}\right|^2 + \left|\frac{e(-ht)-1}{2i\pi h}\right|^2\right) \leqslant \sum_{h\geqslant 1}\frac{1}{h^2} < +\infty$$

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

for any $t \in [0,1]$. From Kolmogorov's criterion for almost sure convergence of random series with finite variance (Theorem B.10.1), it follows that for any $t \in [0,1]$, the series $\mathrm{K}(t)$ converges almost surely and in L^2 to a complex-valued random variable.

To prove convergence in $\mathrm{C}([0,1])$, we will use convergence of finite distributions combined with Kolmogorov's Tightness Criterion. Consider the partial sums

$$\mathrm{K}_{\mathrm{H}}(t) = t\mathrm{ST}_0 + \sum_{1\leqslant|h|\leqslant \mathrm{H}} \frac{e(ht)-1}{2i\pi h}\mathrm{ST}_h$$

for $\mathrm{H} \geqslant 1$. These are $\mathrm{C}([0,1])$-valued random variables. The convergence of $\mathrm{K}_{\mathrm{H}}(t)$ to $\mathrm{K}(t)$ in L^1, for any $t \in [0,1]$, implies (see Lemma B.11.3) that the sequence $(\mathrm{K}_{\mathrm{H}})_{\mathrm{H}\geqslant 1}$ converges to K in the sense of finite distributions. Therefore, by Proposition B.11.10, the sequence converges in the sense of $\mathrm{C}([0,1])$-valued random variables if there exist constants $\mathrm{C} \geqslant 0$, $\alpha > 0$ and $\delta > 0$ such that for any $\mathrm{H} \geqslant 1$, and real numbers $0 \leqslant s < t \leqslant 1$, we have

$$\mathbf{E}(|\mathrm{K}_{\mathrm{H}}(t) - \mathrm{K}_{\mathrm{H}}(s)|^{\alpha}) \leqslant \mathrm{C}|t-s|^{1+\delta}. \tag{6.3}$$

We will take $\alpha = 4$. We have

$$\mathrm{K}_{\mathrm{H}}(t) - \mathrm{K}_{\mathrm{H}}(s) = (t-s)\mathrm{ST}_0 + \sum_{1\leqslant|h|\leqslant \mathrm{H}} \frac{e(ht)-e(hs)}{2i\pi h}\mathrm{ST}_h.$$

This is a sum of independent, centered and bounded random variables, so that by Proposition B.8.2 (1) and (2), it is σ_{H}^2-sub-Gaussian with

$$\sigma_{\mathrm{H}}^2 = |t-s|^2 + \sum_{1\leqslant|h|\leqslant \mathrm{H}} \left|\frac{e(ht)-e(hs)}{2i\pi h}\right|^2 \leqslant |t-s|^2 + \sum_{h\neq 0} \left|\frac{e(ht)-e(hs)}{2i\pi h}\right|^2.$$

By Parseval's formula for ordinary Fourier series, we have

$$|t-s|^2 + \sum_{h\neq 0} \left|\frac{e(ht)-e(hs)}{2i\pi h}\right|^2 = \int_0^1 |\varphi_{s,t}(x)|^2 dx,$$

where $\varphi_{s,t}$ is the characteristic function of the interval $[s,t]$. Therefore $\sigma_{\mathrm{H}}^2 \leqslant |t-s|$. By the properties of sub-Gaussian random variables (see Proposition B.8.3 in Section B.8), we deduce that there exists $\mathrm{C} \geqslant 0$ such that

$$\mathbf{E}(|\mathrm{K}_{\mathrm{H}}(t) - \mathrm{K}_{\mathrm{H}}(s)|^4) \leqslant \mathrm{C}\sigma_{\mathrm{H}}^4 \leqslant \mathrm{C}|t-s|^2,$$

which establishes (6.3).

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

Step 2. (Computation of Fourier coefficients)

As in Section B.11, we will denote by $C_0([0,1])$ the subspace of functions $f \in C([0,1])$ such that $f(0) = 0$. For $f \in C_0([0,1])$, the sequence $FT(f) = (\widetilde{f}(h))_{h\in\mathbf{Z}}$ is defined by $\widetilde{f}(0) = f(1)$ and

$$\widetilde{f}(h) = \int_0^1 (f(t) - tf(1))e(-ht)dt$$

for $h \neq 0$. The map FT is a continuous linear map from $C_0([0,1])$ to $C_0(\mathbf{Z})$, the Banach space of functions $\mathbf{Z} \to \mathbf{C}$ that tend to zero at infinity.

