Bulletin

de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

KLOOSTERMAN PATHS OF PRIME POWERS MODULI, II

Guillaume Ricotta, Emmanuel Royer & Igor Shparlinski

Tome 148
Fascicule 1

2020

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

pages 173-188

Le *Bulletin de la Société Mathématique de France* est un périodique trimestriel de la Société Mathématique de France.

Fascicule 1, tome 148, mars 2020

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
commandes@smf.emath.fr

AMS
P.O. Box 6248
Providence RI 02940
USA
www.ams.org

Tarifs

Vente au numéro : 43 € ($ 64)
Abonnement électronique : 135 € ($ 202),
avec supplément papier : Europe 179 €, hors Europe 197 € ($ 296)
Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Bulletin de la SMF

Bulletin de la Société Mathématique de France
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 1 44 27 67 99 • Fax : (33) 1 40 46 90 96
bulletin@smf.emath.fr • smf.emath.fr

ISSN 0037-9484 (print) 2102-622X (electronic)

Directeur de la publication : Stéphane SEURET

Bull. Soc. Math. France
148 (1), 2020, p. 173-188

KLOOSTERMAN PATHS OF PRIME POWERS MODULI, II

BY GUILLAUME RICOTTA, EMMANUEL ROYER & IGOR SHPARLINSKI

ABSTRACT. — G. Ricotta and E. Royer (2018) have recently proved that the polygonal paths joining the partial sums of the normalized classical Kloosterman sums $S\left(a, b; p^n\right)/p^{n/2}$ converge in law in the Banach space of complex-valued continuous function on $[0,1]$ to an explicit random Fourier series as (a, b) varies over $(\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times$, p tends to infinity among the odd prime numbers and $n \geq 2$ is a fixed integer. This is the analogue of the result obtained by E. Kowalski and W. Sawin (2016) in the prime moduli case. The purpose of this work is to prove a convergence law in this Banach space as only a varies over $(\mathbb{Z}/p^n\mathbb{Z})^\times$, p tends to infinity among the odd prime numbers and $n \geq 31$ is a fixed integer.

Texte reçu le 31 janvier 2019, modifié le 7 mai 2019, accepté le 9 mai 2019.

GUILLAUME RICOTTA, Université de Bordeaux, Institut de Mathématiques de Bordeaux, 351, cours de la Libération, 33405 Talence cedex, France • *E-mail :* `Guillaume.Ricotta@math.u-bordeaux.fr`

EMMANUEL ROYER, Laboratoire de mathématiques Blaise Pascal, Campus universitaire des Cézeaux, 3 place Vasarely, TSA 60026, CS 60026, 63178 Aubière cedex, France • *E-mail :* `emmanuel.royer@math.cnrs.fr`

IGOR SHPARLINSKI, The University of New South Wales, Sydney NSW 2052, Australia • *E-mail :* `igor.shparlinski@unsw.edu.au`

Mathematical subject classification (2010). — 11T23, 11L05, 60F17, 60G17, 60G50.

Key words and phrases. — Kloosterman sums, Moments, Probability in Banach spaces.

 0037-9484/2020/173/$ 5.00
 doi:10.24033/bsmf.2802

Résumé (*Chemins de Kloosterman de modules une puissance d'un nombre premier, II*). — G. Ricotta et E. Royer (2018) ont récemment prouvé que le chemin polygonal joignant les sommes partielles des sommes de Kloosterman classiques normalisées $S(a,b;p^n)/p^{n/2}$ converge en loi dans l'espace de Banach des fonctions continues sur $[0,1]$ à valeurs complexes vers une série de Fourier aléatoire explicite lorsque (a,b) parcourt $(\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times$, p tend vers l'infini parmi les nombres premiers impairs et $n \geq 2$ est un entier fixé. Ceci est l'analogue du résultat obtenu par E. Kowalski et W. Sawin (2016) dans le cas des modules premiers. L'objectif de ce travail est de prouver une convergence en loi dans cet espace de Banach lorsque seul a parcourt $(\mathbb{Z}/p^n\mathbb{Z})^\times$, p tend vers l'infini parmi les nombres premiers impairs et $n \geq 31$ est un entier fixé.

In memory of Alexey Zynkin.

1. Introduction and statement of the results

1.1. Background. — Let p be an odd prime number and $n \geq 1$ be an integer. For a and b in $\mathbb{Z}/p^n\mathbb{Z}$, the corresponding normalized Kloosterman sum of modulus p^n is the real number given by

$$\mathsf{Kl}_{p^n}(a,b) := \frac{1}{p^{n/2}} S(a,b;p^n) = \frac{1}{p^{n/2}} \sum_{\substack{1 \leq x \leq p^n \\ p \nmid x}} e\left(\frac{ax+b\overline{x}}{p^n}\right),$$

where as usual $\overline{x}$ stands for the inverse of x modulo p^n and we also define $e(z) := \exp(2i\pi z)$ for any complex number z. Recall that its absolute value is less than 2 by its explicit formula (see [5, Lemma 4.6] for instance). For a and b in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, the associated partial sums are the $\varphi(p^n) = p^{n-1}(p-1)$ complex numbers

$$\mathsf{Kl}_{j;p^n}(a,b) := \frac{1}{p^{n/2}} \sum_{\substack{1 \leq x \leq j \\ p \nmid x}} e\left(\frac{ax+b\overline{x}}{p^n}\right)$$

for j in $\mathcal{J}_p^n := \{j \in \{1,\dots,p^n\}, p \nmid j\}$. If we write $\mathcal{J}_p^n = \{j_1,\dots,j_{\varphi(p^n)}\}$, the corresponding Kloosterman path $\gamma_{p^n}(a,b)$ is defined by

$$\gamma_{p^n}(a,b) = \bigcup_{i=1}^{\varphi(p^n)-1} \left[\mathsf{Kl}_{j_i;p^n}(a,b), \mathsf{Kl}_{j_{i+1};p^n}(a,b)\right].$$

