Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 93 (2018)
Heft: 3

Artikel: Kloosterman paths of prime powers moduli
Autor: Ricotta, Guillaume / Henriot, Kevin
DOI: https://doi.org/10.5169/seals-787375

Comment. Math. Helv. 93 (2018), 493–532
DOI 10.4171/CMH/442

Commentarii Mathematici Helvetici

Kloosterman paths of prime powers moduli

Guillaume Ricotta and Emmanuel Royer

In memory of Kevin Henriot

Abstract. In [12], the authors proved, using a deep independence result of Kloosterman sheaves, that the polygonal paths joining the partial sums of the normalized classical Kloosterman sums $S(a, b_0; p)/p^{1/2}$ converge in the sense of finite distributions to a specific random Fourier series, as a varies over $(\mathbb{Z}/p\mathbb{Z})^\times$, b_0 is fixed in $(\mathbb{Z}/p\mathbb{Z})^\times$ and p tends to infinity among the odd prime numbers. This article considers the case of $S(a, b_0; p^n)/p^{n/2}$, as a varies over $(\mathbb{Z}/p^n\mathbb{Z})^\times$, b_0 is fixed in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, p tends to infinity among the odd prime numbers and $n \geq 2$ is a fixed integer. A convergence in law in the Banach space of complex-valued continuous function on $[0, 1]$ is also established, 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 in [12] in the prime moduli case.

Mathematics Subject Classification (2010). 11T23, 11L05, 60F17, 60G17, 60G50.

Keywords. Kloosterman sums, moments, random Fourier series, probability in Banach spaces.

1. Introduction and statement of the results

The shape of the path induced by various partial exponential sums has been considered by many people since the seventies. See for instance [13], [14] for the case of Gauß sums, [15] for polynomial exponential sums of higher degree, [2], [1] and [4] for the case of character sums. Very recently, E. Kowalski and W. Sawin successfully investigated the case of partial Kloosterman sums of prime moduli in [12]. The main purpose of this work is to consider the case of partial Kloosterman sums to prime power moduli and to give a probabilistic meaning to graphs like the one given in Figure 1[1].

[1]The axes are orthonormal but a rotation by $\pi/2$ has been applied to the real plot of $t \mapsto \mathrm{Kl}_{67^2}(t; (1, 1))$.

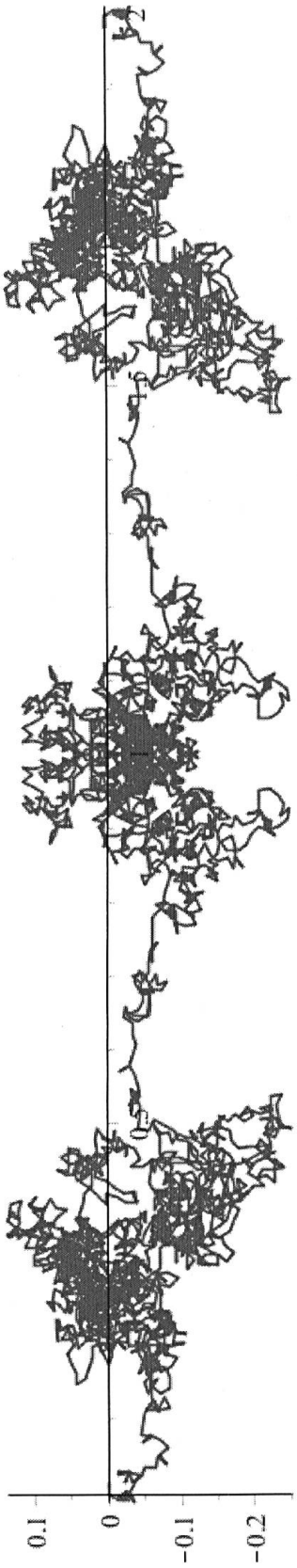

Figure 1. Plot of $t \mapsto \mathsf{Kl}_{67^2}(t;(1,1))$.

More precisely, let p be a prime number and $n \geq 1$ 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 $e(z) := \exp(2i\pi z)$ for any complex number z. 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 $J_p^n := \{j \in \{1, \ldots, p^n\}, p \nmid j\}$. If we write $J_p^n = \{j_1, \ldots, j_{\varphi(p^n)}\}$ with

$$j_1 < j_2 < \cdots < j_{\varphi(p^n)}$$

then the corresponding Kloosterman path $\gamma_{p^n}(a,b)$ is defined by

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

This is the polygonal path obtained by concatenating the closed segments

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

for j_1 and j_2 two consecutive indices in J_p^n. Finally, one defines a continuous map on the interval $[0,1]$

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

by parametrizing 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 J_p^n being parametrized linearly by an interval of length $1/(\varphi(p^n)-1)$.

For a fixed b_0 in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, the function $a \mapsto \mathsf{Kl}_{p^n}(*;(a,b_0))$ is viewed as a random variable on the probability space $(\mathbb{Z}/p^n\mathbb{Z})^\times$ 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 $C^0([0,1],\mathbb{C})$.

Remark 1.1. In particular, with our definition, $\mathsf{Kl}_{p^n}(0;(a,b))$ is defined y

$$\exists \lim_{t \to 0} \mathsf{Kl}_{p^n}(t;(a,b)) = \frac{1}{p^{n/2}} e\left(\frac{a+b}{p^n}\right) = \mathsf{Kl}_{p^n}(0;(a,b)).$$

The Kloosterman path does not start at the origin, in contrast with [12].

Let μ be the probability measure given by

$$\mu = \frac{1}{2}\delta_0 + \mu_1 \tag{1.1}$$

for the Dirac measure δ_0 at 0 and

$$\mu_1(f) = \frac{1}{2\pi}\int_{x=-2}^{2} \frac{f(x)\,\mathrm{d}x}{\sqrt{4-x^2}}$$

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

Theorem A (Convergence of finite distributions). *Let $n \geq 2$ be a fixed integer. For any odd prime number p, fix an element b_0 in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Let $(U_h)_{h\in\mathbb{Z}}$ be a sequence of independent identically distributed random variables of probability law μ defined in* (1.1) *and let* Kl *be the $C^0([0,1],\mathbb{C})$-valued random variable defined by*

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

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 the sense of finite distributions[2] *to the $C^0([0,1],\mathbb{C})$-valued random variable* Kl *as p tends to infinity among the prime numbers.*

Remark 1.2. We have chosen to parametrize the partial sums of the Kloosterman sums so that successive sums always correspond to adding one more term. This implies that partial sums at integers divisible by p are not defined. Another definition would be to define $\mathsf{Kl}_{j;p^n}(a,b)$ for all integer j and to interpolate in the usual way. The geometric path, namely the image of $t \mapsto \mathsf{Kl}_{p^n}(t;(a,b))$, would be unchanged and there is no doubt that the same results hold for this different definition.

Remark 1.3. All the main properties of the random variable Kl are given in Proposition 3.1. As already said, this theorem is the analogue of the result proved by E. Kowalski and W. Sawin in [12] when $n = 1$ for a different random Fourier series given by

$$\forall t \in [0,1], \quad K(t) := t\mathsf{ST}_0 + \sum_{h\in\mathbb{Z}^*} \frac{e(ht)-1}{2i\pi h}\mathsf{ST}_h,$$

where $(\mathsf{ST}_h)_{h\in\mathbb{Z}}$ is an independent identically distributed sequence of random variables of probability law μ_{ST}, the classical Sato-Tate measure also called the semi-circle law. The fact that K and Kl have the same analytic shape heavily depends on the completion method. The fact that K and Kl are different on a probabilistic point of view is not very surprising since $\mathsf{Kl}_{p^n}(a,b)$ is a sum over a finite field when $n = 1$, which requires deep techniques from algebraic geometry, and a character sum when $n \geq 2$, which can be computed explicitly via elementary but not so easy techniques. Thus, the fact that Kloosterman paths of prime moduli and of prime powers moduli behave differently on a probabilistic point of view is quite expected.

[2]See Appendix A for a precise definition of the convergence in the sense of finite distributions.

Remark 1.4. Nevertheless, the referee kindly informed us that both this measure μ and the random series Kl occur when dealing with the path induced by Salié sums of prime moduli. In addition, let us recall that μ_{ST} is the direct image under the trace map of the probability Haar measure on the compact group $SU_2(\mathbb{C})$ whereas, according to [8, Remark 1.2], μ is the direct image under the trace map of the probability Haar measure on the normalizer of a maximal torus in $SU_2(\mathbb{C})$.

Remark 1.5. In particular, choosing $t = 1$, Theorem A implies that the normalized Kloosterman sums $\mathrm{Kl}_{p^n}(a, b_0)$ get equidistributed in $[-2, 2]$ with respect to the measure μ, as a ranges over $(\mathbb{Z}/p^n\mathbb{Z})^\times$ and p tends to infinity among the odd prime numbers for a fixed integer $n \geq 2$ and b_0 is a fixed element in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Remark 1.6. It is worth mentioning that the proof of this theorem requires A. Weil's version of the Riemann hypothesis in one variable. See Proposition 4.8.

The function $(a, b) \mapsto \mathrm{Kl}_{p^n}(t; (a, b))$ is viewed as a $C^0([0, 1], \mathbb{C})$-valued 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. Theorem A trivially implies that the sequence of $C^0([0, 1], \mathbb{C})$-valued random variables $\mathrm{Kl}_{p^n}(*; (*, *))$ converges in the sense of finite distributions to the $C^0([0, 1], \mathbb{C})$-valued random variable Kl as p tends to infinity among the prime numbers too.

Theorem B (Convergence in law). *Let $n \geq 2$ be a fixed integer and p be an odd prime number. The sequence of $C^0([0, 1], \mathbb{C})$-valued random variables $\mathrm{Kl}_{p^n}(*; (*, *))$ on $(\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times$ converges in law[3] to the $C^0([0, 1], \mathbb{C})$-valued random variable Kl as p tends to infinity among the prime numbers.*

Remark 1.7. Once again, this theorem is the analogue of the result proved by E. Kowalski and W. Sawin in [12] when $n = 1$.

Remark 1.8. For a fixed $n \geq 2$ and a fixed b_0 in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, we expect that the sequence of $C^0([0, 1], \mathbb{C})$-valued random variables $\mathrm{Kl}_{p^n}(*; (*, b_0))$ 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 prime numbers too. Nevertheless, such result seems to be out of reach given the current technology. It relies on expected uniform non-trivial individual bounds for incomplete Kloosterman sums

$$\frac{1}{p^{n/2}} \sum_{x \in I} e\left(\frac{ax + b_0\overline{x}}{p^n}\right) \ll p^{-\delta}$$

for some $\delta > 0$ and where I is an interval of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ of length close to $p^{n/2}$. See [12, Remark 3.3] and [10, p. 52] for a discussion on such issues in the prime moduli case.

In [12], the authors deduce from their limit theorems the distribution of the maximum of the partial sums of prime moduli they consider. Their techniques would

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

lead to a straightforward analogue in the case of prime powers moduli investigated in this work.

One can mention that it seems quite natural to consider the same questions in the regime[4] p a fixed prime number and $n \geq 2$ tends to infinity. This problem, both theoretically and numerically, seems to be of completely different nature.

Finally, it makes sense to consider the distribution of paths associated to other exponential sums of prime powers moduli and to ask whether a distribution result remains true. For instance, one could be tempted to look at

$$\mathsf{K}_{p^n}(a) = \frac{1}{p^{n/2}} \sideset{}{^*}\sum_{1 \leq x \leq p^n} e\left(\frac{f_a(x)}{p^n}\right),$$

where $f_a = g_a/h_a$ with g_a and h_a in $\mathbb{Z}[x]$ depending on a parameter a modulo p^n. The symbol $*$ means that the summation is over the elements x satisfying $p \nmid h_a(x)$. These exponential sums can be computed explicitly. See [5, Lemma 12.2, Lemma 12.13] for instance. One key step would be to evaluate asymptotically

$$\frac{1}{\varphi(p^n)} \sum_{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \prod_{\tau \in \mathbb{Z}/p^n\mathbb{Z}} \mathsf{K}_{p^n}(a+\tau)^{\mu(\tau)}$$

for $\boldsymbol{\mu} = (\mu(\tau))_{\tau \in \mathbb{Z}/p^n\mathbb{Z}}$ a p^n-tuple of non-negative integers.

Organization of the paper. The explicit description of the Kloosterman paths is given in Section 2. The relevant random Fourier series, which occurs as an asymptotic process in Theorem A and Theorem B, is defined and studied in Section 3. Section 4 contains the asymptotic evaluation of the moments of the random variable $\mathsf{Kl}_{p^n}(*;(*,*))$ whereas the tightness of this sequence of random variables is established in Section 5. The proofs of Theorem A and Theorem B are completed in Section 6. A probabilistic toolbox is provided in Appendix A.

Notations. – 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 the real variable then the notations $f(p) = O_A(g(p))$ or $f(p) \ll_A g(p)$ mean that $|f(p)|$ is smaller than a "constant", which only depends on A, times $g(p)$ at least for p large enough.

– $n \geq 2$ is a fixed 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 one.

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

[4]Or even worse any intermediate regime.

– Finally, if $\mathcal{P}$ is a property then $\delta_{\mathcal{P}}$ is the Kronecker symbol, namely 1 if $\mathcal{P}$ is satisfied and 0 otherwise.

Acknowledgements. The authors would like to thank the referee for her or his unusually careful reading of the manuscript and very useful suggestions that improved the presentation of the paper.

The authors would like to thank E. Kowalski for his encouragement and for sharing with us his enlightening lectures notes [10]. They also thank F. Martin for fruitful discussions related to Proposition 4.7.

Part of this paper was worked out in Université Blaise Pascal (Clermont-Ferrand, France) in June, 2016. The first author would like to thank this institution for its hospitality and inspiring working conditions.