Lemma 6.2.4 *The "Fourier coefficients"* $FT(\mathsf{K}_p)$ *converge in law to* $FT(K)$*, in the sense of convergence of finite distribution.*

We begin by computing the Fourier coefficients of a polygonal path. Let z_0 and z_1 be complex numbers, and $t_0 < t_1$ real numbers. We define $\Delta = t_1 - t_0$ and $f \in C([0,1])$ by

$$f(t) = \begin{cases} \frac{1}{\Delta}(z_1(t - t_0) + z_0(t_1 - t)) & \text{if } t_0 \leqslant t \leqslant t_1, \\ 0 & \text{otherwise,} \end{cases}$$

which parameterizes the segment from z_0 to z_1 over the interval $[t_0, t_1]$.

Let $h \neq 0$ be an integer. By direct computation, we find

$$\begin{aligned} \int_0^1 f(t)e(-ht)dt &= -\frac{1}{2i\pi h}(z_1e(-ht_1) - z_0e(-ht_0)) \\ &\quad + \frac{1}{2i\pi h}(z_1 - z_0)e(-ht_0)\frac{1}{\Delta}\left(\int_0^\Delta e(-hu)du\right) \\ &= -\frac{1}{2i\pi h}(z_1e(-ht_1) - z_0e(-ht_0)) \\ &\quad + \frac{1}{2i\pi h}(z_1 - z_0)\frac{\sin(\pi h\Delta)}{\pi h\Delta}e\left(-h\left(t_0 + \frac{\Delta}{2}\right)\right). \quad (6.4) \end{aligned}$$

Consider now an integer $n \geqslant 1$ and a family $(z_0, \ldots, z_n)$ of complex numbers. For $0 \leqslant j \leqslant n-1$, let f_j be the function as above relative to the points (z_j, z_{j+1}) and the interval $[j/n, (j+1)/n]$, and define

$$f = \sum_{j=0}^{n-1} f_j$$

so that f parameterizes the polygonal path joining z_0 to z_1 to … to z_n, each over time intervals of equal length $1/n$.

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

For $h \neq 0$, we obtain by summing (6.4), using a telescoping sum and the relations $z_0 = f(0)$, $z_n = f(1)$, the formula

$$\int_0^1 f(t)e(-ht)dt = -\frac{1}{2i\pi h}(f(1) - f(0)) + \frac{1}{2i\pi h}\frac{\sin(\pi h/n)}{\pi h/n}\sum_{j=0}^{n-1}(z_{j+1} - z_j)e\left(-\frac{h(j+\frac{1}{2})}{n}\right). \tag{6.5}$$

We specialize this general formula to Kloosterman paths. Let p be a prime, $(a,b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times$, and apply the formula above to $n = p-1$ and the points

$$z_j = \frac{1}{\sqrt{p}}\sum_{1\leqslant x\leqslant j} e\left(\frac{ax+b\bar{x}}{p}\right), \qquad 0 \leqslant j \leqslant p-1.$$

For $h \neq 0$, the hth Fourier coefficient of $\mathrm{K}_p - t\mathrm{K}_p(1)$ is the random variable on Ω_p that maps (a,b) to

$$\frac{1}{2i\pi h}\frac{\sin(\pi h/(p-1))}{\pi h/(p-1)}e\left(-\frac{h}{2(p-1)}\right)\frac{1}{\sqrt{p}}\sum_{x=1}^{p-1} e\left(\frac{ax+b\bar{x}}{p}\right)e\left(-\frac{hx}{p-1}\right).$$

Note that for fixed h, we have

$$e\left(-\frac{hx}{p-1}\right) = e\left(-\frac{hx}{p}\right)e\left(-\frac{hx}{p(p-1)}\right) = e\left(-\frac{hx}{p}\right)(1+\mathrm{O}(p^{-1}))$$

for all p and all x such that $1 \leqslant x \leqslant p-1$, hence

$$\frac{1}{\sqrt{p}}\sum_{x=1}^{p-1} e\left(\frac{ax+b\bar{x}}{p}\right)e\left(-\frac{hx}{p-1}\right) = \mathrm{Kl}(a-h,b;p) + \mathrm{O}\left(\frac{1}{\sqrt{p}}\right),$$

where the implied constant depends on h. Let

$$\beta_p(h) = \frac{\sin(\pi h/(p-1))}{\pi h/(p-1)}e\left(-\frac{h}{2(p-1)}\right).$$

Note that $|\beta_p(h)| \leqslant 1$, so we can express the hth Fourier coefficient as

$$\frac{1}{2i\pi h}\,\mathrm{Kl}(a-h,b;p)\beta_p(h) + \mathrm{O}(p^{-1/2}),$$

where the implied constant depends on h.