This is the polygonal path obtained by concatenating the closed segments

$$[\mathsf{Kl}_{j_1;p^n}(a,b), \mathsf{Kl}_{j_2;p^n}(a,b)]$$

for j_1 and j_2 two consecutive indices in $\mathcal{J}_{p^n}$. Finally, one defines a continuous map on the interval $[0,1]$

$$t \mapsto \mathsf{Kl}_{p^n}(t;(a,b))$$

by parameterizing the path $\gamma_{p^n}(a,b)$, each segment

$$[\mathsf{Kl}_{j_1;p^n}(a,b),\ \mathsf{Kl}_{j_2;p^n}(a,b)]$$

for j_1 and j_2 two consecutive indices in $\mathcal{J}_{p^n}$ being parametrized linearly by an interval of length $1/(\varphi(p^n)-1)$.

The function $(a,b)\mapsto \mathsf{Kl}_{p^n}(*;(a,b))$ is viewed as a random variable on the probability space $(\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times$ endowed with the uniform probability measure with values in the Banach space of complex-valued continuous functions on $[0,1]$ endowed with the supremum norm, say $C^0([0,1],\mathbb{C})$.

Let μ be the probability measure given by

$$\mu = \frac{1}{2}\delta_0 + \mu_0$$

for the Dirac measure δ_0 at 0 and

$$\mu_0(f) = \frac{1}{2\pi}\int_{x=-2}^{2} \frac{f(x)\mathrm{d}x}{\sqrt{4-x^2}}$$

for any real-valued continuous function f on $[-2,2]$.

Let $(U_h)_{h\in\mathbb{Z}}$ be a sequence of independent identically distributed random variables of probability law μ and let Kl be the $C^0([0,1],\mathbb{C})$-valued random variable defined by

$$\forall t\in[0,1],\quad \mathsf{Kl}(t)(*) = tU_0(*) + \sum_{h\in\mathbb{Z}^*} \frac{e(ht)-1}{2i\pi h} U_h(*)$$

where the series should be summed with symmetric partial sums. The basic properties of this random Fourier series are given in [5, Proposition 3.1].

In [5], it has been proved that the sequence of $C^0([0,1],\mathbb{C})$-valued random variables $\mathsf{Kl}_{p^n}(*;(*,*))$ on $(\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times$ converges in law[1] to the $C^0([0,1],\mathbb{C})$-valued random variable Kl as p tends to infinity among the prime numbers and $n\geq 2$ is a fixed integer. This is the analogue of the result proved by E. Kowalski and W. Sawin in [3] when $n=1$ where a different random Fourier series occurs, the measure μ being replaced by the Sato-Tate measure.

1.2. Our results and approach. — The purpose of this work is the following substantial refinement of [5].

Theorem 1.1 (Convergence in law). — *Let b_0 be a fixed non-zero integer, $n\geq 31$ be a fixed integer and p be an odd prime number. The sequence of $C^0([0,1],\mathbb{C})$-valued random variables $\mathsf{Kl}_{p^n}(*;(*,b_0))$ on $(\mathbb{Z}/p^n\mathbb{Z})^\times$ converges in law to the $C^0([0,1],\mathbb{C})$-valued random variable Kl as p tends to infinity among the odd prime numbers.*

1. See [5, Appendix A] for a precise definition of the convergence in law in the Banach space $C^0([0,1],\mathbb{C})$.

This result is not a purely technical problem. This question should be seen as a very challenging one already highlighted as a key open problem in [3]. Note that the case of prime moduli remains open.

The general strategy to prove Theorem 1.1 is the one used in [3] and in [5]. It consists of two distinct steps.

First of all, the convergence in the sense of finite distributions[2] of the sequence of $C^0([0,1],\mathbb{C})$-valued random variables $\mathsf{Kl}_{p^n}(*;(*,b_0))$ on $(\mathbb{Z}/p^n\mathbb{Z})^\times$ to the $C^0([0,1],\mathbb{C})$-valued random variable Kl as p tends to infinity among the odd prime numbers is proved. This result is nothing other than [5, Theorem A] and heavily relies on Weil's version of the Riemann hypothesis in one variable, see [4]. Note that $n \geq 2$ is fixed in this work, although most of our ingredients work for arbitrary n as well. Indeed, the only place where n has to be a fixed integer is when using [5, Theorem A] page 187.

Then, to deduce the convergence in law from the convergence of finite distributions, one has to prove that the sequence of $C^0([0,1],\mathbb{C})$-valued random variables $\mathsf{Kl}_{p^n}(*;(*,b_0))$ on $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is tight, a weak-compactness property which takes into account that $C^0([0,1],\mathbb{C})$ is infinite-dimensional. See [5, Appendix A] for a precise definition. This is the main input in this work.