2. Explicit description of the Kloosterman path

Let us construct the Kloosterman path $\gamma(a,b)$ for a and b in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

We enumerate the partial Kloosterman sums and define $z_j((a,b);p^n)$ to be the jth term of $(\mathsf{Kl}_{j;p^n}(a,b))_{j\in J_p^n}$. More explicitly, we organise the partial Kloosterman sums in p^{n-1} blocks each of them containing $p-1$ successive sums. For $1\le k\le p^{n-1}$, the kth block contains $\mathsf{Kl}_{(k-1)p+1;p^n}(a,b),\dots,\mathsf{Kl}_{kp-1;p^n}(a,b)$. These sums are numbered by defining

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

It implies that the enumeration is given by

$$z_j((a,b);p^n)=\mathsf{Kl}_{j+\lfloor\frac{j-1}{p-1}\rfloor;p^n}(a,b)\qquad(1\le j<\varphi(p^n))\tag{2.1}$$

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

$$\left]z_j((a,b);p^n),z_{j+1}((a,b);p^n)\right]$$

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

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

with

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

and

$$j=\lceil(\varphi(p^n)-1)t\rceil.$$

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

$$|\alpha_j((a,b);p^n)| \leq \frac{\varphi(p^n)-1}{p^{n/2}} \tag{2.2}$$

and

$$|\mathsf{Kl}_{p^n}(t;(a,b)) - z_j((a,b);p^n)| \leq \frac{1}{p^{n/2}}. \tag{2.3}$$

3. On the relevant random Fourier series

The moments of the measure μ defined in (1.1) are given by

$$\int_{x\in\mathbb{R}} x^m \,\mathrm{d}\mu(x) = \begin{cases} 1, & \text{if } m=0, \\ \frac{\delta_{2|m}}{2}\binom{m}{m/2}, & \text{otherwise.} \end{cases} \tag{3.1}$$

Let U be a random variable of law μ on a probability space $(\Omega, \mathcal{A}, P)$. By (3.1), the value of the expectation of such random variable is 0 and its variance equals 1. In addition, μ is also the law of the random variable $-U$ since the probability measure μ is symmetric.

Let $(U_h)_{h\in\mathbb{Z}}$ be a sequence of independent random variables of law μ on a probability space $(\Omega, \mathcal{A}, P)$. One defines for t in $[0,1]$ the symmetric partial sums

$$\mathsf{Kl}_H(t;\omega) := tU_0(\omega) + \sum_{1\leq|h|\leq H} \frac{e(ht)-1}{2i\pi h} U_h(\omega)$$

for any integer $H \geq 1$ and any $\omega \in \Omega$. Let $t \in [0,1]$ and $\omega \in \Omega$. If $\mathsf{Kl}_H(t;\omega)$ has a limit when H tends to infinity, we denote by $\mathsf{Kl}(t;\omega)$ this limit, namely

$$\mathsf{Kl}(t;\omega) := tU_0(\omega) + \sum_{h\in\mathbb{Z}^*} \frac{e(ht)-1}{2i\pi h} U_h(\omega).$$

It turns out that $\mathsf{Kl}(t;\omega)$ is closely related to the set of Fourier random series, which have been intensively studied in [6].

Proposition 3.1 (Properties of the random series). *The following properties hold.*

- *For any t in $[0,1]$, the random series $\mathsf{Kl}(t;*)$ converges almost surely, hence in law.*
- *For almost all $\omega \in \Omega$, the random series $\mathsf{Kl}(*;\omega)$ is a continuous function on $[0,1]$.*
- *For any t in $[0,1]$, the Laplace transform*

$$\mathbb{E}\left(e^{\lambda\Re(\mathsf{Kl}(t;*))+\mu\Im(\mathsf{Kl}(t;*))}\right)$$

is well-defined for all non-negative integers λ and μ. In particular, $\mathsf{Kl}(*;\omega)$ has moments of all orders.

- *Finally, for any t in $[0,1]$,*

$$\|\mathsf{Kl}_H(t;*)\|_\infty \ll \log(H) \tag{3.2}$$

and

$$|\mathbb{E}(|\mathsf{Kl}(t;*) - \mathsf{Kl}_H(t;*)|)| \ll H^{-1/2} \tag{3.3}$$

for any $H \geq 1$.

Remark 3.2. In particular, the map

$$\begin{array}{rccccc} \mathsf{Kl}: & (\Omega, \mathcal{A}, P) & \to & (C^0([0,1],\mathbb{C}), \|.\|_\infty) & & \\ & & & \mathsf{Kl}(*;\omega): & [0,1] & \to & \mathbb{C} \\ & \omega & \mapsto & & t & \mapsto & \mathsf{Kl}(t;\omega) \end{array}$$

defines a random variable on the probability space $(\Omega, \mathcal{A}, P)$ with values in the Banach space of continuous complex-valued functions on the segment $[0,1]$ endowed with the supremum norm $\|.\|_\infty$.

Remark 3.3. The proof is omitted since it is very close to the proof of [12, Proposition 2.1]. The reader may have a look at [10, Section 4] too.

4. Asymptotics of complex moments

In this section, b_0 is a *fixed* element in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Let $k \geq 1$ be a fixed integer, $\boldsymbol{t} = (t_1, \ldots, t_k)$ be a fixed k-tuple of elements in $[0,1]$ with $t_1 < \cdots < t_k$, $\boldsymbol{n} = (n_1, \ldots, n_k)$ and $\boldsymbol{m} = (m_1, \ldots, m_k)$ be two fixed k-tuples of non-negative integers. Let us define

$$\ell(\boldsymbol{m} + \boldsymbol{n}) := \sum_{i=1}^{k} (m_i + n_i).$$

The purpose of this section is to find an asymptotic formula for the complex moments defined by

$$\mathsf{M}_{p^n}(\boldsymbol{t}; \boldsymbol{m}, \boldsymbol{n}; b_0) := \frac{1}{\varphi(p^n)} \sum_{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \prod_{i=1}^{k} \overline{\mathsf{Kl}_{p^n}(t_i;(a,b_0))}^{m_i} \mathsf{Kl}_{p^n}(t_i;(a,b_0))^{n_i}. \tag{4.1}$$

The following proposition describes the asymptotic expansion of these moments. Its proof will be given at the very end of this section since it requires a series of intermediate results.

Proposition 4.1 (Asymptotic expansion of the moments). *If*

$$p > \max\left(\ell(\boldsymbol{m}+\boldsymbol{n}), 2n-5\right) \tag{4.2}$$

then

$$\mathsf{M}_{p^n}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n},b_0) = \mathbb{E}\Big(\prod_{i=1}^{k}\overline{\mathsf{Kl}(t_i;*)}^{m_i}\mathsf{Kl}(t_i;*)^{n_i}\Big) + O_{\ell(\boldsymbol{m}+\boldsymbol{n}),\epsilon}\Big(\log^{\ell(\boldsymbol{m}+\boldsymbol{n})}(p^n)\big(p^{-\frac{4(n-1)}{2^n}+\epsilon}+p^{-1/2}\big)\Big)$$

for any $\epsilon > 0$ and where the implied constant only depends on $\ell(\boldsymbol{m}+\boldsymbol{n})$ and ϵ.

For a in $(\mathbb{Z}/p^n\mathbb{Z})^\times$, let us define a step function on the segment $[0,1]$ by, for any $k \in \{1,\dots,p^{n-1}\}$,

$$\forall t \in \left(\frac{k-1}{p^{n-1}}, \frac{k}{p^{n-1}}\right], \quad \widetilde{\mathsf{Kl}_{p^n}}(t;(a,b_0)) := \frac{1}{p^{n/2}}\sideset{}{^\times}\sum_{1\le x\le x_k(t)} e_{p^n}(ax+b_0\overline{x}), \tag{4.3}$$

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 $1 \le k \le p^{n-1}$,

$$\forall t \in \left(\frac{k-1}{p^{n-1}}, \frac{k}{p^{n-1}}\right], \quad \alpha_{p^n}(h;t) := \frac{1}{p^{n/2}}\sum_{1\le x\le x_k(t)} e_{p^n}(hx). \tag{4.4}$$

These coefficients are nothing else than the discrete Fourier coefficients of the finite union of intervals given by $1 \le x \le x_k(t)$ with $(p,x)=1$ for $1 \le k \le p^{n-1}$. All their useful properties are encapsulated in the following lemma.

Lemma 4.2 (The completion method).

- *For H_{p^n} any complete system of residues modulo p^n,*

$$\widetilde{\mathsf{Kl}_{p^n}}(t;(a,b_0)) = \frac{1}{p^{n/2}}\sum_{h\in H_{p^n}} \alpha_{p^n}(h;t)\,\mathsf{Kl}_{p^n}(a-h,b_0). \tag{4.5}$$

- *For any integer h and any real number $t \in [0,1]$,*

$$\alpha_{p^n}(h;t) \le p^{n/2} \times \begin{cases} 1, & \text{if } h=0,\\ \frac{1}{2|h|}, & \text{if } |h| \le (p^n-1)/2 \text{ and } h \ne 0. \end{cases} \tag{4.6}$$

- *For any integer h and any real number $t \in [0,1]$,*

$$\frac{1}{p^{n/2}}\alpha_{p^n}(h;t) = \beta(h;t) + O\Big(\frac{1}{p^n}\Big), \tag{4.7}$$

where

$$\beta(h;t) = \begin{cases} t, & \text{if } h = 0, \\ \frac{e(ht)-1}{2i\pi h}, & \text{otherwise.} \end{cases}$$

Remark 4.3. The proof is omitted since it is very close to the proof of [12, Lemma 2.3, Proposition 2.4]. The reader may have a look at [10, Section 4] too.

Let us also define the corresponding moment

$$\widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n};b_0) := \frac{1}{\varphi(p^n)} \sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \prod_{i=1}^{k} \overline{\widetilde{\mathsf{Kl}_{p^n}}(t_i;(a,b_0))}^{m_i} \widetilde{\mathsf{Kl}_{p^n}}(t_i;(a,b_0))^{n_i}. \tag{4.8}$$

The following lemma reveals that it is enough to prove an asymptotic formula for $\widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n};b_0)$.

Lemma 4.4 (Approximation of the moments). *One has*

$$\mathsf{M}_{p^n}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n};b_0) = \widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n};b_0) + O\left(\frac{\log^{\ell(\boldsymbol{m}+\boldsymbol{n})}(p^n)}{p^{n/2}}\right).$$

Remark 4.5. The proof is omitted but relies on Lemma 4.2, which implies that

$$\sum_{h\in H_{p^n}} |\alpha_{p^n}(h;t)| \le 4p^{n/2}\log(p^n) \tag{4.9}$$

for $H_{p^n} = \{(1-p^n)/2,\dots,(p^n-1)/2\}$, which is admissible since p is odd, and is close to the proof of [12, Proposition 2.4]. The reader may have a look at [10, Section 4] too. Note that both Lemma 4.7 and (4.9) entail that

$$|\mathsf{Kl}_{p^n}(t;(a,b)) - \widetilde{\mathsf{Kl}_{p^n}}(t;(a,b))| \le \frac{6}{p^{n/2}} \tag{4.10}$$

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

The crucial ingredient in the proof of Proposition 4.1 is the asymptotic evaluation of the complete sums of products of shifted Kloosterman sums $\mathsf{S}_{p^n}(\boldsymbol{\mu};b_0)$ defined by

$$\mathsf{S}_{p^n}(\boldsymbol{\mu};b_0) := \frac{1}{\varphi(p^n)} \sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \prod_{\tau\in\mathbb{Z}/p^n\mathbb{Z}} \mathsf{Kl}_{p^n}(a+\tau,b_0)^{\mu(\tau)} \tag{4.11}$$

for $\boldsymbol{\mu} = (\mu(\tau))_{\tau\in\mathbb{Z}/p^n\mathbb{Z}}$ a sequence of p^n-tuples of non-negative integers different from the 0-tuple.

The following notations will be used throughout this section. Let us define for such sequence $\boldsymbol{\mu}$

$$\mathsf{T}(\boldsymbol{\mu}) := \{\tau \in \mathbb{Z}/p^n\mathbb{Z}, \mu(\tau) \ge 1\} \subset \mathbb{Z}/p^n\mathbb{Z},$$
$$\overline{\mathsf{T}}(\boldsymbol{\mu}) := \{\tau \bmod p, \tau \in \mathsf{T}(\boldsymbol{\mu})\} \subset \mathbb{Z}/p\mathbb{Z}.$$

Let $\mathsf{B}_{p^n}(\boldsymbol{\mu})$ be the subset of the $|\mathsf{T}(\boldsymbol{\mu})|$-tuples $\boldsymbol{b} = (b_\tau)_{\tau\in\mathsf{T}(\boldsymbol{\mu})}$ of integers in $\{1,\dots,(p-1)/2\}$ satisfying

$$\forall(\tau,\tau')\in\mathsf{T}(\boldsymbol{\mu})^2,\quad b_\tau^2-\tau\equiv b_{\tau'}^2-\tau' \bmod p \tag{4.12}$$

and

$$\forall\tau\in\mathsf{T}(\boldsymbol{\mu}),\quad p\nmid b_\tau^2-\tau. \tag{4.13}$$

Let $\boldsymbol{\ell}=(\ell_\tau)_{\tau\in\mathsf{T}(\boldsymbol{\mu})}$ be a $|\mathsf{T}(\boldsymbol{\mu})|$-tuple of integers. For any integer j in $\{1,\dots,n-1\}$, let us define

$$m_{\boldsymbol{b},\boldsymbol{\ell}}(j,j)=\sum_{\tau\in\mathsf{T}(\boldsymbol{\mu})}\ell_\tau\overline{b_\tau}^{2j-1} \tag{4.14}$$

and the the following associated object

$$\mathsf{N}(\boldsymbol{\mu},\boldsymbol{\ell};w):=\sum_{\substack{\boldsymbol{b}\in\mathsf{B}_{p^n}(\boldsymbol{\mu}),\ m_{\boldsymbol{b},\boldsymbol{\ell}}(1,1)\equiv w \bmod p\\ \forall j\in\{2,\dots,n-1\},\ m_{\boldsymbol{b},\boldsymbol{\ell}}(j,j)\equiv 0 \bmod p}}1 \tag{4.15}$$

for any w modulo p.