Note further that the 0th component of $\mathrm{FT}(\mathsf{K}_p)$ is $\mathrm{Kl}(a,b;p)$. Since $\beta_p(h) \to 1$ as $p \to +\infty$ for each fixed h, we deduce from Katz's equidistribution theorem (Theorem 6.2.2) and from Lemma B.4.3 (applied to the vectors of

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

Fourier coefficients at $h_1, \dots, h_m$ for arbitrary $m \geqslant 1$) that $\mathrm{FT}(\mathsf{K}_p)$ converges in law to $\mathrm{FT}(\mathrm{K})$ in the sense of finite distributions.

Step 3. (Tightness of the Kloosterman paths)

We now come to the second main step of the proof of Theorem 6.1.1: the fact that the sequence $(\mathsf{K}_p)_p$ is tight. According to Kolmogorov's Criterion (Proposition B.11.10), it is enough to find constants $\mathrm{C} \geqslant 0$, $\alpha > 0$ and $\delta > 0$ such that, for all primes $p \geqslant 3$ and all t and s with $0 \leqslant s < t \leqslant 1$, we have

$$\mathbf{E}_p(|\mathsf{K}_p(t) - \mathsf{K}_p(s)|^\alpha) \leqslant \mathrm{C}|t-s|^{1+\delta}. \tag{6.6}$$

We denote by $\gamma \geqslant 0$ the real number such that

$$|t-s| = (p-1)^{-\gamma}.$$

So γ is larger when t and s are closer. The proof of (6.6) involves two different ranges.

Assume first that $\gamma > 1$ (that is, that $|t-s| < 1/(p-1)$). In that range, we use the polygonal nature of the paths $x \mapsto \mathsf{K}_p(x)$, which implies that

$$|\mathsf{K}_p(t) - \mathsf{K}_p(s)| \leqslant \sqrt{p-1}|t-s| \leqslant \sqrt{|t-s|}$$

(since the "velocity" of the path is $(p-1)/\sqrt{p} \leqslant \sqrt{p-1}$). Consequently, for any $\alpha > 0$, we have

$$\mathbf{E}_p(|\mathsf{K}_p(t) - \mathsf{K}_p(s)|^\alpha) \leqslant |t-s|^{\alpha/2}. \tag{6.7}$$

In the remaining range $\gamma \leqslant 1$, we will use the discontinuous partial sums $\tilde{\mathsf{K}}_p(t)$ instead of $\mathsf{K}_p(t)$. To check that this is legitimate, note that

$$|\tilde{\mathsf{K}}_p(t) - \mathsf{K}_p(t)| \leqslant \frac{1}{\sqrt{p}}$$

for all primes $p \geqslant 3$ and all t. Hence, using Hölder's inequality, we derive for $\alpha \geqslant 1$ the relation

$$\begin{aligned}\mathbf{E}_p(|\mathsf{K}_p(t) - \mathsf{K}_p(s)|^\alpha) &= \mathbf{E}_p(|\tilde{\mathsf{K}}_p(t) - \tilde{\mathsf{K}}_p(s)|^\alpha) + \mathrm{O}(p^{-\alpha/2}) \\ &= \mathbf{E}_p(|\tilde{\mathsf{K}}_p(t) - \tilde{\mathsf{K}}_p(s)|^\alpha) + \mathrm{O}(|t-s|^{\alpha/2}),\end{aligned} \tag{6.8}$$

where the implied constant depends only on α.

We take $\alpha = 4$. The following computation of the fourth moment is an idea that goes back to Kloosterman's very first nontrivial estimate for individual Kloosterman sums.

We have

$$\tilde{\mathsf{K}}_p(t) - \tilde{\mathsf{K}}_p(s) = \frac{1}{\sqrt{p}} \sum_{n \in \mathrm{I}} e\left(\frac{an + b\bar{n}}{p}\right),$$

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

where I is the discrete interval

$$(p-1)s < n \leqslant (p-1)t$$

of summation. The length of I is

$$\lfloor (p-1)t \rfloor - \lceil (p-1)s \rceil \leqslant 2(p-1)|t-s|$$

since $(p-1)|t-s| \geqslant 1$.