Theorem 1.2 (Tightness property). — *Let b_0 be a fixed non-zero integer, $n \geq 31$ be a fixed integer and p be an odd prime number. The sequence of $C^0([0,1],\mathbb{C})$-valued random variables $\mathsf{Kl}_{p^n}(*;(*,b_0))$ on $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is tight as p tends to infinity among the odd prime numbers.*

The proof of this tightness property in Theorem 1.2 follows the strategy outlined in [3]. The core of the proof is a uniform estimate of the shape

$$\frac{1}{p^{n/2}} \sum_{x \in \mathcal{I}}^{\times} e\left(\frac{ax + b\overline{x}}{p^n}\right) \ll p^{-\delta}$$

for some $\delta > 0$ when $\mathcal{I}$ is an interval of $\mathbb{Z}$ of length close to $p^{n/2}$, and a and b are some integers coprime with p. See [3, Remark 3.3] and [1, Page 52] for a discussion on such issues in the prime moduli case. It turns out that for n large enough, such estimate follows from the work contained in [2].

Finally, one can mention that it seems quite natural to consider the same questions in the regime p a fixed prime number and $n \geq 2$ tends to infinity, or even in a more complicated regime when both p and n vary. This problem, both theoretically and numerically, seems to be of a completely different nature.

1.3. Organization of the paper. — The explicit description of the Kloosterman paths and some required results proved in [5] are recalled in Section 2. Section 3 deals with Korolev's estimate for short Kloosterman sums of powerful moduli.

2. See [5, Appendix A] for a precise definition of the convergence in the sense of finite distributions in the Banach space $C^0([0,1],\mathbb{C})$.

The tightness condition is proved in Section 4. Theorems 1.1 and 1.2 are proved in Section 5.

1.4. Notation. — The main parameter in this paper is an odd prime p, which tends to infinity. Thus, if f and g are some $\mathbb{C}$-valued function of one real variable then the notations

$$f(p) = O_A(g(p)) \quad \text{or} \quad f(p) \ll_A g(p) \quad \text{or} \quad g(p) \gg_A f(p)$$

mean that $|f(p)|$ is smaller than a constant, which only depends on A, times $g(p)$ at least for p large enough.

Throughout the paper, $n \geq 2$ is a fixed integer and b_0 is a fixed non-zero integer.

For any real number x and integer k,

$$e_k(x) := \exp\left(\frac{2i\pi x}{k}\right).$$

For any finite set S, $|S|$ stands for its cardinality.

We will denote by ε an absolute positive constant whose definition may change from one line to the next.

The notation $\sum^{\times}$ means that the summation is over a set of integers coprime with p.

2. Background on the Kloosterman path

2.1. Explicit description of the Kloosterman path. — Let us recall the construction of the Kloosterman path $\gamma_{p^n}(a, b_0)$ given in [5, Section 2] for a in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

We enumerate the partial Kloosterman sums and define $z_j((a, b_0); p^n)$ to be the j-th term of $(\mathsf{Kl}_{j;p^n}(a, b_0))_{j \in \mathcal{J}_p^n}$. More explicitly, we organise the partial Kloosterman sums in p^{n-1} blocks each of them containing $p-1$ successive sums. For $1 \leq k \leq p^{n-1}$, the k-th block contains

$$\mathsf{Kl}_{(k-1)p+1;p^n}(a, b_0), \ldots, \mathsf{Kl}_{kp-1;p^n}(a, b_0).$$

These sums are numbered by defining

$$z_{(k-1)(p-1)+\ell}((a, b_0); p^n) = \mathsf{Kl}_{(k-1)p+\ell;p^n}(a, b_0) \qquad (1 \leq \ell \leq p-1).$$

It implies that the enumeration is given by

$$z_j((a, b_0); p^n) = \mathsf{Kl}_{j+\lfloor \frac{j-1}{p-1} \rfloor;p^n}(a, b_0) \qquad (1 \leq j < \varphi(p^n)).$$

For any $j \in \{1, \ldots, \varphi(p^n) - 1\}$, we parametrize the open segment

$$(z_j((a, b_0); p^n), z_{j+1}((a, b_0); p^n)]$$

and obtain the parametrization of $\gamma_{p^n}(a,b_0)$ given by

(1)
$$\forall t\in[0,1],\quad \mathsf{Kl}_{p^n}(t;(a,b_0))=\alpha_j((a,b_0);p^n)\left(t-\frac{j-1}{\varphi(p^n)-1}\right)+z_j((a,b_0);p^n)$$

with

$$\alpha_j((a,b_0);p^n)=(\varphi(p^n)-1)\left(z_{j+1}((a,b_0);p^n)-z_j((a,b_0);p^n)\right)$$

and

$$j=\lceil(\varphi(p^n)-1)\,t\rceil\quad\text{namely}\quad\frac{j-1}{\varphi(p^n)-1}<t\leq\frac{j}{\varphi(p^n)-1}.$$

Since $(z_j((a,b_0);p^n),z_{j+1}((a,b_0);p^n)]$ has length $p^{-n/2}$, we have

(2)
$$|\alpha_j((a,b_0);p^n)|\leq\frac{\varphi(p^n)-1}{p^{n/2}}.$$

2.2. Approximation of the Kloosterman path. — For a in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, let us define a step function on the segment $[0,1]$ by, for any $k\in\left\{1,\ldots,p^{n-1}\right\}$,

(3)
$$\forall t\in\left(\frac{k-1}{p^{n-1}},\frac{k}{p^{n-1}}\right],\quad \widetilde{\mathsf{Kl}_{p^n}}(t;(a,b_0)):=\frac{1}{p^{n/2}}\sideset{}{^\times}\sum_{1\leq x\leq x_k(t)}e_{p^n}\left(ax+b_0\overline{x}\right).$$

where

$$x_k(t):=\varphi(p^n)t+k-1.$$

In addition, let us define for h in $\mathbb{Z}/p^n\mathbb{Z}$ and $1\leq k\leq p^{n-1}$,

(4)
$$\forall t\in\left(\frac{k-1}{p^{n-1}},\frac{k}{p^{n-1}}\right],\quad \alpha_{p^n}(h;t):=\frac{1}{p^{n/2}}\sum_{1\leq x\leq x_k(t)}e_{p^n}\left(hx\right).$$

These coefficients are nothing other than the discrete Fourier coefficients of the finite union of intervals given by $1\leq x\leq x_k(t)$ with $(p,x)=1$ for $1\leq k\leq p^{n-1}$.