Finally, let

$$\mathsf{A}_{p^n}(\boldsymbol{\mu}):=\left\{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times,\forall\tau\in\mathsf{T}(\boldsymbol{\mu}),a+\tau\in((\mathbb{Z}/p^n\mathbb{Z})^\times)^2\right\}. \tag{4.16}$$

Firstly, let us prove and recall some useful facts related to Kloosterman sums of prime powers moduli.

Lemma 4.6 (Kloosterman sums of prime powers moduli). *Let p be an odd prime number satisfying $p\geq 2n-5$ and a be an integer.*

- *If a is divisible by p or a is not a square modulo p then $\mathsf{Kl}_{p^n}(a,1)=0$.*
- *If a is a non-zero square modulo p then*

$$\mathsf{Kl}_{p^n}(a,1)=2\Big(\frac{s}{p^n}\Big)\cos\Big(\frac{4\pi s}{p^n}+\theta_{p^n}\Big),$$

where

$$\theta_{p^n}=\begin{cases}0, & \text{if } 2\mid n \text{ or } p\equiv 1 \bmod 4,\\ \pi/2, & \text{if } 2\nmid n \text{ and } p\equiv 3 \bmod 4,\end{cases}$$

and s is any solution of

$$s^2\equiv a \bmod p^n.$$

- *The bound*

$$|\mathsf{Kl}_{p^n}(a,1)|\leq 2 \tag{4.17}$$

holds.

- *Let a be a non-zero square modulo p. There exists some integers $c'_0, \dots, c'_{n-1}$ satisfying*

$$\forall m \in \{0, \dots, n-1\}, \qquad c'_m \neq 0 \quad \text{and} \quad v_p(c'_m) = 0 \tag{4.18}$$

and some integers k and $b \in \{0, \dots, (p-1)/2\}$ depending on a and p so that

$$s_{a,p^n} = b \sum_{m=0}^{n-1} c'_m \bar{b}^{2m} p^m k^m \tag{4.19}$$

is a solution of $s^2 \equiv a \bmod p^n$, where $\bar{b}$ stands for the inverse of b modulo p^n.

Proof of Lemma 4.6. The three first items are standard. See [5, Ch. 12, Eq. (12.39)]. In particular, recall that a is a non-zero square modulo p is equivalent to saying that a is a non-zero square modulo p^n.

Let us consider the last one. The elements of $((\mathbb{Z}/p\mathbb{Z})^\times)^2$ are given by

$$b^2, \quad 1 \leq b \leq (p-1)/2.$$

Thus,

$$a \equiv b^2 \bmod p$$

for some $1 \leq b = b_{a,p} \leq (p-1)/2$ so that

$$a = b^2 + pk$$

for some $k = k_{a,b,p}$ in $\mathbb{Z}$. The congruence to be solved becomes

$$s^2 \equiv a = b^2 + pk \equiv b^2(1 + \bar{b}^2 pk) \bmod p^n$$

where $\bar{b}$ stands for a representative of the inverse of b modulo p^n. Let us define the p-adic integers[5] $c_0 = 1, c_1 = 1/2$ and

$$\forall m \geq 2, \quad c_m := \frac{(-1)^{m-1}(2m-3)!}{2^{2(m-1)} m!(m-2)!} = \frac{1/2(1/2-1)\dots(1/2-m+1)}{m!}.$$

Obviously,

$$\forall m \geq 1, \quad c_m = -\frac{2m-3}{2m} c_{m-1}$$

so that

$$\forall m \in \{0, \dots, n-1\}, \quad v_p(c_m) = 0 \tag{4.20}$$

since $p \geq 2n-5$. If $x \in p\mathbb{Z}_p$ then, by [9, Chapter IV.1], the power series

$$\sum_{m \geq 0} c_m x^m \in \mathbb{Z}_p[\![x]\!]$$

[5]Recall that the prime p is odd.

converges in the p-adic norm to a square root of $1+x$. As a consequence, one has

$$s \equiv b \sum_{m=0}^{n-1} c'_m \bar{b}^{2m} p^m k^m \bmod p^n,$$

where the coefficients c'_m are some integers satisfying $c'_0 = 1$, and

$$\forall m \geq 1, \quad c'_m \equiv c_m \bmod p^n, \quad 0 \leq c'_m < p^n.$$

In particular, if $0 \leq m \leq n-1$, then

$$c'_m \neq 0 \quad \text{and} \quad v_p(c'_m) = v_p(c_m) = 0$$

by (4.20). □

The following proposition contains the upper-bound for $\mathsf{N}(\boldsymbol{\mu}, \boldsymbol{\ell}; w)$ defined in (4.15).

Proposition 4.7 (A counting argument). *Let $\boldsymbol{\mu} = (\mu(\tau))_{\tau \in \mathbb{Z}/p^n\mathbb{Z}}$ be a sequence of p^n-tuples of non-negative integers satisfying $|\mathsf{T}(\boldsymbol{\mu})| = |\overline{\mathsf{T}}(\boldsymbol{\mu})|$ and $\boldsymbol{\ell}$ a $|\mathsf{T}(\boldsymbol{\mu})|$-tuple of integers satisfying*

$$\forall \tau \in \mathsf{T}(\boldsymbol{\mu}), \quad |\ell_\tau| < p$$

and $\boldsymbol{\ell} \neq \mathbf{0}$. One uniformly has

$$\mathsf{N}(\boldsymbol{\mu}, \boldsymbol{\ell}; w) \ll_{|\mathsf{T}(\boldsymbol{\mu})|} 1$$

for any $w \bmod p$ where the implied constant only depends on $|\mathsf{T}(\boldsymbol{\mu})|$.

Proof of Proposition 4.7. Let $k := |\mathsf{T}(\boldsymbol{\mu})|$ for simplicity.

Let us assume that $k = 1$. In this case, $\mathsf{T}(\boldsymbol{\mu}) = \{\tau_0\}$ and one has

$$\ell_{\tau_0} \overline{b_{\tau_0}} = m_{\boldsymbol{b},\boldsymbol{\ell}}(1,1) \equiv w \bmod p,$$

which fixes the value of b_{τ_0} since ℓ_{τ_0} is coprime with p.

Let us assume from now on that $k \geq 2$. One has

$$\mathsf{N}(\boldsymbol{\mu}, \boldsymbol{\ell}; w) = \sum_{\substack{c \bmod p, \\ (p,c)=1}} \sum_{\substack{\boldsymbol{b} \in \mathsf{B}_{p^n}(\boldsymbol{\mu}),\, m_{\boldsymbol{b}}(1,1) \equiv w \bmod p \\ \forall j \in \{2,\dots,n-1\},\, m_{\boldsymbol{b}}(j,j) \equiv 0 \bmod p \\ \forall \tau \in \mathsf{T}(\boldsymbol{\mu}),\, b_\tau^2 \equiv c+\tau \bmod p}} 1. \tag{4.21}$$

Note that for a fixed c, there is at most one tuple $\boldsymbol{b}$ since their coordinates satisfy the given quadratic equations modulo p. The basic idea to show that there is a bounded number of integers c modulo p is to find a polynomial, which vanishes on these c's and whose degree only depends on k.

Let us consider the polynomial

$$Q(\boldsymbol{a}; X) = \prod_{\boldsymbol{\epsilon}=(\epsilon_\tau)_{\tau\in\mathsf{T}(\boldsymbol{\mu})}\in\{\pm 1\}^k} \left(X - \sum_{\tau\in\mathsf{T}(\boldsymbol{\mu})} \epsilon_\tau a_\tau\right) \in \mathbb{F}_p[\boldsymbol{a}, X]$$

in the variables a_τ, $\tau \in \mathsf{T}(\boldsymbol{\mu})$, and X.

This polynomial can be written as

$$Q(\boldsymbol{a}; X) = \sum_{i=0}^{2^{k-1}} Q_i(\boldsymbol{a}) X^{2i} + X^{2^k}$$

where $Q_i \in \mathbb{F}_p[\boldsymbol{a}]$ is a homogeneous polynomial of degree $2^k - 2i$ for $0 \le i \le 2^{k-1}$, which only involves even powers of a_i ($0 \le i \le k$). The fact that only even powers of X occur easily follows from the fact that if $\boldsymbol{\epsilon}$ belongs to $\{\pm 1\}^k$ then so does $-\boldsymbol{\epsilon}$. The fact that each monomial only contains even powers of a_i for $1 \le i \le k$ is due to the obvious invariance property given by

$$\forall \boldsymbol{\epsilon} \in \{\pm 1\}^k, \quad Q(\boldsymbol{\epsilon}.\boldsymbol{a}; X) = Q(\boldsymbol{a}; X)$$

where "." stands for the coordinates by coordinates product between tuples.

The previous discussion implies that

$$R_{\boldsymbol{\ell}}(\boldsymbol{Y}; X) := \left(\prod_{\tau\in\mathsf{T}(\boldsymbol{\mu})} Y_\tau\right)^{2^k} Q(\boldsymbol{\ell}.\boldsymbol{Y}^{-1}; X) = \sum_{i=0}^{2^{k-1}} R_{i,\boldsymbol{\ell}}(\boldsymbol{Y}) X^{2i} + \left(\prod_{\tau\in\mathsf{T}(\boldsymbol{\mu})} Y_\tau\right)^{2^k} X^{2^k}$$

where $\boldsymbol{Y} = (Y_\tau)_{\tau\in\mathsf{T}(\boldsymbol{\mu})}$ and $\boldsymbol{Y}^{-1} = (Y_\tau^{-1})_{\tau\in\mathsf{T}(\boldsymbol{\mu})}$ and for $0 \le i \le 2^{k-1}$, $R_{i,\boldsymbol{\ell}} \in \mathbb{F}_p[\boldsymbol{Y}^2]$ is a homogeneous polynomial of degree $(k-1)2^k + 2i$, which only involves even powers of Y_τ for $\tau \in \mathsf{T}(\boldsymbol{\mu})$. Here, $\boldsymbol{Y}^2 = (Y_\tau^2)_{\tau\in\mathsf{T}(\boldsymbol{\mu})}$.

Let us denote by ψ the ring morphism from $\mathbb{F}_p[\boldsymbol{Y}^2]$ to $\mathbb{F}_p[Z]$ defined by

$$\forall \tau \in \mathsf{T}(\boldsymbol{\mu}), \quad \psi(Y_\tau^2) = Z + \tau.$$

Let us assume that $(p, w) = 1$. Note that if the tuple $\boldsymbol{b}$ satisfies the constraints given in (4.21) then $R_{\boldsymbol{\ell}}(\boldsymbol{b}; w) = 0$ since the contribution of $\boldsymbol{\epsilon} = (1, \ldots, 1)$ in $Q(\boldsymbol{\ell}.\boldsymbol{b}^{-1}; w)$ is exactly $w - m_{\boldsymbol{b},\boldsymbol{\ell}}(1, 1) \equiv 0 \bmod p$. Thus, c is a root of the polynomial $\psi(R_{\boldsymbol{\ell}}(\boldsymbol{Y}; w))$, which is of degree $k2^{k-1}$ and leading coefficient $w^{2^k} \not\equiv 0 \bmod p$. As a consequence, the number of c's in (4.21) is less than $k2^{k-1}$.

Let us assume that $w \equiv 0 \bmod p$. Let τ_0 in $\mathsf{T}(\boldsymbol{\mu})$ satisfying

$$p \nmid \ell_{\tau_0},$$

which exists by the conditions of the tuple $\boldsymbol{\ell}$.

Let us consider

$$S_{\boldsymbol{\ell}}(\boldsymbol{Y}) := \Big(\prod_{\tau\in\mathsf{T}(\boldsymbol{\mu})} Y_\tau\Big)^{2^{k-1}} Q\big(\widetilde{\boldsymbol{\ell}}.\widetilde{\boldsymbol{Y}}^{-1}; \ell_{\tau_0} Y_{\tau_0}^{-1}\big) \in \mathbb{F}_p[\widetilde{\boldsymbol{Y}}, Y_{\tau_0}],$$

where $\widetilde{\boldsymbol{Y}}^{-1} = (Y_\tau^{-1})_{\tau\in\mathsf{T}(\boldsymbol{\mu})\setminus\{\tau_0\}}$ and $\widetilde{\boldsymbol{\ell}} = (\ell_\tau)_{\tau\in\mathsf{T}(\boldsymbol{\mu})\setminus\{\tau_0\}}$. This polynomial is homogenous of degree $(k-1)2^{k-1}$ and only involves even powers of Y_τ for $\tau \in \mathsf{T}(\boldsymbol{\mu})$.

Thus, the polynomial $U = \psi(S_{\boldsymbol{\ell}}(\boldsymbol{Y})) \in \mathbb{F}_p(Z)$ is of degree less than $(k-1)2^{k-2}$. Let us show that this polynomial is of degree at least one. If not, all the coefficients but the constant one of the polynomial U vanish. If the tuple $\boldsymbol{b}$ satisfies the constraints given in (4.21) then $S_{\boldsymbol{\ell}}(\boldsymbol{b}) = 0$ because of the contribution of $\boldsymbol{\epsilon} = (-1,\dots,-1)$ in $Q(\widetilde{\boldsymbol{\ell}}.\widetilde{\boldsymbol{Y}}^{-1}; \ell_{\tau_0} Y_{\tau_0}^{-1})$. This implies that $U(c) = 0$ and that U is the constant polynomial of value 0. Choosing $Z = -\tau_0$ leads to

$$\ell_{\tau_0}^{2^{k-1}} \prod_{\substack{\tau\in\mathsf{T}(\boldsymbol{\mu})\\ \tau\neq\tau_0}} (\tau-\tau_0)^{2^{k-1}} \equiv 0 \bmod p$$

so that

$$\ell_{\tau_0} \equiv 0 \bmod p$$

since the τ's are distinct modulo p. This is a contradiction.