By expanding the fourth power, we get

$$\begin{aligned}
&\mathbf{E}_p(|\tilde{\mathsf{K}}_p(t) - \tilde{\mathsf{K}}_p(s)|^4) \\
&= \frac{1}{(p-1)^2} \sum_{(a,b)\in \mathbf{F}_p^\times \times \mathbf{F}_p^\times} \left| \frac{1}{\sqrt{p}} \sum_{n\in \mathrm{I}} e\left(\frac{an+b\bar{n}}{p}\right)\right|^4 \\
&= \frac{1}{p^2(p-1)^2} \sum_{a,b} \sum_{n_1,\dots,n_4\in \mathrm{I}} e\left(\frac{a(n_1+n_2-n_3-n_4)}{p}\right) \\
&\quad \times e\left(\frac{b(\bar{n}_1+\bar{n}_2-\bar{n}_3-\bar{n}_4)}{p}\right).
\end{aligned}$$

After exchanging the order of the sums, which "separates" the two variables a and b, we get

$$\begin{aligned}
&\frac{1}{p^2(p-1)^2} \sum_{n_1,\dots,n_4\in \mathrm{I}} \left(\sum_{a\in \mathbf{F}_p^\times} e\left(\frac{a(n_1+n_2-n_3-n_4)}{p}\right)\right) \\
&\qquad \times \left(\sum_{b\in \mathbf{F}_p^\times} e\left(\frac{b(\bar{n}_1+\bar{n}_2-\bar{n}_3-\bar{n}_4)}{p}\right)\right).
\end{aligned}$$

The orthogonality relations for additive character (namely, the relation

$$\frac{1}{p}\sum_{a\in \mathbf{F}_p^\times} e\left(\frac{ah}{p}\right) = \delta(h,0) - \frac{1}{p}$$

for any $h \in \mathbf{F}_p$) imply that

$$\mathbf{E}_p(|\tilde{\mathsf{K}}_p(t) - \tilde{\mathsf{K}}_p(s)|^4) = \frac{1}{(p-1)^2} \sum_{\substack{n_1,\dots,n_4\in \mathrm{I} \\ n_1+n_2=n_3+n_4 \\ \bar{n}_1+\bar{n}_2=\bar{n}_3+\bar{n}_4}} 1 + \mathrm{O}(|\mathrm{I}|^3(p-1)^{-3}). \quad (6.9)$$

Fix first n_1 and n_2 in I with $n_1+n_2 \neq 0$. Then if (n_3,n_4) satisfy

$$n_1+n_2 = n_3+n_4 \quad \text{and} \quad \bar{n}_1+\bar{n}_2 = \bar{n}_3+\bar{n}_4,$$

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

the value of $n_3 + n_4$ is fixed, and $\bar{n}_1 + \bar{n}_2$ is nonzero, so

$$n_3 n_4 = \frac{n_3 + n_4}{\bar{n}_1 + \bar{n}_2}$$

(in $\mathbf{F}_p^\times$) is also fixed. Hence there are at most two pairs (n_3, n_4) that satisfy the equations for these given (n_1, n_2). This means that the contribution of these n_1, n_2 to (6.9) is $\leqslant 2|\mathrm{I}|^2(p-1)^{-2}$. Similarly, if $n_1 + n_2 = 0$, the equations imply that $n_3 + n_4 = 0$, and hence the solutions are determined uniquely by (n_1, n_3). Hence the contribution is then $\leqslant |\mathrm{I}|^2(p-1)^2$, and we get

$$\mathbf{E}_p(|\tilde{\mathsf{K}}_p(t) - \tilde{\mathsf{K}}_p(s)|^4) \ll |\mathrm{I}|^2(p-1)^{-2} + |\mathrm{I}|^3(p-1)^{-3} \ll |t-s|^2,$$

where the implied constants are absolute. Using (6.8), this gives

$$\mathbf{E}_p(|\mathsf{K}_p(t) - \mathsf{K}_p(s)|^4) \ll |t-s|^2 \tag{6.10}$$

with an absolute implied constant. Combined with (6.7) with $\alpha = 4$ in the former range, this completes the proof of tightness.

Final Step. (Proof of Theorem 6.1.1) In view of Proposition B.11.8, the theorem follows directly from the results of Steps 2 and 3.