The sequence of random variables $\widetilde{\mathsf{Kl}_{p^n}}(*;(*,b_0))$ on $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is an approximation of the sequence of $C^0([0,1],\mathbb{C})$-valued random variables $\mathsf{Kl}_{p^n}(*;(*,b_0))$ on $(\mathbb{Z}/p^n\mathbb{Z})^\times$ in the sense that

(5)
$$\left|\mathsf{Kl}_{p^n}(t;(a,b_0))-\widetilde{\mathsf{Kl}_{p^n}}(t;(a,b_0))\right|\leq\frac{6}{p^{n/2}}$$

for any a in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ and any $t\in[0,1]$. See [5, Equation (2.3)].

Finally, by [5, Lemma 4.2] and [5, Remark 4.5],

(6)
$$\widetilde{\mathsf{Kl}_{p^n}}(t;(a,b_0))\ll\log\left(p^n\right).$$

Note that (5) and (6) are essentially a consequence of the very classical completion method.

3. On Korolev's estimate for short Kloosterman sums of powerful moduli

A key ingredient in this work is the following particular case of an estimate proved by M.A. Korolev for short Kloosterman sums of powerful moduli, see [2, Theorem 1].

PROPOSITION 3.1 (Korolev's estimate [2]). — *Let a b and c be integers and N be a positive integer. If*

$$\max\left(p^{15}, \exp\left(\gamma_1 \left(\log\left(p^n\right)\right)^{2/3}\right)\right) \leq N \leq p^{n/2} \tag{7}$$

then

$$\left|\sum_{c<x\leq c+N}^{\times} e_{p^n}\left(ax+b\overline{x}\right)\right| \leq N \exp\left(-\gamma_2 \frac{\left(\log\left(N\right)\right)^3}{\left(\log\left(p^n\right)\right)^2}\right)$$

where $\gamma_1 = 900$ *and* $\gamma_2 = 160^{-4}$.

COROLLARY 3.2. — *Let a b and c be integers and N be a positive integer. If* $n \geq 31$ *then*

$$\left|\sum_{c<x\leq c+N}^{\times} e_{p^n}\left(ax+b\overline{x}\right)\right| \leq 4N \exp\left(-\gamma_2 \frac{\left(\log\left(N\right)\right)^3}{\left(\log\left(p^n\right)\right)^2}\right).$$

Proof of Corollary 3.2. — By Proposition 3.1, one can assume that

$$N < \min\left(\exp\left(\gamma_1 \left(\log\left(p^n\right)\right)^{2/3}\right), p^{n/2}\right),$$

which implies that

$$\exp\left(-\gamma_2\gamma_1^3\right) \leq \exp\left(-\gamma_2 \frac{\left(\log\left(N\right)\right)^3}{\left(\log\left(p^n\right)\right)^2}\right).$$

Trivially, one gets

$$\begin{aligned}\left|\sum_{c<x\leq c+N}^{\times} e_{p^n}\left(ax+b\overline{x}\right)\right| &\leq N = \exp\left(\gamma_2\gamma_1^3\right)\exp\left(-\gamma_2\gamma_1^3\right)N \\ &\leq 4\exp\left(-\gamma_2\gamma_1^3\right)N \\ &\leq 4\exp\left(-\gamma_2 \frac{\left(\log\left(N\right)\right)^3}{\left(\log\left(p^n\right)\right)^2}\right).\end{aligned}$$

□

COROLLARY 3.3. — *Let a and b be some integers and*

$$0 < \delta \leq \min\left(\gamma_2 n/16, n/2 - 15\right). \tag{8}$$

If $n \geq 31$ then for any interval $\mathcal{I}$ of $\mathbb{Z}$ whose length satisfies

$$p^{n/2-\delta} \leq |\mathcal{I}| \leq p^{n/2+\delta},$$

one has

$$\frac{1}{p^{n/2}} \sum_{x \in \mathcal{I}}^{\times} e_{p^n}\left(ax + b\overline{x}\right) \ll \left(\frac{1}{p^n}\right)^{\delta/n}.$$

Proof of Corollary 3.3. — Let us denote by N the length of $\mathcal{I} = (c, c+N]$.

If $p^{n/2-\delta} \leq N \leq p^{n/2}$ then

(9)
$$\left|\frac{1}{p^{n/2}} \sum_{x \in \mathcal{I}}^{\times} e_{p^n}\left(ax + b\overline{x}\right)\right| \leq 4\frac{N}{p^{n/2}} \exp\left(-\gamma_2 \frac{\left(\log\left(N\right)\right)^3}{\left(\log\left(p^n\right)\right)^2}\right) \leq 4\left(\frac{1}{p^n}\right)^{\gamma_2\left(\frac{n/2-\delta}{n}\right)^3}$$

by Corollary 3.2. Note that (7) is satisfied since $15 \leq n/2 - \delta$.