Finally, the c's satisfy the polynomial equation $U(c) = 0$ of degree at least 1 and less than $(k-1)2^{k-2}$. As a consequence, the number of c's in (4.21) is less than $(k-1)2^{k-2}$. □

The following proposition contains the asymptotic evaluation of the cardinality of the set $\mathsf{A}_{p^n}(\boldsymbol{\mu})$ defined in (4.16).

Proposition 4.8 (Applying A. Weil's version of the Riemann hypothesis). *Let $\boldsymbol{\mu} = (\mu(\tau))_{\tau\in\mathbb{Z}/p^n\mathbb{Z}}$ be a sequence of p^n-tuples of non-negative integers. If p is odd then*

$$|\mathsf{A}_{p^n}(\boldsymbol{\mu})| = \frac{\varphi(p^n)}{2^{|\overline{\mathsf{T}}(\boldsymbol{\mu})|}}\Big(1 + O\Big(\frac{2^{|\overline{\mathsf{T}}(\boldsymbol{\mu})|}|\overline{\mathsf{T}}(\boldsymbol{\mu})|}{p^{1/2}}\Big)\Big). \tag{4.22}$$

Remark 4.9. The equation (4.22) is an asymptotic expansion if and only if

$$\frac{2^{|\overline{\mathsf{T}}(\boldsymbol{\mu})|}|\overline{\mathsf{T}}(\boldsymbol{\mu})|}{p^{1/2}} \to 0 \tag{4.23}$$

as p tends to infinity among the prime numbers.

Proof of Proposition 4.8. Obviously,

$$\begin{aligned}|\mathsf{A}_{p^n}(\boldsymbol{\mu})| &= p^{n-1} \sum_{\substack{a\in(\mathbb{Z}/p\mathbb{Z})^\times,\\ \forall \tau\in\mathsf{T}(\boldsymbol{\mu}),\, a+\tau\in((\mathbb{Z}/p\mathbb{Z})^\times)^2}} 1\\ &= p^{n-1} \sum_{\substack{a\in(\mathbb{Z}/p\mathbb{Z})^\times,\\ \forall t\in\overline{\mathsf{T}}(\boldsymbol{\mu}),\, a+t\in((\mathbb{Z}/p\mathbb{Z})^\times)^2}} 1\\ &= p^{n-1} \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \prod_{\substack{t\in\overline{\mathsf{T}}(\boldsymbol{\mu}),\\ (a+t,p)=1}} \tfrac{1}{2}(\chi_2(a+t)+1),\end{aligned}$$

where χ_2 is the quadratic character modulo the odd prime number p.

At this point, the problem becomes a variant of the question considered by H. Davenport in 1931 of counting elements x modulo p such that both $x, x+1, \dots, x+k$ are quadratic residues modulo p uniformly with respect to the integer $k \geq 1$. See for instance [7, Section 1.4.2]. Thus, the end of the proof is omitted. □

The core of the proof of proposition 4.1 is the following result.

Proposition 4.10 (Moments of shifted Kloosterman sums). *Let $\boldsymbol{\mu} = (\mu(\tau))_{\tau\in\mathbb{Z}/p^n\mathbb{Z}}$ be a sequence of p^n-tuples of non-negative integers satisfying*

$$\sum_{\tau\in\mathbb{Z}/p^n\mathbb{Z}} \mu(\tau) \leq M \tag{4.24}$$

for some absolute positive constant M and $|\mathsf{T}(\boldsymbol{\mu})| = |\overline{\mathsf{T}}(\boldsymbol{\mu})|$. If

$$p > \max(M, 2n-5) \tag{4.25}$$

then

$$\mathsf{S}_{p^n}(\boldsymbol{\mu}; b_0) = \left[\prod_{\tau\in\mathbb{Z}/p^n\mathbb{Z}} \delta_{2|\mu(\tau)} \binom{\mu(\tau)}{\mu(\tau)/2}\right] \frac{|\mathsf{A}_{p^n}(\boldsymbol{\mu})|}{\varphi(p^n)} + O_{M,\epsilon}\left(p^{-\frac{4(n-1)}{2^n}+\epsilon}\right) \tag{4.26}$$

for any $\epsilon > 0$ and where the implied constant only depends on M and ϵ.

Remark 4.11. In particular, for any non-negative integer m,

$$\frac{1}{\varphi(p^n)} \sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \mathsf{Kl}_{p^n}(a, b_0)^m = \delta_{2|m} \frac{1}{2}\binom{m}{m/2} + O_{m,\epsilon}\left(p^{-\frac{4(n-1)}{2^n}+\epsilon}\right) \tag{4.27}$$

for any $\epsilon > 0$ under (4.25). In other words, under the same assumption,

$$\frac{1}{\varphi(p^n)} \sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \mathsf{Kl}_{p^n}(a, b_0)^m = \mathbb{E}(U^m) + O_{m,\epsilon}\left(p^{-\frac{4(n-1)}{2^n}+\epsilon}\right),$$

where U is any real-valued random variable of law the probability measure μ defined in (1.1). Hence, by (3.1), the normalized Kloosterman sums $\mathsf{Kl}_{p^n}(a, b_0)$ become equidistributed in $[-2, 2]$ with respect to the measure μ as briefly indicated in Remark 1.5. Such equidistribution result was stated without proof in [8, Remark 1.1]. This measure has already occured in [8], where the author proves that the twisted normalized Kloosterman sums $\mathsf{Kl}_{p^n}(a, \chi)$ for a fixed a in $\mathbb{Z}/p^n\mathbb{Z}$ and χ ranging over the Dirichlet characters of modulus p^n get equidistributed with respect to μ as p tends to infinity.

Remark 4.12. It follows from the results proved in [3] that if $1 \leq m \leq p^{n-1}$ then

$$\frac{1}{\varphi(p^n)} \sum_{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \mathsf{Kl}_{p^n}(a, 1)^m = \mathbb{E}(U^m),$$

where U is any real-valued random variable of law the probability measure μ, which agrees with (4.27).

Remark 4.13. For any integer $r \geq 1$, any non-negative integers $m_1, \ldots, m_r$ and any distinct integers $\tau_1, \ldots, \tau_r$, the previous proposition implies that

$$\frac{1}{\varphi(p^n)} \sum_{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \prod_{i=1}^{r} \mathsf{Kl}_{p^n}(a + \tau_i, b_0)^{m_i} = \mathbb{E}\Big(\prod_{i=1}^{r} U_i^{m_i} \Big) + O_{m_1+\cdots+m_r,\epsilon}\big(p^{-\frac{4(n-1)}{2^n}+\epsilon}\big)$$

for any $\epsilon > 0$ and for any sequence of real-valued independent random variables $(U_i)_{1 \leq i \leq r}$ of law the probability measure μ under (4.25) provided that

$$p > \max_{1 \leq i,j \leq r} |\tau_i - \tau_j|.$$

In other words, the r-tuple $(\mathsf{Kl}_{p^n}(a + \tau_i, b_0))_{1 \leq i \leq r}$ gets equidistributed in $[-2, 2]^r$ with respect to the measure $\otimes^r \mu$.

Proof of Proposition 4.10. Firstly,

$$\mathsf{Kl}_{p^n}(a + \tau, b_0) = \mathsf{Kl}_{p^n}(b_0 a + b_0 \tau, 1)$$

since b_0 is coprime with p. The change of variable $a' = b_0 a$ in $\mathsf{S}_{p^n}(\boldsymbol{\mu}; b_0)$ combined with the change of multiplicities

$$\mu(\tau) = \begin{cases} \mu(\tau'), & \text{if } \tau = b_0 \tau', \\ 0, & \text{otherwise} \end{cases}$$

for $\tau \in \mathbb{Z}/p^n\mathbb{Z}$ implies that one has to prove this proposition only for $b_0 = 1$. Thus, $b_0 = 1$ up to the completion of the proof.

Let us come back to the moment $\mathsf{S}_{p^n}(\boldsymbol{\mu})$. By Lemma 4.6,

$$\mathsf{S}_{p^n}(\boldsymbol{\mu}) = \frac{1}{\varphi(p^n)} \sum_{\boldsymbol{b}\in \mathsf{B}_{p^n}(\boldsymbol{\mu})} \prod_{\tau\in\mathsf{T}(\boldsymbol{\mu})} \left(\frac{b_\tau}{p^n}\right)^{\mu(\tau)} \sum_{\substack{a\in\mathbb{Z}/p^n\mathbb{Z},\\ \forall \tau\in\mathsf{T}(\boldsymbol{\mu}),\, a\equiv b_\tau^2-\tau \bmod p}} \prod_{\tau\in\mathsf{T}(\boldsymbol{\mu})} \left(2\cos\left(\frac{4\pi s_{a+\tau,p^n}}{p^n} + \theta_{p^n}\right)\right)^{\mu(\tau)}.$$

Recall that $s_{a+\tau,p^n}^2 \equiv a+\tau \bmod p^n$. In addition, the second condition in (4.13) is satisfied since a has to be coprime with p.

Now, recall that[6]

$$(2\cos(x))^M = \sum_{m=0}^{M} \binom{M}{m} \cos((M-2m)x)$$

for any real number x and any non-negative integer M. Thus,

$$\mathsf{S}_{p^n}(\boldsymbol{\mu}) = \frac{1}{\varphi(p^n)} \sum_{\boldsymbol{b}\in \mathsf{B}_{p^n}(\boldsymbol{\mu})} \prod_{\tau\in\mathsf{T}(\boldsymbol{\mu})} \left(\frac{b_\tau}{p^n}\right)^{\mu(\tau)} \sum_{\substack{a\in\mathbb{Z}/p^n\mathbb{Z}\\ \forall \tau\in\mathsf{T}(\boldsymbol{\mu}),\, a\equiv b_\tau^2-\tau \bmod p}} \prod_{\tau\in\mathsf{T}(\boldsymbol{\mu})} \sum_{u_\tau=0}^{\mu(\tau)} \binom{\mu(\tau)}{u_\tau} \cos\left[(\mu(\tau)-2u_\tau)\left(\frac{4\pi s_{a+\tau,p^n}}{p^n} + \theta_{p^n}\right)\right]. \tag{4.28}$$

One can split $\mathsf{S}_{p^n}(\boldsymbol{\mu})$ into $\mathsf{S}_{p^n}(\boldsymbol{\mu}) = \mathsf{MT}_{p^n}(\boldsymbol{\mu}) + \mathsf{Err}_{p^n}(\boldsymbol{\mu})$, where

$$\mathsf{MT}_{p^n}(\boldsymbol{\mu}) := \frac{1}{\varphi(p^n)} \sum_{\boldsymbol{b}\in \mathsf{B}_{p^n}(\boldsymbol{\mu})} \prod_{\tau\in\mathsf{T}(\boldsymbol{\mu})} \left(\frac{b_\tau}{p^n}\right)^{\mu(\tau)} \sum_{\substack{a\in\mathbb{Z}/p^n\mathbb{Z}\\ \forall \tau\in\mathsf{T}(\boldsymbol{\mu}),a\equiv b_\tau^2-\tau \bmod p}} \prod_{\tau\in\mathsf{T}(\boldsymbol{\mu})} \sum_{2u_\tau=\mu(\tau)} \binom{\mu(\tau)}{u_\tau} \cos\left[(\mu(\tau)-2u_\tau)\left(\frac{4\pi s_{a+\tau,p^n}}{p^n} + \theta_{p^n}\right)\right]$$

and $\mathsf{Err}_{p^n}(\boldsymbol{\mu})$ is the remaining term. Note that $\mathsf{MT}_{p^n}(\boldsymbol{\mu})$ is nothing else than the term obtained when the multiplicities $\mu(\tau)$ are even and $u_\tau = \mu(\tau)/2$.

[6]The referee kindly informed us that this expansion can be interpreted as an expansion in terms of Chebychev polynomials of the first kind, which are orthogonal polynomials for the measure μ.

Let us start with $\mathsf{MT}_{p^n}(\boldsymbol{\mu})$. Obviously, $\mathsf{MT}_{p^n}(\boldsymbol{\mu}) = 0$ unless

$$\forall \tau \in \mathsf{T}(\boldsymbol{\mu}), \quad 2 \mid \mu(\tau).$$

Hence

$$\mathsf{MT}_{p^n}(\boldsymbol{\mu}) = \left[\prod_{\tau \in \mathsf{T}(\boldsymbol{\mu})} \delta_{2|\mu(\tau)} \binom{\mu(\tau)}{\mu(\tau)/2} \right] \frac{|\mathsf{A}_{p^n}(\boldsymbol{\mu})|}{\varphi(p^n)}.$$

Let us bound $\mathsf{Err}_{p^n}(\boldsymbol{\mu})$. Trivially,

$$\mathsf{Err}_{p^n}(\boldsymbol{\mu}) \ll_M \sup_{\substack{\boldsymbol{\ell} \in \prod_{\tau \in \mathsf{T}(\boldsymbol{\mu})} [-\mu(\tau), \mu(\tau)] \\ \boldsymbol{\ell} \neq \mathbf{0}}} \mathsf{Err}_{p^n}(\boldsymbol{\mu}, \boldsymbol{\ell}),$$

where

$$\begin{aligned} \mathsf{Err}_{p^n}(\boldsymbol{\mu}, \boldsymbol{\ell}) &= \frac{1}{\varphi(p^n)} \sum_{\boldsymbol{b} \in \mathsf{B}_{p^n}(\boldsymbol{\mu})} \left| \sum_{\substack{a \in \mathbb{Z}/p^n\mathbb{Z} \\ \forall \tau \in \mathsf{T}(\boldsymbol{\mu}), a \equiv b_\tau^2 - \tau \bmod p}} e_{p^n}\left(\sum_{\tau \in \mathsf{T}(\boldsymbol{\mu})} \ell_\tau s_{a+\tau, p^n} \right) \right| \\ &:= \frac{1}{\varphi(p^n)} \sum_{\boldsymbol{b} \in \mathsf{B}_{p^n}(\boldsymbol{\mu})} |\mathsf{Err}_{p^n}(\boldsymbol{\mu}, \boldsymbol{\ell}, \boldsymbol{b})|. \end{aligned}$$

for any $|\mathsf{T}(\boldsymbol{\mu})|$-tuple $\boldsymbol{\ell}$ of integers with the properties written above.