Remark 6.2.5 The proof of tightness uses crucially that we average over both a and b to reduce the problem to counting the number of solutions of certain equations over $\mathbf{F}_p$ (see (6.9)), which turn out to be accessible. Since $\mathrm{Kl}(a,b;p) = \mathrm{Kl}(ab;1,p)$ for all a and b in $\mathbf{F}_p^\times$, it seems natural to try to prove an analogue of Theorem 6.1.1 when averaging only over a, with $b = 1$ fixed. The convergence of finite distributions extends to that setting (since Theorem 6.2.2 holds for any fixed b), but a proof of tightness is not currently known for fixed b. Using moment estimates (derived from Deligne's Riemann Hypothesis) and the trivial bound

$$\left|\tilde{\mathsf{K}}_p(t) - \tilde{\mathsf{K}}_p(s)\right| \leqslant |\mathrm{I}|p^{-1/2},$$

one can check that it is enough to prove a suitable estimate for the average over a in the restricted range where

$$\frac{1}{2} - \eta \leqslant \gamma \leqslant \frac{1}{2} + \eta$$

for some fixed but arbitrarily small value of $\eta > 0$ (see [79, §3]). The next exercise illustrates this point.

Exercise 6.2.6 Assume p is odd. Let $\Omega'_p = \mathbf{F}_p^\times \times (\mathbf{F}_p^\times)^2$, where $(\mathbf{F}_p^\times)^2$ is the set of nonzero squares in $\mathbf{F}_p^\times$. We denote by $\mathsf{K}'_p(t)$ the random variable $\mathsf{K}_p(t)$

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

restricted to Ω'_p, with the uniform probability measure, for which $\mathbf{P}'_p(\cdot)$ and $\mathbf{E}'_p(\cdot)$ denote probability and expectation.

(1) Prove that $\mathrm{FT}(\mathsf{K}'_p)$ converges to FT(K) in the sense of finite distributions.

(2) For $n \in \mathbf{F}_p$, prove that

$$\sum_{b\in(\mathbf{F}_p^\times)^2} e\left(\frac{bn}{p}\right) = \frac{p-1}{2}\delta(n,0) + \mathrm{O}(\sqrt{p}),$$

where the implied constant is absolute. [**Hint**: Show that if $n \in \mathbf{F}_p^\times$, we have

$$\left|\sum_{b\in\mathbf{F}_p^\times} e\left(\frac{nb^2}{p}\right)\right| = \sqrt{p},$$

where the left-hand sum is known as a *quadratic Gauss sum*; see Example C.6.2 (1) and Exercise C.6.5.]

(3) Deduce that if $|t-s| \geqslant 1/p$, then

$$\mathbf{E}'_p(|\mathsf{K}'_p(t) - \mathsf{K}'_p(s)|^4) \ll \sqrt{p}|t-s|^3 + |t-s|^2,$$

where the implied constant is absolute.

(3) Using notation as in the proof of tightness for K_p, prove that if $\eta > 0$, $\alpha \geqslant 1$ and

$$\frac{1}{2} + \eta \leqslant \gamma \leqslant 1,$$

then

$$\mathbf{E}'_p(|\mathsf{K}'_p(t) - \mathsf{K}'_p(s)|^\alpha) \ll |t-s|^{\alpha\eta} + |t-s|^{\alpha/2},$$

where the implied constant depends only on α.

(4) Prove that if $\eta > 0$ and

$$0 \leqslant \gamma \leqslant \frac{1}{2} - \eta,$$

then there exists $\delta > 0$ such that

$$\mathbf{E}'_p(|\mathsf{K}'_p(t) - \mathsf{K}'_p(s)|^4) \ll |t-s|^{1+\delta},$$

where the implied constant depends only on η.

(5) Conclude that (K'_p) converges in law to K in $\mathrm{C}([0,1])$. [**Hint**: It may be convenient to use the variant of Kolmogorov's tightness Criterion in Proposition B.11.11.]

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

6.3 Applications

We can use Theorem 6.1.1 to gain information on partial sums of Kloosterman sums. We will give two examples, one concerning large values of the partial sums, and the other dealing with the support of the Kloosterman paths, following [12].