Let us assume from now on that $N > p^{n/2}$ and let us denote by k the ceiling part of $N/p^{n/2}$. One can decompose the interval $\mathcal{I}$ into a disjoint union of the $k-1$ intervals

$$\mathcal{I}_\ell := \left(c + (\ell-1)p^{n/2}, c + \ell p^{n/2}\right], \quad 1 \leq \ell \leq k-1$$

of lengths $p^{n/2}$ and of the interval

$$\mathcal{I}_k := \left(c + (k-1)p^{n/2}, c + N\right]$$

of length $0 < N - (k-1)p^{n/2} \leq p^{n/2}$. For any $1 \leq \ell \leq k-1$,

$$\left|\frac{1}{p^{n/2}} \sum_{x \in \mathcal{I}_\ell}^{\times} e_{p^n}\left(ax + b\overline{x}\right)\right| \leq \left(\frac{1}{p^n}\right)^{\gamma_2/8} \tag{10}$$

by Proposition 3.1. Note that (7) is satisfied since $15 \leq n/2$.

Let us deal with the last interval $\mathcal{I}_k$. If $N - (k-1)p^{n/2} < p^{n/2-\delta}$ then a trivial estimate leads to

$$\left|\frac{1}{p^{n/2}} \sum_{x \in \mathcal{I}_k}^{\times} e_{p^n}\left(ax + b\overline{x}\right)\right| \leq \left(\frac{1}{p^n}\right)^{\delta/n} \tag{11}$$

whereas if $p^{n/2-\delta} \leq N - (k-1)p^{n/2} \leq p^{n/2}$ then

$$\left|\frac{1}{p^{n/2}} \sum_{x \in \mathcal{I}_k}^{\times} e_{p^n}\left(ax + b\overline{x}\right)\right| \leq 4\left(\frac{1}{p^n}\right)^{\gamma_2\left(\frac{n/2-\delta}{n}\right)^3}. \tag{12}$$

Altogether, if $N > p^{n/2}$ then

(13)
$$\left|\frac{1}{p^{n/2}}\sum_{x\in\mathcal{I}}^{\times} e_{p^n}\left(ax+\overline{x}\right)\right| \leq \left(\frac{1}{p^n}\right)^{\gamma_2/8-\delta/n} + 4\left(\frac{1}{p^n}\right)^{\gamma_2\left(\frac{n/2-\delta}{n}\right)^3} + \left(\frac{1}{p^n}\right)^{\delta/n}.$$

by (10), (11) and (12).

By (9) and (13), one gets

$$\begin{aligned}\left|\frac{1}{p^{n/2}}\sum_{x\in\mathcal{I}}^{\times} e_{p^n}\left(ax+\overline{x}\right)\right| &\leq \left(\frac{1}{p^n}\right)^{\gamma_2/8-\delta/n} + 4\left(\frac{1}{p^n}\right)^{\gamma_2\left(\frac{n/2-\delta}{n}\right)^3} + \left(\frac{1}{p^n}\right)^{\delta/n} \\ &\ll \left(\frac{1}{p^n}\right)^{\delta/n}\end{aligned}$$

since a simple computation ensures that

$$\frac{\delta}{n} \leq \frac{\gamma_2}{8} - \frac{\delta}{n} \leq \gamma_2\left(\frac{n/2-\delta}{n}\right)^3$$

by (8). □

4. On the tightness property via Kolmogorov's criterion

The goal of this section is to prove the following proposition.

Proposition 4.1 (Tightness property). — *Let $n \geq 31$ be a fixed integer and b_0 be a fixed non-zero integer. There exists $\alpha > 0$ depending only on n and $\beta > 0$ depending only on α and n such that*

$$\frac{1}{\varphi\left(p^n\right)}\sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\left|\mathsf{Kl}_{p^n}(t;(a,b_0)) - \mathsf{Kl}_{p^n}(s;(a,b_0))\right|^\alpha \ll_n (t-s)^{1+\beta}$$

for any $0 \leq s,t \leq 1$.

The proof of Proposition 4.1 is a consequence of the following series of lemmas.

Lemma 4.2. — *Let $n \geq 2$ be a fixed integer, b_0 be a fixed non-zero integer and $\alpha > 0$. If*

$$0 \leq t-s \leq \frac{1}{\varphi\left(p^n\right)-1}$$

then

$$\frac{1}{\varphi\left(p^n\right)}\sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\left|\mathsf{Kl}_{p^n}(t;(a,b_0)) - \mathsf{Kl}_{p^n}(s;(a,b_0))\right|^\alpha \leq 2^\alpha(t-s)^{\alpha/2}.$$

Proof of Lemma 4.2. — Note that

$$p^n \leq \frac{4}{t-s}. \tag{14}$$

Let us assume that

$$\frac{j-1}{\varphi\left(p^n\right)-1} < t \leq \frac{j}{\varphi\left(p^n\right)-1}$$

where $1 \leq j \leq \varphi\left(p^n\right)-1$. Two cases can occur. If

$$\frac{j-1}{\varphi\left(p^n\right)-1} < s < t \leq \frac{j}{\varphi\left(p^n\right)-1}$$

then by (1)

$$\begin{aligned}\left|\mathsf{Kl}_{p^n}(t;(a,b_0)) - \mathsf{Kl}_{p^n}(s;(a,b_0))\right| &= \left|\alpha_j\left((a,b_0);p^n\right)\right|(t-s)\\ &\leq \frac{\varphi\left(p^n\right)-1}{p^{n/2}}(t-s)\\ &\leq 2\sqrt{t-s}\end{aligned}$$

by (14) and (2). If

$$\frac{j-2}{\varphi\left(p^n\right)-1} \leq s \leq \frac{j-1}{\varphi\left(p^n\right)-1} \leq t \leq \frac{j}{\varphi\left(p^n\right)-1}$$

where $2 \leq j \leq \varphi\left(p^n\right)-1$ then

$$\begin{aligned}\left|\mathsf{Kl}_{p^n}(t;(a,b_0)) - \mathsf{Kl}_{p^n}(s;(a,b_0))\right| \leq\ &\left|\mathsf{Kl}_{p^n}(t;(a,b_0)) - z_j\left((a,b_0);p^n\right)\right|\\ &+ \left|z_j\left((a,b_0);p^n\right) - \mathsf{Kl}_{p^n}(s;(a,b_0))\right|.\end{aligned}$$