Let us fix from now on a $|\mathsf{T}(\boldsymbol{\mu})|$-tuple $\boldsymbol{\ell} = (\ell_\tau)_{\tau \in \mathsf{T}(\boldsymbol{\mu})}$ of integers different from the tuple $\mathbf{0}$ and satisfying

$$\forall \tau \in \mathsf{T}(\boldsymbol{\mu}), \quad |\ell_\tau| \leq \mu(\tau) \leq M < p \tag{4.29}$$

by (4.24). Let τ_0 be a fixed element of $\mathsf{T}(\boldsymbol{\mu})$. For $\boldsymbol{b}$ in $\mathsf{B}_{p^n}(\boldsymbol{\mu})$, (4.12) implies that

$$\forall \tau \in \mathsf{T}(\boldsymbol{\mu}), \ \exists d_\tau \in \mathbb{Z}, \quad b_\tau^2 - \tau = b_{\tau_0}^2 - \tau_0 - d_\tau p.$$

One gets a $|\mathsf{T}(\boldsymbol{\mu})|$-tuple $\boldsymbol{d} = (d_\tau)_{\tau \in \mathsf{T}(\boldsymbol{\mu})}$ of integers. The change of variables

$$a = b_{\tau_0^2} - \tau_0 + up$$

with $u \bmod p^{n-1}$ so that

$$a + \tau = b_{\tau_0}^2 - \tau_0 + up + \tau = b_\tau^2 + (d_\tau + u)p$$

and (4.19) entail that

$$\begin{aligned}\mathrm{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell},\boldsymbol{b}) &= \sum_{u \bmod p^{n-1}} e_{p^n}\Big(\sum_{\tau\in\mathsf{T}(\boldsymbol{\mu})} \ell_\tau s_{b_\tau^2+(d_\tau+u)p,p^n}\Big)\\ &= \sum_{u \bmod p^{n-1}} e_{p^n}\Big(\sum_{\tau\in\mathsf{T}(\boldsymbol{\mu})} \ell_\tau b_\tau \sum_{m=0}^{n-1} c'_m \overline{b_\tau}^{2m} p^m (d_\tau+u)^m\Big)\\ &= \sum_{u \bmod p^{n-1}} e_{p^n}\big(P_{\boldsymbol{b}}(u)\big)\end{aligned}$$

where

$$P_{\boldsymbol{b}}(u) := \sum_{\tau\in\mathsf{T}(\boldsymbol{\mu})} \ell_\tau b_\tau \sum_{m=0}^{n-1} c'_m \overline{b_\tau}^{2m} p^m (d_\tau+u)^m \tag{4.30}$$

is a polynomial in the variable u of degree less than $n-1$ with integer coefficients. Note that all the quantities defined here and below depend on the tuples $\boldsymbol{\mu}$, $\boldsymbol{\ell}$, $\boldsymbol{b}$ and $\boldsymbol{d}$ but we only state the dependence on $\boldsymbol{b}$ for simplicity. One can check that

$$P_{\boldsymbol{b}}(u) = \sum_{j=0}^{n-1} a_j(\boldsymbol{b}) u^j,$$

where

$$\forall j \in \{0,\dots,n-1\},\quad a_j(\boldsymbol{b}) = \sum_{r=j}^{n-1} \binom{r}{j} c'_r m_{\boldsymbol{b}}(r,j) p^r$$

and

$$\forall j \in \{0,\dots,n-1\},\ \forall r \in \{j,\dots,n-1\},\quad m_{\boldsymbol{b}}(r,j) = \sum_{\tau\in\mathsf{T}(\boldsymbol{\mu})} \ell_\tau \overline{b_\tau}^{2r-1} d_\tau^{r-j}.$$

An important fact is that p^j divides $a_j(\boldsymbol{b})$ for any $j \in \{0,\dots,n-1\}$. Note also that when $r = j$, the quantity $m_{\boldsymbol{b}}(r,j)$ gets simpler and does not depend on the tuple $\boldsymbol{d}$ since $m_{\boldsymbol{b}}(j,j) = m_{\boldsymbol{b},\boldsymbol{\ell}}(j,j)$ previously defined in (4.14) for $1 \le j \le n-1$. In particular,

$$m_{\boldsymbol{b}}(1,1) = \sum_{\tau\in\mathsf{T}(\boldsymbol{\mu})} \ell_\tau \overline{b_\tau}.$$

Let us define

$$j(\boldsymbol{b}) := \sup\big(\{j \in \{1,\dots,n-1\},\ p^n \nmid a_j(\boldsymbol{b})\}\big) \in \{1,\dots,n-1\} \cup \{-\infty\}.$$

Having this notation in mind,

$$\mathrm{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell},\boldsymbol{b}) = \sum_{u \bmod p^{n-1}} e_{p^n}\Big(\sum_{j=0}^{n-1} a_j(\boldsymbol{b})u^j\Big).$$

This new polynomial in the exponential sum is still denoted by $P_{\boldsymbol{b}}(u)$ for simplicity, even though some terms are missing.

The strategy to find an upper-bound for $\mathrm{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell})$ is to decompose it into

$$\mathrm{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell}) = \frac{1}{\varphi(p^n)} \sum_{\substack{\boldsymbol{b}\in \mathsf{B}_{p^n}(\boldsymbol{\mu}),\\ j(\boldsymbol{b})=-\infty}} |\mathrm{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell},\boldsymbol{b})| + \frac{1}{\varphi(p^n)} \sum_{\substack{\boldsymbol{b}\in \mathsf{B}_{p^n}(\boldsymbol{\mu}),\\ j(\boldsymbol{b})=1}} |\mathrm{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell},\boldsymbol{b})|$$
$$+ \frac{1}{\varphi(p^n)} \sum_{\substack{\boldsymbol{b}\in \mathsf{B}_{p^n}(\boldsymbol{\mu}),\\ j(\boldsymbol{b})\in\{2,\dots,n-1\}}} |\mathrm{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell},\boldsymbol{b})| \quad (4.31)$$

and to proceed as follows.

- In the first term of (4.31), the exponential sum $\mathrm{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell},\boldsymbol{b})$ is bounded trivially by p^{n-1} but the counting of the tuples $\boldsymbol{b}$ is done carefully;
- In the third term of (4.31), Weyl's differencing process enables us to find an upper-bound for the exponential sum $\mathrm{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell},\boldsymbol{b})$ and the counting of the tuples $\boldsymbol{b}$ is done trivially by $\ll p$. Note that this term only occurs if $n \geq 3$.
- In the second term of (4.31), both the exponential sum $\mathrm{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell},\boldsymbol{b})$ and the counting of the tuples $\boldsymbol{b}$ are handled carefully.

Let us define $N = p^{n-1}$ for simplicity.

Let us begin with the third term of (4.31). The purpose is to show that if $\boldsymbol{b} \in \mathsf{B}_{p^n}(\boldsymbol{\mu})$ with $j(\boldsymbol{b}) \in \{2,\dots,n-1\}$ then

$$\mathrm{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell},\boldsymbol{b}) \ll_\epsilon p^{n-1-\frac{4(n-1)}{2^n}+\epsilon} \quad (4.32)$$

for any $\epsilon > 0$ and where the implied constant only depends on ϵ. For these tuples $\boldsymbol{b}$, $P_{\boldsymbol{b}}(u)$ is a polynomial of degree $j(\boldsymbol{b})$ and leading coefficient divisible by $p^{j(\boldsymbol{b})}$. Let us define $a_{j(\boldsymbol{b})}(\boldsymbol{b}) = p^k \alpha_{j(\boldsymbol{b})}$ where $j(\boldsymbol{b}) \leq k \leq n-1$ and $p \nmid \alpha_{j(\boldsymbol{b})}$. We are tempted to apply Weyl's differencing process (see [16]). By [5, Proposition 8.2]), one gets

$$|\mathrm{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell},\boldsymbol{b})| \leq 2N \times E^{2^{1-j(\boldsymbol{b})}}, \quad (4.33)$$

where

$$E := \frac{1}{N^{j(\boldsymbol{b})}} \sum_{-N<\ell_1,\dots,\ell_{j(\boldsymbol{b})-1}<N} \min\Big(N, \Big\|\frac{\alpha_{j(\boldsymbol{b})} j(\boldsymbol{b})! \ell_1 \dots \ell_{j(\boldsymbol{b})-1}}{p^{n-j(\boldsymbol{b})}}\Big\|^{-1}\Big).$$

As usual, $\|*\|$ stands for the distance to the nearest integer. The contribution to $\Sigma_{j(\boldsymbol{b})}$ of the integers satisfying $\ell_1 \dots \ell_{j(\boldsymbol{b})-1} = 0$ is trivially bounded by $1/N$. Up to this error term,

$$\begin{aligned} E &= \frac{1}{N^{j(\boldsymbol{b})}} \sum_{0\neq|\ell|<N^{j(\boldsymbol{b})-1}} d_{j(\boldsymbol{b})-1}(\ell) \min\left(N, \left\|\frac{\alpha_{j(\boldsymbol{b})} j(\boldsymbol{b})!\ell}{p^{n-k}}\right\|^{-1}\right) \\ &= \frac{1}{N^{j(\boldsymbol{b})}} \sum_{i=0}^{(n-1)(j(\boldsymbol{b})-1)-1} \sum_{\substack{0\neq|\ell|<N^{j(\boldsymbol{b})-1}, \\ p^i\|\ell}} d_{j(\boldsymbol{b})-1}(\ell) \min\left(N, \left\|\frac{\alpha_{j(\boldsymbol{b})} j(\boldsymbol{b})!\ell}{p^{n-k}}\right\|^{-1}\right) \\ &= \frac{1}{N^{j(\boldsymbol{b})}} \sum_{i=0}^{(n-1)(j(\boldsymbol{b})-1)-1} \sum_{\substack{0\neq|\ell|<\frac{N^{j(\boldsymbol{b})-1}}{p^i}, \\ (p,\ell)=1}} d_{j(\boldsymbol{b})-1}(p^i\ell) \min\left(N, \left\|\frac{\alpha_{j(\boldsymbol{b})} j(\boldsymbol{b})!\ell}{p^{n-k-i}}\right\|^{-1}\right). \end{aligned}$$

The contribution to E of the non-negative integers i less than $n-k-1$ can be written as

$$\frac{1}{N^{j(\boldsymbol{b})}} \sum_{\substack{0\le i\le(n-1)(j(\boldsymbol{b})-1)-1, \\ i\le n-k-1}} \sum_{\substack{|v|\le(p^{n-k-i}-1)/2, \\ (p,v)=1}} \sum_{\substack{0\neq|\ell|<\frac{N^{j(\boldsymbol{b})-1}}{p^i}, \\ \ell\equiv\overline{\alpha_{j(\boldsymbol{b})} j(\boldsymbol{b})!}v \bmod p^{n-k-i}}} d_{j(\boldsymbol{b})-1}(p^i\ell) \min\left(N, \left\|\frac{v}{p^{n-k-i}}\right\|^{-1}\right)$$

and is bounded by $(pN)^\epsilon/N$. The contribution of the remaining integers i is trivially bounded by $(pN)^\epsilon/p^{n-k}$, which is less than $(pN)^\epsilon/N$. As a consequence,

$$|\mathrm{Err}_{p^n}(\boldsymbol{\mu}, \boldsymbol{\ell}, \boldsymbol{b})| \ll_\epsilon (pN)^\epsilon N^{1-2^{1-j(\boldsymbol{b})}} \le (pN)^\epsilon N^{1-2^{2-n}},$$

which implies (4.32).

About the first term of of (4.31), let us show that

$$\frac{1}{\varphi(p^n)} \sum_{\substack{\boldsymbol{b}\in\mathsf{B}_{p^n}(\boldsymbol{\mu}), \\ j(\boldsymbol{b})=-\infty}} |\mathrm{Err}_{p^n}(\boldsymbol{\mu}, \boldsymbol{\ell}, \boldsymbol{b})| \ll \frac{p^{n-1}}{\varphi(p^n)} \mathsf{N}(\boldsymbol{\mu}, \boldsymbol{\ell}; 0), \tag{4.34}$$

where $\mathsf{N}(\boldsymbol{\mu}, \boldsymbol{\ell}; w)$ is defined in (4.15) for any w modulo p. The exponential sum in (4.31) is trivially bounded by p^{n-1}. Now, let $\boldsymbol{b}$ in $\mathsf{B}_{p^n}(\boldsymbol{\mu})$ with $j(\boldsymbol{b}) = -\infty$. If $1 \le j \le n-1$ then p^n divides $a_j(\boldsymbol{b})$, which implies that

$$c'_j m_{\boldsymbol{b}}(j, j) \equiv 0 \bmod p$$

and $m_{\boldsymbol{b}}(j, j) \equiv 0 \bmod p$ since c'_j is coprime with p for $p \ge 2n-5$ by (4.18). This implies (4.34).