Theorem 6.3.1 *For p prime and $\mathrm{A} > 0$, let $\mathrm{M}_p(\mathrm{A})$ and $\mathrm{N}_p(\mathrm{A})$ be the events*

$$\mathrm{M}_p(\mathrm{A}) = \left\{(a,b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times \mid \max_{1\leqslant j\leqslant p-1} \frac{1}{\sqrt{p}}\left|\sum_{1\leqslant n\leqslant j} e\left(\frac{an+b\bar{n}}{p}\right)\right| > \mathrm{A}\right\},$$

$$\mathrm{N}_p(\mathrm{A}) = \left\{(a,b) \in \mathbf{F}_p^\times \times \mathbf{F}_p^\times \mid \max_{1\leqslant j\leqslant p-1} \frac{1}{\sqrt{p}}\left|\sum_{1\leqslant n\leqslant j} e\left(\frac{an+b\bar{n}}{p}\right)\right| \geqslant \mathrm{A}\right\}.$$

There exists a positive constant $c > 0$ such that, for any $\mathrm{A} > 0$, we have

$$\begin{aligned} c^{-1}\exp(-\exp(c\mathrm{A})) &\leqslant \liminf_{p\to+\infty} \mathbf{P}_p(\mathrm{N}_p(\mathrm{A})) \\ &\leqslant \limsup_{p\to+\infty} \mathbf{P}_p(\mathrm{M}_p(\mathrm{A})) \leqslant c\exp(-\exp(c^{-1}\mathrm{A})). \end{aligned}$$

In particular, partial sums of normalized Kloosterman sums are unbounded (whereas the full normalized Kloosterman sums are always of modulus at most 2), but large values of partial sums are extremely rare.

Proof The functions $t \mapsto \mathsf{K}_p(a,b)(t)$ describe polygonal paths in the complex plane. Since the maximum modulus of a point on such a path is achieved at one of the vertices, it follows that

$$\max_{1\leqslant j\leqslant p-1} \frac{1}{\sqrt{p}}\left|\sum_{1\leqslant n\leqslant j} e\left(\frac{an+b\bar{n}}{p}\right)\right| = \|\mathsf{K}_p(a,b)\|_\infty,$$

so that the event $\mathrm{M}_p(\mathrm{A})$ is the same as $\{\|\mathsf{K}_p\|_\infty > \mathrm{A}\}$, and $\mathrm{N}_p(\mathrm{A})$ is the same as $\{\|\mathsf{K}_p\|_\infty \geqslant \mathrm{A}\}$.

By Theorem 6.1.1 and composition with the norm map (Proposition B.3.2), the real-valued random variables $\|\mathsf{K}_p\|_\infty$ converge in law to the random variable $\|\mathrm{K}\|_\infty$, the norm of the random Fourier series K. By elementary properties of convergence in law, we have therefore

$$\mathbf{P}(\|\mathrm{K}\|_\infty > \mathrm{A}) \leqslant \liminf_{p\to+\infty} \mathbf{P}_p(\mathrm{N}_p(\mathrm{A})) \leqslant \limsup_{p\to+\infty} \mathbf{P}_p(\mathrm{M}_p(\mathrm{A})) \leqslant \mathbf{P}(\|\mathrm{K}\|_\infty \geqslant \mathrm{A}).$$

So the problem is reduced to questions about the limiting random Fourier series.

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

We first consider the upper bound. Here it suffices to prove the existence of a constant $c > 0$ such that

$$\mathbf{P}(\| \operatorname{Im}(\mathrm{K})\|_\infty > \mathrm{A}) \leqslant c \exp(-\exp(c^{-1}\mathrm{A})),$$
$$\mathbf{P}(\| \operatorname{Re}(\mathrm{K})\|_\infty > \mathrm{A}) \leqslant c \exp(-\exp(c^{-1}\mathrm{A})).$$

We will do this for the real part, since the imaginary part is very similar and can be left as an exercise. The random variable $\mathrm{R} = \operatorname{Re}(\mathrm{K})$ takes values in the separable real Banach space $\mathrm{C}_{\mathbf{R}}([0,1])$ of real-valued continuous functions on $[0,1]$. It is almost surely the sum of the random Fourier series

$$\mathrm{R} = \sum_{h \geqslant 0} \varphi_h \mathrm{Y}_h,$$

where $\varphi_h \in \mathrm{C}_{\mathbf{R}}([0,1])$ and the random variables Y_h are defined by

$$\varphi_0(t) = 2t, \qquad \mathrm{Y}_0 = \tfrac{1}{2}\mathrm{ST}_0,$$
$$\varphi_h(t) = \frac{\sin(2\pi h t)}{8\pi h}, \quad \mathrm{Y}_h = \tfrac{1}{4}(\mathrm{ST}_h + \mathrm{ST}_{-h}) \text{ for } h \geqslant 1.$$

We note that the random variables (Y_h) are independent and that $|\mathrm{Y}_h| \leqslant 1$ (almost surely) for all h. We can then apply the bound of Proposition B.11.13 (1) to conclude.