The first term is less than

$$\left|\alpha_j\left((a,b_0);p^n\right)\right|\left(t - \frac{j-1}{\varphi\left(p^n\right)-1}\right)$$

whereas the second term is less than

$$\left|\alpha_{j-1}\left((a,b_0);p^n\right)\right|\left(\frac{j-1}{\varphi\left(p^n\right)-1} - s\right)$$

which leads to

$$\left|\mathsf{Kl}_{p^n}(t;(a,b_0)) - \mathsf{Kl}_{p^n}(s;(a,b_0))\right| \leq 2\sqrt{t-s}$$

by (2).

This ensures the result. □

Lemma 4.3. — *Let $n \geq 2$ be a fixed integer, b_0 be a fixed non-zero integer and $\alpha \geq 1$. If*

$$t - s \geq \frac{1}{\varphi\left(p^n\right)-1}$$

then

$$\frac{1}{\varphi(p^n)} \sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} |\mathsf{Kl}_{p^n}(t;(a,b_0)) - \mathsf{Kl}_{p^n}(s;(a,b_0))|^\alpha \ll (t-s)^{\alpha/2} + \frac{1}{\varphi(p^n)} \sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \left|\widetilde{\mathsf{Kl}_{p^n}}(t;(a,b_0)) - \widetilde{\mathsf{Kl}_{p^n}}(s;(a,b_0))\right|^\alpha . \tag{15}$$

Proof of Lemma 4.3. — By (5),

$$\left|\mathsf{Kl}_{p^n}(x;(a,b_0)) - \widetilde{\mathsf{Kl}_{p^n}}(x;(a,b_0))\right| \leq \frac{6}{p^{n/2}}$$

for any $0 \leq x \leq 1$ and any a in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Thus, the left-hand side of (15) is bounded by

$$\frac{1}{\varphi(p^n)} \sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \left|\widetilde{\mathsf{Kl}_{p^n}}(t;(a,b_0)) - \widetilde{\mathsf{Kl}_{p^n}}(s;(a,b_0))\right|^\alpha + O_\alpha\left(\frac{1}{p^n}\right)^{\alpha/2}$$

which implies the result by the assumption on $t-s$. □

For $0 \leqslant s,t \leqslant 1$, we define

$$j = \lceil(\varphi(p^n)-1)s\rceil \quad \text{and} \quad k = \lceil(\varphi(p^n)-1)t\rceil \tag{16}$$

such that

$$\frac{j-1}{\varphi(p^n)-1} < s \leq \frac{j}{\varphi(p^n)-1} \quad \text{and} \quad \frac{k-1}{\varphi(p^n)-1} < t \leq \frac{k}{\varphi(p^n)-1}. \tag{17}$$

These notations will be used in the proofs of Lemma 4.4, Lemma 4.5 and Lemma 4.6.

Lemma 4.4. — *Let $n \geq 2$ be a fixed integer, b_0 be a fixed non-zero integer and $\alpha \geq 1$. If*

$$\frac{1}{\varphi(p^n)-1} \leq t-s \leq \frac{1}{p^{n/2+\delta}}$$

where $0 < \delta < n/2$ then

$$\frac{1}{\varphi(p^n)} \sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} |\mathsf{Kl}_{p^n}(t;(a,b_0)) - \mathsf{Kl}_{p^n}(s;(a,b_0))|^\alpha \ll (t-s)^{\alpha/2} + (t-s)^{\alpha\delta/n}.$$

Proof of Lemma 4.4. — Recall (16) and (17). By (3), one trivially gets

$$\left|\widetilde{\mathsf{Kl}_{p^n}}(t;(a,b_0)) - \widetilde{\mathsf{Kl}_{p^n}}(s;(a,b_0))\right| \leq \frac{|\mathcal{I}_{s,t}|}{p^{n/2}}$$

where $\mathcal{I}_{s,t}$ is the non-empty interval in $\mathbb{Z}$ given by

$$(x_j(s) = \varphi(p^n)\, s + j - 1\ ,\ x_k(t) = \varphi(p^n)\, t + k - 1]\,. \tag{18}$$

Its length satisfies

$$\begin{aligned}|\mathcal{I}_{s,t}| &= \lfloor x_k(t)\rfloor - \lceil x_j(s)\rceil\\ &\leq \varphi(p^n)(t-s) + \lceil(\varphi(p^n)-1)t\rceil - \lceil(\varphi(p^n)-1)s\rceil\\ &\leq 4(\varphi(p^n)-1)(t-s)+1\\ &\leq 8(\varphi(p^n)-1)(t-s)\end{aligned}\tag{19}$$

since $(\varphi(p^n)-1)(t-s)\geq 1$. Thus,

$$\left|\widetilde{\mathsf{Kl}_{p^n}}(t;(a,b_0)) - \widetilde{\mathsf{Kl}_{p^n}}(s;(a,b_0))\right| \leq 8p^{-\delta}.$$

This implies the desired result by Lemma 4.3. □

We recall the definitions of the constants γ_1 and γ_2 from Proposition 3.1.