Finally, let us prove that

$$\frac{1}{\varphi(p^n)} \sum_{\substack{\boldsymbol{b}\in \mathsf{B}_{p^n}(\boldsymbol{\mu}),\\ j(\boldsymbol{b})=1}} |\mathsf{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell},\boldsymbol{b})| \ll \frac{1}{\varphi(p^n)} \sum_{k=1}^{n-1} p^{n-k} \sum_{\substack{v \bmod p^{n-k},\\ (p,v)=1}} \frac{1}{|v|} \mathsf{N}\big(\boldsymbol{\mu},\boldsymbol{\ell};\overline{c_1'} v p^{k-1}\big). \tag{4.35}$$

For these tuples $\boldsymbol{b}$, $P_{\boldsymbol{b}}(u)$ is a polynomial of degree 1 and leading coefficient divisible by p. By [5, Equation (8.6)],

$$|\mathsf{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell},\boldsymbol{b})| \le \frac{1}{2} \min\Big(2N, \Big\|\frac{a_1(\boldsymbol{b})}{p^n}\Big\|^{-1}\Big) \tag{4.36}$$

so that

$$\begin{aligned}
\sum_{\substack{\boldsymbol{b}\in \mathsf{B}_{p^n}(\boldsymbol{\mu}),\\ j(\boldsymbol{b})=1}} |\mathsf{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell},\boldsymbol{b})| &\le \sum_{k=1}^{n-1} \sum_{\substack{\boldsymbol{b}\in \mathsf{B}_{p^n}(\boldsymbol{\mu}),\\ p^k \| a_1(\boldsymbol{b})}} \Big\|\frac{a_1(\boldsymbol{b})/p^k}{p^{n-k}}\Big\|^{-1} \\
&= \sum_{k=1}^{n-1} \sum_{\substack{v \bmod p^{n-k},\\ (p,v)=1}} \sum_{\substack{\boldsymbol{b}\in \mathsf{B}_{p^n}(\boldsymbol{\mu}),\\ a_1(\boldsymbol{b})/p^k \equiv v \bmod p^{n-k}}} \Big\|\frac{v}{p^{n-k}}\Big\|^{-1} \\
&= \sum_{k=1}^{n-1} p^{n-k} \sum_{\substack{v \bmod p^{n-k},\\ (p,v)=1}} \frac{1}{|v|} \sum_{\substack{\boldsymbol{b}\in \mathsf{B}_{p^n}(\boldsymbol{\mu}),\\ a_1(\boldsymbol{b})/p^k \equiv v \bmod p^{n-k}}} 1.
\end{aligned}$$

Now, if $\boldsymbol{b}$ in $\mathsf{B}_{p^n}(\boldsymbol{\mu})$ satisfies $a_1(\boldsymbol{b})/p^k \equiv v \bmod p^{n-k}$ then this implies $c_1' m_{\boldsymbol{b}}(1,1) \equiv a_1(\boldsymbol{b})/p \equiv v p^{k-1} \bmod p$ with c_1' coprime with p by (4.18). This is exactly (4.35).

By (4.31), (4.32), (4.32) and (4.34), one gets

$$\begin{aligned}
\mathsf{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell}) \ll_\epsilon p^{-\frac{4(n-1)}{2^n}+\epsilon} &+ \frac{\mathsf{N}(\boldsymbol{\mu},\boldsymbol{\ell};0)}{p} \\
&+ \sum_{k=1}^{n-1} \frac{1}{p^k} \sum_{\substack{v \bmod p^{n-k},\\ (p,v)=1}} \frac{1}{|v|} \mathsf{N}\big(\boldsymbol{\mu},\boldsymbol{\ell};\overline{c_1'} v p^{k-1}\big)
\end{aligned} \tag{4.37}$$

for any $\epsilon > 0$. Everything boils down to bounding $\mathsf{N}(\boldsymbol{\mu},\boldsymbol{\ell};w)$ uniformly with respect to $w \bmod p$. Proposition 4.7 implies that

$$\mathsf{Err}_{p^n}(\boldsymbol{\mu},\boldsymbol{\ell}) \ll_\epsilon p^{-\frac{4(n-1)}{2^n}+\epsilon}$$

for any $\epsilon > 0$. □

The following lemma will be used in the proof of Proposition 4.1.

Lemma 4.14. *Let $M \geq 2$ be an integer. If a_h is a sequence of real numbers indexed by non-negative integers satisfying*

$$\forall h \in \mathbb{N}, \quad 0 \leq a_h \leq \begin{cases} 1, & \text{if } h = 0, \\ \frac{1}{h}, & \text{otherwise,} \end{cases}$$

then

$$\Sigma_M = \sum_{\substack{0 \leq h_1, \dots, h_M \leq p^n, \\ \exists i \neq j,\ h_i \equiv h_j \bmod p, \\ h_i \neq h_j}} \prod_{i=1}^{M} a_{h_i} \ll \frac{\log^M (p^n)}{p}.$$

Proof of Lemma 4.14. Let us proceed by induction on M. If $M = 2$ then

$$\Sigma_2 = 2a_0 \sum_{\substack{1 \leq h \leq p^n, \\ p \mid h}} a_h + \sum_{\substack{1 \leq h_1, h_2 \leq p^n, \\ h_1 \equiv h_2 \bmod p}} a_{h_1} a_{h_2} \ll \frac{\log (p^{n-1})}{p} + \frac{\log (p^n) \log (p^{n-1})}{p}.$$

Let us assume that $M \geq 3$. We use the combinatorial identity given in [11, Lemma 7.1], which entails that

$$\Sigma_M = \sum_{s=1}^{M} \sum_{\sigma \in P(M,s)} \sum_{\substack{0 \leq h_1, \dots, h_s \leq p^n, \\ \exists i \neq j,\ h_i \equiv h_j \bmod p, \\ h_i \neq h_j}} \prod_{u=1}^{s} a_{h_u}^{\sigma_u},$$

where

$$\forall u \in \{1, \dots, s\}, \quad \sigma_u := |\sigma^{-1}(\{u\})|,$$

and for $1 \leq s \leq M$, $P(M, s)$ stands for the set of surjective functions

$$\sigma : \{1, \dots, M\} \to \{1, \dots, s\}$$

satisfying

$$\forall j \in \{1, \dots, M\}, \quad \sigma(j) = 1 \quad \text{or} \quad \exists k < j,\ \sigma(j) = \sigma(k) + 1.$$

The sum over $h_1, \dots, h_s$ can be decomposed into

$$\sum_{\substack{0 \leq h_1, \dots, h_s \leq p^n, \\ h_1, \dots, h_s \text{ distinct}, \\ \exists i_0, h_{i_0} = 0, \\ \exists j \neq i_0,\ h_j \equiv 0 \bmod p}} \prod_{u=1}^{s} a_{h_u}^{\sigma_u} + \sum_{\substack{0 \leq h_1, \dots, h_s \leq p^n, \\ h_1, \dots, h_s \text{ distinct}, \\ \exists i_0, h_{i_0} = 0, \\ \forall i \neq i_0,\ p \nmid h_i, \\ \exists i \neq j \neq i_0,\ h_i \equiv h_j \bmod p}} \prod_{u=1}^{s} a_{h_u}^{\sigma_u} + \sum_{\substack{1 \leq h_1, \dots, h_s \leq p^n, \\ h_1, \dots, h_s \text{ distinct}, \\ \exists i \neq j,\ h_i \equiv h_j \bmod p}} \prod_{u=1}^{s} a_{h_u}^{\sigma_u}.$$

The first sum is trivially bounded whereas the second and third sums are bounded by induction. This gives

$$\Sigma_M \ll \sum_{s=1}^{M} \sum_{\sigma\in P(M,s)} \Bigg(\frac{\log^{s-2}(p^n)\log(p^{n-1})}{p} + \frac{\log^{s-2}(p^n)\log(p^{n-1})}{p} + \frac{\log^{s-1}(p^n)\log(p^{n-1})}{p} \Bigg),$$

which ensures the result. □

Let us give now the proof of Proposition 4.1

Proof of Proposition 4.1. By Lemma 4.4, it is enough to consider $\widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n},b_0)$.

Recall that $H_{p^n} = \{(1-p^n)/2,\dots,(p^n-1)/2\}$. By (4.5),

$$\widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n};b_0) = \frac{1}{p^{n\ell(\boldsymbol{m}+\boldsymbol{n})/2}\varphi(p^n)} \sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \prod_{i=1}^{k} \Bigg(\sum_{u_i\in H_{p^n}} \overline{\alpha_{p^n}(u_i;t_i)}\mathsf{Kl}_{p^n}(a-u_i,b_0)\Bigg)^{m_i} \Bigg(\sum_{v_i\in H_{p^n}} \alpha_{p^n}(v_i;t_i)\mathsf{Kl}_{p^n}(a-v_i,b_0)\Bigg)^{n_i}$$

since the complete Kloosterman sums are real numbers. Expanding the powers, one gets

$$\widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n};b_0) = \frac{1}{p^{n\ell(\boldsymbol{m}+\boldsymbol{n})/2}\varphi(p^n)} \sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \prod_{i=1}^{k} \sum_{\boldsymbol{u}_i=(u_{i,1},\dots,u_{i,m_i})\in H_{p^n}^{m_i}} \sum_{\boldsymbol{v}_i=(v_{i,1},\dots,v_{i,n_i})\in H_{p^n}^{n_i}} \prod_{e_i=1}^{m_i} \overline{\alpha_{p^n}(u_{i,e_i};t_i)}\,\mathsf{Kl}_{p^n}(a-u_{i,e_i},b_0) \prod_{f_i=1}^{n_i} \alpha_{p^n}(v_{i,f_i};t_i)\,\mathsf{Kl}_{p^n}(a-v_{i,f_i},b_0).$$

Let us set for $1\le i\le k$,

$$\begin{aligned}\boldsymbol{h}_i &= (h_{i,1},\dots,h_{i,m_i},h_{i,m_i+1},\dots,h_{i,m_i+n_i})\\ &= (u_{i,1},\dots,u_{i,m_i},v_{i,1},\dots,v_{i,n_i}) \in H_{p^n}^{m_i+n_i}\end{aligned}$$

and

$$\boldsymbol{h} = (\boldsymbol{h}_1,\dots,\boldsymbol{h}_k) \in H_{p^n}^{\ell(\boldsymbol{m}+\boldsymbol{n})}.$$

Exchanging the order of summations, one is led to

$$\widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n};b_0) = \frac{1}{p^{n\ell(\boldsymbol{m}+\boldsymbol{n})/2}} \sum_{\boldsymbol{h}\in H_{p^n}^{\ell(\boldsymbol{m}+\boldsymbol{n})}} \prod_{i=1}^{k}\prod_{j=1}^{m_i} \overline{\alpha_{p^n}(h_{i,j};t_i)}$$
$$\prod_{j=m_i+1}^{m_i+n_i} \alpha_{p^n}(h_{i,j};t_i)\,\frac{1}{\varphi(p^n)} \sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \prod_{i=1}^{k}\prod_{j=1}^{m_i+n_i} \mathsf{Kl}_{p^n}(a-h_{i,j},b_0).$$

By Lemma 4.14 and (4.6), the contribution of the tuples $\boldsymbol{h}$ different from the tuple $\mathbf{0}$ and whose components are not distinct modulo p is bounded by

$$\ll_{\ell(\boldsymbol{m}+\boldsymbol{n})} \frac{\log^{\ell(\boldsymbol{m}+\boldsymbol{n})}(p^n)}{p}, \tag{4.38}$$

where the implied constant only depends on $\ell(\boldsymbol{m}+\boldsymbol{n})$.

Thus, up to all the previous error terms,

$$\widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n};b_0) = \frac{1}{p^{n\ell(\boldsymbol{m}+\boldsymbol{n})/2}} \sideset{}{^*}\sum_{\boldsymbol{h}\in H_{p^n}^{\ell(\boldsymbol{m}+\boldsymbol{n})}} \prod_{i=1}^{k}\prod_{j=1}^{m_i} \overline{\alpha_{p^n}(h_{i,j};t_i)}$$
$$\prod_{j=m_i+1}^{m_i+n_i} \alpha_{p^n}(h_{i,j};t_i)\,\frac{1}{\varphi(p^n)} \sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \prod_{i=1}^{k}\prod_{j=1}^{m_i+n_i} \mathsf{Kl}_{p^n}(a-h_{i,j},b_0), \tag{4.39}$$

where the $*$ means that the summation is over the tuples $\boldsymbol{h} = (h_{i,j})_{\substack{1\le i\le k\\ 1\le j\le m_i}}$ whose components are either equal or distinct modulo p, namely

$$h_{i,j} = h_{k,\ell} \quad \text{or} \quad p \nmid h_{i,j} - h_{k,\ell}$$

for any $(i,j)\neq(k,\ell)$ in the relevant ranges.

Note that by (4.11),

$$\frac{1}{\varphi(p^n)} \sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \prod_{i=1}^{k}\prod_{j=1}^{m_i+n_i} \mathsf{Kl}_{p^n}(a-h_{i,j},b_0) = \mathsf{S}_{p^n}(\boldsymbol{\mu}_{\boldsymbol{h}};b_0),$$

where $\boldsymbol{\mu}_{\boldsymbol{h}} = (\mu_{\boldsymbol{h}}(\tau))_{\tau\in\mathbb{Z}/p^n\mathbb{Z}}$ is the p^n-tuple of non-negative integers defined by

$$\forall \tau\in\mathbb{Z}/p^n\mathbb{Z},\quad \mu_{\boldsymbol{h}}(\tau) := \sum_{i=1}^{k} |\{j\in\{1,\dots,m_i+n_i\}, -h_{i,j}\equiv\tau \bmod p^n\}|.$$

Note also that

$$\sum_{\tau\in\mathbb{Z}/p^n\mathbb{Z}} \mu_{\boldsymbol{h}}(\tau) = \ell(\boldsymbol{m}+\boldsymbol{n})$$

so that

$$|\{\tau \bmod p, \tau \in \mathbb{Z}/p^n\mathbb{Z}, \mu_{\boldsymbol{h}}(\tau) \geq 1\}| = |\{\tau \in \mathbb{Z}/p^n\mathbb{Z}, \mu_{\boldsymbol{h}}(\tau) \geq 1\}| \leq \ell(\boldsymbol{m}+\boldsymbol{n})$$

according to the property satisfied by the relevant tuples $\boldsymbol{h}$ in (4.39).