We now prove the lower bound. It suffices to prove that there exists $c > 0$ such that

$$\mathbf{P}(|\operatorname{Im}(\mathrm{K}(1/2))| > \mathrm{A}) \geqslant c^{-1} \exp(-\exp(c\mathrm{A})), \tag{6.11}$$

since this implies that

$$\mathbf{P}(\|\mathrm{K}\|_\infty > \mathrm{A}) \geqslant c^{-1} \exp(-\exp(c\mathrm{A})).$$

We have

$$\operatorname{Im}(\mathrm{K}(1/2)) = -\frac{1}{2\pi} \sum_{h \neq 0} \frac{\cos(\pi h) - 1}{h} \mathrm{ST}_h = \frac{1}{\pi} \sum_{h \geqslant 1} \frac{1}{h} \mathrm{ST}_h,$$

which is a series that converges almost surely in $\mathbf{R}$ with independent terms, and where $\frac{1}{\pi}\mathrm{ST}_h$ is symmetric and $\leqslant 1$ in absolute value for all h. Thus the bound

$$\mathbf{P}(|\operatorname{Im}(\mathrm{K}(1/2))| > \mathrm{A}) \geqslant c^{-1} \exp(-\exp(c\mathrm{A}))$$

for some $c > 0$ follows immediately from Proposition B.11.13 (2). □

Remark 6.3.2 In the lower bound, the point $1/2$ could be replaced by any $t \in]0,1[$ for the imaginary part, and one could also use the real part and any t such

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

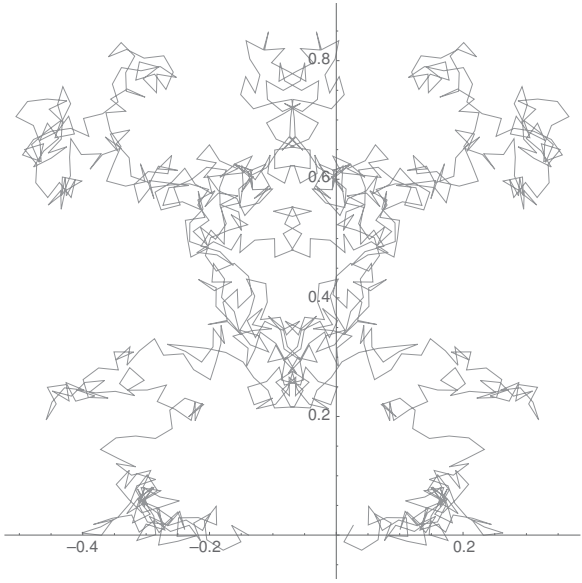

Figure 6.4 The partial sums of Kl(88, 1; 1021).

that $t \notin \{0, 1/2, 1\}$; the symmetry of the Kloosterman paths with respect to the line $x = \frac{1}{2}\,\mathrm{Kl}(a, b; p)$ shows that the real part of $\mathsf{K}_p(a, b)(1/2)$ is $\frac{1}{2}\,\mathrm{Kl}(a, b; p)$, and this is a real number in $[-1, 1]$.

For our second application, we compute the support of the random Fourier series K.

Theorem 6.3.3 *The support of the law of* K *is the set of all* $f \in \mathrm{C}_0([0, 1])$ *such that*

(1) *we have* $f(1) \in [-2, 2]$*;*
(2) *for all* $h \neq 0$*, we have* $\widetilde{f}(h) \in i\mathbf{R}$ *and*

$$|\widetilde{f}(h)| \leqslant \frac{1}{\pi\,|h|}.$$

Proof Denote by $\mathcal{S}$ the set described in the statement. Then $\mathcal{S}$ is closed in $\mathrm{C}([0, 1])$, since it is the intersection of closed sets. By Theorem 6.1.1, a sample function $f \in \mathrm{C}([0, 1])$ of the random process K is almost surely given by a series

$$f(t) = \alpha_0 t + \sum_{h \neq 0} \frac{e(ht) - 1}{2\pi i h}\alpha_h$$

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

that is uniformly convergent in the sense of symmetric partial sums, for some real numbers α_h such that $|\alpha_h| \leqslant 2$. We have $\widetilde{f}(0) = f(1) \in [-2,2]$, and the uniform convergence implies that for $h \neq 0$, we have

$$\widetilde{f}(h) = \frac{\alpha_h}{2i\pi h},$$

so that f certainly belongs to $\mathcal{S}$. Consequently, the support of K is contained in $\mathcal{S}$.