Lemma 4.5. — *Let $n\geq 31$ be a fixed integer, b_0 be a fixed non-zero integer and $\alpha\geq 1$. If*

$$\frac{1}{p^{n/2+\delta}} \leq t-s \leq \frac{1}{p^{n/2-\delta}}$$

where $0<\delta\leq \min(\gamma_2 n/16, n/2-15)$ then

$$\frac{1}{\varphi(p^n)}\sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} |\mathsf{Kl}_{p^n}(t;(a,b_0)) - \mathsf{Kl}_{p^n}(s;(a,b_0))|^\alpha \ll (t-s)^{\alpha/2} + (t-s)^{\alpha\delta/(n/2+\delta)}.$$

Proof of Lemma 4.5. — Recall (16) and (17). Once again,

$$\widetilde{\mathsf{Kl}_{p^n}}(t;(a,b_0)) - \widetilde{\mathsf{Kl}_{p^n}}(s;(a,b_0)) = \frac{1}{p^{n/2}}\sum_{x\in\mathcal{I}_{s,t}} e_{p^n}(ax+b_0\overline{x})$$

by (3) for any a in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ and where $\mathcal{I}_{s,t}$ is given by (18). According to (19) for its length $|\mathcal{I}_{s,t}|$ we have

$$p^{n/2+\delta} \gg |\mathcal{I}_{s,t}| \gg p^{n/2-\delta}.$$

By Corollary 3.3,

$$\left|\widetilde{\mathsf{Kl}_{p^n}}(t;(a,b_0)) - \widetilde{\mathsf{Kl}_{p^n}}(s;(a,b_0))\right| \ll \left(\frac{1}{p^n}\right)^{\delta/n} \ll (t-s)^{\frac{\delta}{n/2+\delta}}$$

for any a in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, which implies the result. □

Lemma 4.6. — *Let $n\geq 2$ be a fixed integer, b_0 be a fixed non-zero integer and α be a non-zero even integer. If*

$$\frac{1}{p^{n/2-\delta}} \leq t-s \leq 1$$

where $0 < \delta < n/2$ *then*

$$\frac{1}{\varphi(p^n)} \sum_{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \left|\mathsf{Kl}_{p^n}(t;(a,b_0)) - \mathsf{Kl}_{p^n}(s;(a,b_0))\right|^\alpha \ll (t-s)^{\alpha/2} + (t-s)^{1+\delta/(n/2-\delta)-\varepsilon}$$

for any $\varepsilon > 0$.

Proof of Lemma 4.6. — Let us define for any $0 \leq x \leq 1$ the random variables

$$\mathsf{Kl}_{p^n}\left(x; \frac{p^n-1}{2}; *\right) := \frac{1}{p^{n/2}} \sum_{|h| \leq (p^n-1)/2} \alpha_{p^n}(h;x) U_h(*).$$

Recall that each random variable U_h, $h \in \mathbb{Z}$, is 4-subgaussian since it is centered and bounded by 2 (see [1, Proposition B.6.2]). It turns out that for any real number u,

$$\mathbb{E}\left(e^{u\left(\mathsf{Kl}_{p^n}\left(t;\frac{p^n-1}{2};*\right) - \mathsf{Kl}_{p^n}\left(s;\frac{p^n-1}{2};*\right)\right)}\right) = \prod_{|h| \leq (p^n-1)/2} \mathbb{E}\left(e^{u\frac{\alpha_{p^n}(h;t)-\alpha_{p^n}(h;s)}{p^{n/2}} U_h(*)}\right) \leq \prod_{|h| \leq (p^n-1)/2} e^{\frac{4\left|\alpha_{p^n}(h;t)-\alpha_{p^n}(h;s)\right|^2}{p^n} u^2/2}$$

by the independence of the random variables U_h, $h \in \mathbb{Z}$. Thus, by definition, the random variable $\mathsf{Kl}_{p^n}\left(t; \frac{p^n-1}{2}; *\right) - \mathsf{Kl}_{p^n}\left(s; \frac{p^n-1}{2}; *\right)$ is σ_{p^n}-subgaussian, where

$$\sigma_{p^n}^2 = \frac{4}{p^n} \sum_{|h| \leq (p^n-1)/2} \left|\alpha_{p^n}(h;t) - \alpha_{p^n}(h;s)\right|^2.$$

Consequently,

$$\mathbb{E}\left(\left|\mathsf{Kl}_{p^n}\left(t; \frac{p^n-1}{2}; *\right) - \mathsf{Kl}_{p^n}\left(s; \frac{p^n-1}{2}; *\right)\right|^\alpha\right) \leq c_\alpha \sigma_{p^n}^\alpha$$

for some positive constant c_α by [1, Proposition B.6.3].