Hence, one can apply Proposition 4.10. By (4.6), the contribution of the error term is bounded by

$$\ll_{\ell(\boldsymbol{m}+\boldsymbol{n}),\epsilon} \log^{\ell(\boldsymbol{m}+\boldsymbol{n})}(p^n) p^{-\frac{4(n-1)}{2^n}+\epsilon}$$

for any $\epsilon > 0$, where the implied constant only depends on $\ell(\boldsymbol{m}+\boldsymbol{n})$ and ϵ. Thus, up to the previous error terms,

$$\widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t}; \boldsymbol{m}, \boldsymbol{n}; b_0) = \frac{1}{p^{n\ell(\boldsymbol{m}+\boldsymbol{n})/2}} \sum_{\boldsymbol{h} \in H_{p^n}^{\ell(\boldsymbol{m}+\boldsymbol{n})}} \prod_{i=1}^{k} \prod_{j=1}^{m_i} \overline{\alpha_{p^n}(h_{i,j}; t_i)}$$
$$\prod_{j=m_i+1}^{m_i+n_i} \alpha_{p^n}(h_{i,j}; t_i) \left[\prod_{\tau \in \mathbb{Z}/p^n\mathbb{Z}} \delta_{2|\mu_{\boldsymbol{h}}(\tau)} \binom{\mu_{\boldsymbol{h}}(\tau)}{\mu_{\boldsymbol{h}}(\tau)/2} \right] \frac{|\mathsf{A}_{p^n}(\mu_{\boldsymbol{h}}(\tau))|}{\varphi(p^n)},$$

where $\mathsf{A}_{p^n}(\mu_{\boldsymbol{h}}(\tau))$ is defined in (4.16).

Let us apply Proposition 4.8. By (4.6), the contribution of the error term is bounded by

$$\ll_{\ell(\boldsymbol{m}+\boldsymbol{n})} \frac{\log^{\ell(\boldsymbol{m}+\boldsymbol{n})}(p^n)}{\sqrt{p}},$$

where the implied constant only depends on $\ell(\boldsymbol{m}+\boldsymbol{n})$ and, up to all the previous error terms,

$$\widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t}; \boldsymbol{m}, \boldsymbol{n}; b_0) = \frac{1}{p^{n\ell(\boldsymbol{m}+\boldsymbol{n})/2}} \sum_{\boldsymbol{h} \in H_{p^n}^{\ell(\boldsymbol{m}+\boldsymbol{n})}} \prod_{i=1}^{k} \prod_{j=1}^{m_i} \overline{\alpha_{p^n}(h_{i,j}; t_i)}$$
$$\prod_{j=m_i+1}^{m_i+n_i} \alpha_{p^n}(h_{i,j}; t_i) \left[\prod_{\tau \in \mathbb{Z}/p^n\mathbb{Z}} \delta_{2|\mu_{\boldsymbol{h}}(\tau)} \binom{\mu_{\boldsymbol{h}}(\tau)}{\mu_{\boldsymbol{h}}(\tau)/2} \right] \frac{1}{2^{|\mathsf{T}(\mu_{\boldsymbol{h}})|}}.$$

It should be pointed out that the fact that

$$|\mathsf{T}(\mu_{\boldsymbol{h}})| = |\overline{\mathsf{T}}(\mu_{\boldsymbol{h}})|$$

is crucial since recognizing the moments of the measure μ requires the left-hand side of the previous equation whereas the right-hand side appears by Proposition 4.8.

By (3.1),

$$\widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n};b_0)=\frac{1}{p^{n\ell(\boldsymbol{m}+\boldsymbol{n})/2}}\sideset{}{^*}\sum_{\boldsymbol{h}\in H_{p^n}^{\ell(\boldsymbol{m}+\boldsymbol{n})}}\prod_{i=1}^{k}\prod_{j=1}^{m_i}\overline{\alpha_{p^n}(h_{i,j};t_i)}$$
$$\prod_{j=m_i+1}^{m_i+n_i}\alpha_{p^n}(h_{i,j};t_i)\,\mathbb{E}\Big(\prod_{i=1}^{k}\prod_{j=1}^{m_i+n_i}U_{h_{i,j}}\Big)$$

for any finite sequence of real-valued independent random variables $(U_h)_{h\in\mathbb{Z}/p^n\mathbb{Z}}$ of law the probability measure μ defined in (1.1). The fact that

$$\mathbb{E}\Big(\prod_{i=1}^{k}\prod_{j=1}^{m_i+n_i}U_{h_{i,j}}\Big)=\mathbb{E}\Big(\prod_{\tau\in\mathbb{Z}/p^n\mathbb{Z}}U_\tau^{\mu(\tau)}\Big)$$

has also been used. One can add the missing tuples $\boldsymbol{h}$ at the admissible cost given in (4.38) so that, up to all the previous error terms,

$$\widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n};b_0)=\frac{1}{p^{n\ell(\boldsymbol{m}+\boldsymbol{n})/2}}\sum_{\boldsymbol{h}\in H_{p^n}^{\ell(\boldsymbol{m}+\boldsymbol{n})}}\prod_{i=1}^{k}\prod_{j=1}^{m_i}\overline{\alpha_{p^n}(h_{i,j};t_i)}$$
$$\prod_{j=m_i+1}^{m_i+n_i}\alpha_{p^n}(h_{i,j};t_i)\,\mathbb{E}\Big(\prod_{i=1}^{k}\prod_{j=1}^{m_i+n_i}U_{h_{i,j}}\Big).$$

Let us approximate the coefficients $\alpha_{p^n}(h;t)$. By (4.7) and (4.6), one gets, up to all the previous error terms,

$$\widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n};b_0)=\frac{1}{p^{n\ell(\boldsymbol{m}+\boldsymbol{n})/2}}\sum_{\boldsymbol{h}\in H_{p^n}^{\ell(\boldsymbol{m}+\boldsymbol{n})}}\prod_{i=1}^{k}\prod_{j=1}^{m_i}\overline{\beta(h_{i,j};t_i)}$$
$$\prod_{j=m_i+1}^{m_i+n_i}\beta(h_{i,j};t_i)\,\mathbb{E}\Big(\prod_{i=1}^{k}\prod_{j=1}^{m_i+n_i}U_{h_{i,j}}\Big)+O_{\ell(\boldsymbol{m}+\boldsymbol{n})}\Big(\frac{\log^{\ell(\boldsymbol{m}+\boldsymbol{n})-1}(p^n)}{p^n}\Big).$$

Reverting the computation done at the very beginning of the proof of this proposition, one is led to

$$\widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n};b_0)=\mathbb{E}\Big(\prod_{i=1}^{k}\overline{\mathsf{Kl}_{\frac{p^n-1}{2}}(t_i)}^{m_i}\,\mathsf{Kl}_{\frac{p^n-1}{2}}(t_i)^{n_i}\Big)$$

up to all the previous error terms and where

$$\mathsf{Kl}_{\frac{p^n-1}{2}}(t;*)=\sum_{|h|\le\frac{p^n-1}{2}}\beta(h;t)\,U_h(*).$$

Finally, by (3.2) and (3.3) in Proposition 3.1, up to all the previous error terms,

$$\widetilde{\mathsf{M}_{p^n}}(\boldsymbol{t};\boldsymbol{m},\boldsymbol{n};b_0)=\mathbb{E}\Big(\prod_{i=1}^{k}\overline{\mathsf{Kl}(t_i)}^{m_i}\,\mathsf{Kl}(t_i)^{n_i}\Big)+O_{\ell(\boldsymbol{m}+\boldsymbol{n})}\Big(\frac{\log^{\ell(\boldsymbol{m}+\boldsymbol{n})}(p^n)}{p^{n/2}}\Big),$$

where

$$\mathsf{Kl}(t;*)=\sum_{h\in\mathbb{Z}}\beta(h;t)U_h(*)$$

for any sequence of real-valued independent random variables $(U_h)_{h\in\mathbb{Z}}$ of law the probability measure μ. □

5. The tightness condition

5.1. The counting ingredient. The following lemma states, without any proof, the version of Hensel's lemma, which will be used in the proof of Lemma 5.2. This result is so standard that we do not give any reference too.

Lemma 5.1 (Hensel's lemma). *Let k be a positive integer and f be a polynomial with integer coefficients. Assume that x_0 is a solution modulo p^k of the congruence $f(x)\equiv 0 \bmod p^k$.*

- *If $p\nmid f'(x_0)$ then there is exactly one solution modulo p^{k+1} of the congruence $f(x)\equiv 0 \bmod p^{k+1}$ congruent to x_0 modulo p^k.*
- *If $p\mid f'(x_0)$ and $f(x_0)\equiv 0 \bmod p^{k+1}$ then there are exactly p solutions modulo p^{k+1} of the congruence $f(x)\equiv 0 \bmod p^{k+1}$ congruent to x_0 modulo p^k. They are given by $x_0+p^k j$ for j modulo p.*

Lemma 5.2 (Hensel's lemma in degree 2). *Let $n\geqslant 1$ be an integer and $f(X)=X^2-sX+\pi$ be a polynomial of degree 2 with integer coefficients satisfying $s\equiv\pi+1 \bmod p^n$. Assume that $p^\ell \,||\, \pi-1$ for some integer $\ell\geq 1$. The number of solutions of the congruence $f(x)\equiv 0 \bmod p^n$ equals*

$$\begin{cases}2p^\ell, & \text{if } 1\leq \ell\leq n/2-1,\\ p^{n/2}, & \text{if } n/2\leq \ell\leq n,\end{cases}$$

if n is even, and

$$\begin{cases}2p^\ell, & \text{if } 1\leq \ell\leq (n-1)/2,\\ p^{(n-1)/2}, & \text{if } (n-1)/2+1\leq \ell\leq n,\end{cases}$$

if n is odd.

Remark 5.3. This lemma is proved by a quite technical induction on $n\geq 1$ but understanding the set of solutions for $1\leq n\leq 3$ of $f(x)\equiv 0 \bmod p^n$ gives an idea of how the induction works.

Proof of Lemma 5.2. In this proof, recall that $p \mid \pi - 1$.

Obviously, 1 is the only solution of the congruence $f(x) \equiv 0 \bmod p$ with $s \equiv \pi + 1 \bmod p$.

Let us quickly check what happens for $n = 2$. One has $f(1) \equiv 0 \bmod p^2$ and $f'(1) = 2 - s \equiv 0 \bmod p$. By Lemma 5.1, the only solutions of $f(x) \equiv 0 \bmod p^2$ with $s \equiv \pi + 1 \bmod p^2$ are $1 + pk_1$ for $0 \leq k_1 < p$.

Let us do the case $n = 3$. For $0 \leq k_1 < p$, $1 + pk_1$ is a solution of $f(x) \equiv 0 \bmod p^2$ satisfying $f'(1 + pk_1) \equiv 0 \bmod p$ and

$$f(1 + pk_1) \equiv pk_1(1 - \pi + pk_1) \bmod p^3.$$

If $k_1 = 0$ then by Lemma 5.1, $1 + p^2k_2$ for $0 \leq k_2 < p$ are the only solutions of $f(x) \equiv 0 \bmod p^3$ congruent to 1 modulo p^2. Otherwise, $p \mid\mid \pi - 1$ and $k_{1,\pi}$ must be the unique invertible integer modulo p satisfying $pk_{1,\pi} \equiv \pi - 1 \bmod p^2$. Then, by Lemma 5.1 $1 + pk_{1,\pi} + p^2k_2$ for $0 \leq k_2 < p$ are the solutions of $f(x) \equiv 0 \bmod p^3$ congruent to $1 + pk_{1,\pi}$ modulo p^2. We have just seen that the solutions of $f(x) \equiv 0 \bmod p^3$ with $s \equiv \pi + 1 \bmod p^3$ are

- $1 + p^2k_2$ for $0 \leq k_2 < p$,
- $1 + pk_{1,\pi} + p^2k_2$ for $0 \leq k_2 < p$ and if $p \mid\mid \pi - 1$ and $pk_{1,\pi} \equiv \pi - 1 \bmod p^2$.

Note that the previous simple use of Hensel's lemma proves Lemma 5.2 for $1 \leq n \leq 3$. We will conclude by induction on $n \geq 2$.

Let us set

$$(\ell_1(n), \ell_2(n)) := \begin{cases} (n/2 - 1, n/2), & \text{if } n \text{ is even,} \\ ((n-1)/2, (n-1)/2), & \text{if } n \text{ is odd.} \end{cases}$$

Let us prove that for any $n \geq 2$, the solutions of the congruence $f(x) \equiv 0 \bmod p^n$ for any polynomial $f(X) = X^2 - sX + \pi$ of degree 2 with integer coefficients satisfying $s \equiv \pi + 1 \bmod p^n$ are

$$1 + p^{n-1}k_{n-1},$$

where $0 \leq k_{n-1} < p$ and for any $2 \leq m \leq \ell_2(n)$,

$$1 + p^{n-m}k_{n-m} + \cdots + p^{n-1}k_{n-1},$$

where $0 < k_{n-m} < p$, $0 \leq k_{n-m+1}, \ldots, k_{n-1} < p$ provided that $p^m \mid \pi - 1$ and for any $2 \leq m \leq \ell_1(n)$,

$$1 + p^m k_{m,\pi} + \cdots + p^{n-m-1}k_{n-m-1,\pi} + p^{n-m}k_{n-m} + \cdots + p^{n-1}k_{n-1},$$

where $0 \leq k_{n-m}, \ldots, k_{n-1} < p$ provided that $p^m \mid\mid \pi - 1$. Here, the numbers $k_{u,\pi}$, $m \leq u \leq n - m - 1$, are fixed integers modulo p satisfying

$$p^m k_{m,\pi} + \cdots + p^{n-m-1}k_{n-m-1} \equiv \pi - 1 \bmod p^{n-m}.$$

In particular, $k_{m,\pi}$ is invertible modulo p. This fact trivially implies Lemma 5.2 for $n \geq 2$. The cases $n = 1$, $n = 2$ and $n = 3$ have just been seen above.