We now prove the converse inclusion. By Lemma B.3.3, the support of K contains the set of continuous functions with uniformly convergent (symmetric) expansions

$$t\alpha_0 + \sum_{h\neq 0} \frac{e(ht)-1}{2\pi i h}\alpha_h,$$

where $\alpha_h \in [-2,2]$ for all $h \in \mathbf{Z}$. In particular, since 0 belongs to the support of the Sato–Tate measure, $\mathcal{S}$ contains all finite sums of this type.

Let $f \in \mathcal{S}$ and put $g(t) = f(t) - tf(1)$. We have

$$f(t) - tf(1) = \lim_{N\to+\infty} \sum_{|h|\leqslant N} \widehat{g}(h)e(ht)\left(1 - \frac{|h|}{N}\right)$$

in $C_0([0,1])$, by the uniform convergence of Cesàro means of the Fourier series of a continuous periodic function (see, e.g., [121, III, th. 3.4]). Evaluating at 0 and subtracting yields

$$\begin{aligned} f(t) &= tf(1) + \lim_{N\to+\infty} \sum_{\substack{|h|\leqslant N\\ h\neq 0}} \widetilde{f}(h)(e(ht)-1)\left(1-\frac{|h|}{N}\right)\\ &= tf(1) + \lim_{N\to+\infty} \sum_{\substack{|h|\leqslant N\\ h\neq 0}} \frac{\alpha_h}{2i\pi h}(e(ht)-1)\left(1-\frac{|h|}{N}\right) \end{aligned}$$

in $C([0,1])$, where $\alpha_h = 2i\pi h\widetilde{f}(h)$ for $h \neq 0$. Then $\alpha_h \in \mathbf{R}$ and $|\alpha_h| \leqslant 2$ by the assumption that $f \in \mathcal{S}$, so each function

$$tf(1) + \sum_{\substack{|h|\leqslant N\\ h\neq 0}} \frac{e(ht)-1}{2\pi i h}\alpha_h\left(1-\frac{|h|}{N}\right),$$

belongs to the support of K. Since the support is closed, we conclude that f also belongs to the support of K. □

The support of K is an interesting set of functions. Testing whether a function $f \in C_0([0,1])$ belongs to it, or not, is straightforward if the Fourier

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press

coefficients of f are known, and a positive or negative answer has interesting arithmetic consequences, by Lemma B.3.3. In particular, since 0 clearly belongs to the support of K, we get:

Corollary 6.3.4 *For any $\varepsilon > 0$, we have*

$$\liminf_{p\to+\infty} \frac{1}{(p-1)^2}\left|\left\{(a,b)\in \mathbf{F}_p^\times \times \mathbf{F}_p^\times \mid \max_{0\leqslant j\leqslant p-1}\left|\frac{1}{\sqrt{p}}\sum_{1\leqslant x\leqslant j} e\left(\frac{ax+b\bar{x}}{p}\right)\right| < \varepsilon\right\}\right| > 0.$$

We refer to [12] for further examples of functions belonging (or not) to the support of K and mention only a remarkable result of J. Bober: the support of K contains space-filling curves, that is, functions f such that the image of f has nonempty interior.

6.4 Generalizations

The method of Kowalski and Sawin can be extended to study the "shape" of many other exponential sums. On the other hand, natural generalizations require different tools, when the Riemann Hypothesis is not applicable anymore. This was achieved by Ricotta and Royer [101] for Kloosterman sums modulo p^n when $n \geqslant 2$ is fixed and $p \to +\infty$, and later, they succeeded with Shparlinski [102] in obtaining convergence in law in that setting with a single variable a. If p is fixed and $n \to +\infty$, the corresponding study was done by Milićević and Zhang [87], where tools related to p-adic analysis are crucial. In the three cases, the limit random Fourier series are similar, but have coefficients that have distributions different from the Sato–Tate distribution.

Related developments concern quantitative versions of Theorem 6.3.1: how large (and how often) can one make a partial sum of Kloosterman sums? Results of this kind have been proved by Lamzouri [82] and Bonolis [14], and in great generality by Autissier, Bonolis and Lamzouri [3].

Finally, in another direction, Cellarosi and Marklof [22] have established beautiful functional limit theorems for other types of exponential sums closer to the Weyl sums that arise in the circle method, and especially for quadratic Weyl sums. The tools as well as the limiting functions are completely different.

[Further references: Iwaniec and Kowalski [59, Ch. 11].]

https://doi.org/10.1017/9781108888226.007 Published online by Cambridge University Press