Recall (16) and (17). By (4) and the discrete Plancherel formula,

$$\sigma_{p^n}^2 = \frac{4}{p^n} |\mathcal{I}_{s,t}|$$

where $\mathcal{I}_{s,t}$ is the non-empty interval in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ given by (18) whose length satisfies (19). Thus,

$$\mathbb{E}\left(\left|\mathsf{Kl}_{p^n}\left(t; \frac{p^n-1}{2} *\right) - \mathsf{Kl}_{p^n}\left(s; \frac{p^n-1}{2}; *\right)\right|^\alpha\right) \leq 32^{\alpha/2} c_\alpha (t-s)^{\alpha/2}. \tag{20}$$

The same method of proof than the one used in [5, Proposition 4.1] entails that

$$\begin{aligned}\frac{1}{\varphi(p^n)} &\sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\left|\widetilde{\mathsf{Kl}_{p^n}}(t;(a,b_0))-\widetilde{\mathsf{Kl}_{p^n}}(s;(a,b_0))\right|^\alpha \\ &=\mathbb{E}\left(\left|\mathsf{Kl}_{p^n}\left(t;\frac{p^n-1}{2};*\right)-\mathsf{Kl}_{p^n}\left(s;\frac{p^n-1}{2};*\right)\right|^\alpha\right)+O\left(\frac{\log^\alpha(p^n)}{p^{n/2}}\right) \\ &\ll (t-s)^{\alpha/2}+(t-s)^{1+\delta/(n/2-\delta)-\varepsilon}\end{aligned}$$

by (20) for any $\varepsilon>0$. See [5, Page 322] for more details.

One can apply Lemma 4.3 to conclude the proof. □

Proof of Proposition 4.1. — Obviously, one can assume that

$$0\le s<t\le 1.$$

Let δ be any real number satisfying

$$0<\delta\le\min(\gamma_2 n/16, n/2-15)$$

and α be any even integer satisfying

$$\alpha>\max\left(\frac{n}{\delta},\frac{n/2+\delta}{\delta}\right).$$

Let us define

$$\beta=\min\left(\frac{\alpha}{2},\frac{\alpha\delta}{n},2,\frac{\delta\alpha}{n/2+\delta},1+\frac{\delta}{n/2-\delta}\right)-1>0$$

and let us prove that

$$\frac{1}{\varphi(p^n)}\sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\left|\mathsf{Kl}_{p^n}(t;(a,b_0))-\mathsf{Kl}_{p^n}(s;(a,b_0))\right|^\alpha\ll_{\alpha,\delta,n,\varepsilon}|t-s|^{1+\beta-\varepsilon}$$

for any $\varepsilon>0$.

By Lemmas 4.2, 4.4 and 4.5,

$$\frac{1}{\varphi(p^n)}\sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\left|\mathsf{Kl}_{p^n}(t;(a,b_0))-\mathsf{Kl}_{p^n}(s;(a,b_0))\right|^\alpha\ll|t-s|^{1+\beta}$$

provided that

$$0\le t-s\le\frac{1}{p^{n/2-\delta}}.$$

Let us assume from now on that

$$\frac{1}{p^{n/2-\delta}} \leq t-s \leq 1.$$

By Lemma 4.6,

$$\frac{1}{\varphi\left(p^n\right)} \sum_{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \left|\mathsf{Kl}_{p^n}(t;(a,b_0)) - \mathsf{Kl}_{p^n}(s;(a,b_0))\right|^\alpha$$
$$\ll_\alpha \left((t-s)^{\alpha/2} + (t-s)^{1+\delta/(n/2-\delta)-\epsilon}\right) \ll_\epsilon (t-s)^{1+\beta-\epsilon}. \qquad \square$$

5. Proof of Theorems 1.1 and 1.2

Theorem 1.2 follows from Proposition 4.1 by Kolmogorov's criterion for tightness (see [5, Proposition A.1]).

Remark 5.1. — The proof of tightness in [3, Lemma 3.2] has a small mistake at the end, since the authors use the uniform bound

$$\widetilde{L}_p(t;\omega) \ll \log(p)$$

to uniformize the exponent α across different estimates in order to apply Kolmogorov's criterion for tightness (see [5, Proposition A.1]). This introduces an overlooked dependency on p when $t-s$ is close to 1. One can correct this problem either arithmetically (as done in the present paper) by showing that one can take α to be a sufficiently large even integer, or (as suggested by E. Kowalski) by proving a generalization of Kolmogorov's tightness criterion that involves different exponents α in different ranges.

Theorem 1.1 follows from Theorem 1.2 and [5, Theorem A] by Prokhorov's criterion for the convergence in law (see [5, Theorem A.3]).

Acknowlegments. — The authors would like to thank E. Kowalski for sharing with us his enlightening lecture notes [1] and for helping them with Lemma 4.6 especially when $s-t$ is very close to 1.

The first and second authors are financed by the ANR Project Flair ANR-17-CE40-0012.

The third author is partially supported by the Australian research council grant DP170100786.

Last but not least, the authors would like to thank the anonymous referee for a careful reading of the manuscript, for suggesting Corollary 3.2, and for pointing out a naive mistake in a previous version of Corollary 3.3. These comments made the manuscript more readable.

BIBLIOGRAPHY

[1] E. Kowalski. Arithmetic randonnée. An introduction to probabilistic number theory. Preprint, 2016. Available at `https://people.math.ethz.ch/~kowalski/probabilistic-number-theory.pdf`.

[2] M. A. Korolev – "Short Kloosterman sums to powerful modulus", *Dokl. Math.* **94** (2016), no. 2, p. 561–562.

[3] E. Kowalski & W. F. Sawin – "Kloosterman paths and the shape of exponential sums", *Compos. Math.* **152** (2016), no. 7, p. 1489–1516.

[4] D. Lorenzini – *An invitation to arithmetic geometry*, Amer. Math. Soc., 1996.

[5] G. Ricotta & E. Royer – "Kloosterman paths of prime powers moduli", *Comment. Math. Helv.* **93** (2018), no. 3, p. 493–532.