Let $n \geq 2$. Let us assume that the result holds at the rank n and let us check that it remains true at the rank $n+1$. For instance, let us assume that n is even. We do not provide the proof when n is odd since this is completely similar.

For $0 \leq k_{n-1} < p$, $x_n := 1 + p^{n-1}k_{n-1}$ is a solution of $f(x) \equiv 0 \bmod p^n$, which satisfies $f'(x_n) \equiv 0 \bmod p$ and

$$f(x_n) \equiv p^{n-1}k_{n-1}(1 - \pi + p^{n-1}k_{n-1}) \bmod p^{n+1}.$$

By Lemma 5.1, the only solutions of $f(x) \equiv 0 \bmod p^{n+1}$ congruent to x_n are

- $1 + p^n k_n$ for $0 \leq k_n < p$ if $k_{n-1} = 0$,
- $1 + p^{n-1}k_{n-1} + p^n k_n$ for $0 < k_{n-1} < p$, $0 \leq k_n < p$ and if $p^2 \mid \pi - 1$.

Let $2 \leq m \leq \ell_2(n) = n/2$. Assume that $p^m \mid \pi - 1$. For $0 \leq k_{n-m+1}, \ldots, k_{n-1} < p$ and $0 < k_{n-m} < p$,

$$x_{m,n} := 1 + p^{n-m}k_{n-m} + \cdots + p^{n-1}k_{n-1}$$

is a solution $f(x) \equiv 0 \bmod p^n$, which satisfies $f'(x_{m,n}) \equiv 0 \bmod p$ and

$$f(x_{m,n}) \equiv p^n(k_{n-m} + \cdots + p^{m-1}k_{n-1}) \cdot \left(\frac{1-\pi}{p^m} + p^{n-2m}k_{n-m} + \cdots + p^{n-1-m}k_{n-1}\right) \bmod p^{n+1}.$$

If $2 \leq m < n/2$ then by Lemma 5.1, the only solutions of $f(x) \equiv 0 \bmod p^{n+1}$ congruent to $x_{m,n}$ are

$$1 + p^{n-m}k_{n-m} + \cdots + p^{n-1}k_{n-1} + p^n k_n,$$

where $0 < k_{n-m} < p$, $0 \leq k_{n-m+1}, \ldots, k_n < p$ provided that $p^{m+1} \mid \pi - 1$. If $m = n/2$ then by Lemma 5.1, the only solutions of $f(x) \equiv 0 \bmod p^{n+1}$ congruent to $x_{n/2,n}$ are

$$1 + p^{n/2}k_{n/2,\pi} + p^{n/2+1}k_{n/2+1} + \cdots + p^{n-1}k_{n-1} + p^n k_n,$$

where $0 \leq k_{n/2+1}, \ldots, k_n < p$ provided that $p^{n/2} \mid\mid \pi - 1$ and $p^{n/2}k_{n/2,\pi} \equiv \pi - 1 \bmod p^{n/2+1}$.

Let $1 \leq m \leq \ell_1(n) = n/2 - 1$. Assume that $p^m \mid\mid \pi - 1$. For $0 \leq k_{n-m}, \ldots, k_{n-1} < p$,

$$x_{m,n} := 1 + p^m k_{m,\pi} + \cdots + p^{n-m-1}k_{n-m-1,\pi} + p^{n-m}k_{n-m} + \cdots + p^{n-1}k_{n-1}$$

is a solution $f(x) \equiv 0 \bmod p^n$, which satisfies $f'(x_{m,n}) \equiv 0 \bmod p$ and

$$\begin{aligned} f(x_{m,n}) \equiv p^n \big(&k_{m,\pi} + \cdots + p^{n-2m-1} k_{n-m-1,\pi} \\ &+ p^{n-2m} k_{n-m} + \cdots + p^{n-1-m} k_{n-1}\big) \\ \cdot \Big(&\frac{1 - \pi + p^m k_{m,\pi} + \cdots + p^{n-1-m} k_{n-m-1,\pi}}{p^{n-m}} \\ &+ k_{n-m} + p k_{n-m+1} + \cdots + k_{n-1} p^{n-1-m}\Big) \bmod p^{n+1}. \end{aligned}$$

By Lemma 5.1, the only solutions of $f(x) \equiv 0 \bmod p^{n+1}$ congruent to $x_{m,n}$ are

$$1 + p^m k_{m,\pi} + \cdots + p^{n-m} k_{n-m,\pi} + p^{n-m+1} k_{n-m+1} + \cdots + p^n k_n,$$

where $0 \le k_{n-m+1}, \ldots, k_n < p$, and where

$$p^m k_{m,\pi} + \cdots + p^{n-m} k_{n-m,\pi} \equiv \pi - 1 \bmod p^{n-m+1}.$$

This completes the induction on n. □

Proposition 5.4 (The counting ingredient). *Let $n \ge 1$ be an integer and I be a non-empty interval in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. The number of quadruples $(x_1, x_2, x_3, x_4) \in I^4$ satisfying*

$$\begin{aligned} x_1 + x_2 &\equiv x_3 + x_4 \bmod p^n, \\ \overline{x_1} + \overline{x_2} &\equiv \overline{x_3} + \overline{x_4} \bmod p^n \end{aligned}$$

is bounded by an absolute positive constant times $n|I|^2$.

Proof of Proposition 5.4. Let us denote by $N_{k,\ell}(p^n; I)$ the number of these quadruples (x_1, x_2, x_3, x_4) satisfying $p^k \,||\, x_3 + x_4$ and $p^\ell \,||\, x_3 - x_4$ for some fixed integers $k, \ell \in \{0, \ldots, n\}$, which must satisfy $k\ell = 0$ since p is odd. Let (x_1, x_2, x_3, x_4) be such a quadruple. Let us fix x_4. There are at most $|I|$ such x_4. The bijective change of variables $y_i = \overline{x_4} x_i$ for $1 \le i \le 3$ leads to the system

$$\begin{aligned} y_1 + y_2 &\equiv y_3 + 1 \bmod p^n, \\ \overline{y_1} + \overline{y_2} &\equiv \overline{y_3} + 1 \bmod p^n, \end{aligned}$$

where the triple (y_1, y_2, y_3) belongs to $(\overline{x_4} I)^3$ and whose components satisfy $p^k \,||\, y_3 + 1$ and $p^\ell \,||\, y_3 - 1$. Let us set

$$s = y_1 + y_2 \quad \text{and} \quad \varpi = y_1 y_2.$$

The previous system becomes

$$s \equiv y_3 + 1 \bmod p^n \tag{5.1}$$

and

$$\overline{\varpi} s \equiv \overline{y_3} + 1 \bmod p^n.$$

Thus,

$$1 \equiv y_3 \overline{y_3} \equiv (s-1)(\overline{\varpi} s - 1) \bmod p^n$$

so that $s(s - (\varpi + 1)) \equiv 0 \bmod p^n$ and

$$s \equiv \varpi + 1 \bmod p^{n-k}. \tag{5.2}$$

Let $f(X) = X^2 - sX + \varpi$. Obviously, y_1 and y_2 are solutions modulo p^n of the congruence

$$f(x) \equiv 0 \bmod p^n. \tag{5.3}$$

Note also that

$$f(X) \equiv (X-1)(X-\varpi) \bmod p^{n-k} \tag{5.4}$$

by (5.2). In particular, if $n - k \geq 1$ then the only solutions modulo p of

$$f(x) \equiv 0 \bmod p$$

are 1 and ϖ, which satisfy $f'(\varpi) \equiv -f'(1) = \varpi - 1 \mod p$ by (5.2). Let us consider three distinct cases.

First case: $k = 0$ *and* $0 \leq \ell \leq n$. In this case, $p \nmid s$ by (5.1) and $p^\ell \,||\, \varpi - 1$ since $y_3 - 1 \equiv s - 2 \equiv \varpi - 1 \bmod p^n$ by (5.1) and (5.2). Let us fix y_3, which implies that s is fixed by (5.1) and ϖ is fixed by (5.2). There are $\ll 1 + |I|/p^\ell$ such y_3. By Lemma 5.2, the number $N_\ell(p^n)$ of solutions modulo p^n of the congruence (5.3) satisfies

$$N_\ell(p^n) \ll \begin{cases} p^\ell, & \text{if } n \text{ is even and } 0 \leq \ell \leq n/2 - 1, \\ p^{n/2}, & \text{if } n \text{ is even and } n/2 \leq \ell \leq n, \\ p^\ell, & \text{if } n \text{ is odd and } 0 \leq \ell \leq (n-1)/2, \\ p^{(n-1)/2}, & \text{if } n \text{ is odd and } (n-1)/2 + 1 \leq \ell \leq n. \end{cases}$$

In total,

$$N_{0,\ell}(p^n; I) \ll |I| \Big(1 + \frac{|I|}{p^\ell}\Big) \min\big(N_\ell(p^n), |I|\big).$$

Second case: $1 \leq k \leq n-1$ *and* $\ell = 0$. In this case, $p^k \,||\, s$ by (5.1) and $p \nmid \varpi - 1$ by (5.1) and (5.2). Let us fix y_3, which implies that s is fixed by (5.1) and ϖ is fixed modulo p^{n-k} by (5.2). There are $\ll 1 + |I|/p^k$ such y_3. By Lemma 5.2, the

congruence $f(x) \equiv 0 \bmod p^{n-k}$ has exactly two solutions. Hence, the same holds for the number of pairs (y_1, y_2) modulo p^{n-k}. In total,

$$N_{k,0}(p^n; I) \ll |I|\Big(1 + \frac{|I|}{p^k}\Big)\Big(1 + \frac{|I|}{p^{n-k}}\Big) \ll |I|^2.$$

Third case: $k = n$ *and* $\ell = 0$. In this case $y_3 \equiv -1 \bmod p^n$ is fixed and given y_1, y_2 is fixed. In total,

$$N_{n,0}(p^n; I) \ll |I|^2.$$

Altogether, the number of quadruples (x_1, x_2, x_3, x_4) equals

$$\sum_{\ell=0}^{n} N_{0,\ell}(p^n; I) + \sum_{k=1}^{n-1} N_{k,0}(p^n; I) + N_{n,0}(p^n; I)$$

and is bounded by $\ll n|I|^2$. □

5.2. The fourth moment of incomplete Kloosterman sums.

Proposition 5.5 (Bounding the fourth moment). *Let $n \geqslant 2$ be an integer and I be a non-empty interval in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. One has*

$$\mathsf{M}_4(I) := \frac{1}{\varphi(p^n)^2} \sum_{(a,b)\in(\mathbb{Z}/p^n\mathbb{Z})^\times\times(\mathbb{Z}/p^n\mathbb{Z})^\times} \Big|\frac{1}{p^{n/2}}\sum_{x\in I} e_{p^n}(ax + b\overline{x})\Big|^4 \ll \frac{n|I|^2}{\varphi(p^n)^2}.$$

Proof of Proposition 5.5. Expanding the fourth power, one is led to

$$\mathsf{M}_4(I) = \frac{1}{\varphi(p^n)^2 p^{2n}} \sum_{(x_1,x_2,x_3,x_4)\in I^4} \Big(\sum_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} e_{p^n}\big(a(x_1 + x_2 - x_3 - x_4)\big)\Big) \Big(\sum_{b\in(\mathbb{Z}/p^n\mathbb{Z})^\times} e_{p^n}\big(b(\overline{x_1} + \overline{x_2} - \overline{x_3} - \overline{x_4})\big)\Big).$$

The orthogonality of additive characters ensures that

$$\sum_{c\in(\mathbb{Z}/p^n\mathbb{Z})^\times} e_{p^n}(cz) = p^n\delta_{z\equiv 0 \bmod p^n} - p^{n-1}\delta_{z\equiv 0 \bmod p^{n-1}}$$

for any z in $\mathbb{Z}/p^n\mathbb{Z}$. Thus,

$$\mathsf{M}_4(I) = \frac{1}{\varphi(p^n)^2} \sum_{\substack{(x_1,x_2,x_3,x_4)\in I^4,\\ x_1+x_2\equiv x_3+x_4 \bmod p^n,\\ \overline{x_1}+\overline{x_2}\equiv\overline{x_3}+\overline{x_4} \bmod p^n}} 1 - \frac{1}{\varphi(p^n)^2 p} \sum_{\substack{(x_1,x_2,x_3,x_4)\in I^4\\ x_1+x_2\equiv x_3+x_4 \bmod p^n\\ \overline{x_1}+\overline{x_2}\equiv\overline{x_3}+\overline{x_4} \bmod p^{n-1}}} 1$$
$$- \frac{1}{\varphi(p^n)^2 p} \sum_{\substack{(x_1,x_2,x_3,x_4)\in I^4,\\ x_1+x_2\equiv x_3+x_4 \bmod p^{n-1},\\ \overline{x_1}+\overline{x_2}\equiv\overline{x_3}+\overline{x_4} \bmod p^n}} 1 + \frac{1}{\varphi(p^n)^2 p^2} \sum_{\substack{(x_1,x_2,x_3,x_4)\in I^4,\\ x_1+x_2\equiv x_3+x_4 \bmod p^{n-1},\\ \overline{x_1}+\overline{x_2}\equiv\overline{x_3}+\overline{x_4} \bmod p^{n-1}}} 1.$$

Proposition 5.4 completes the proof. □

5.3. The tightness condition via Kolmogorov's criterion.

Proposition 5.6 (Tightness). *Let $n \geq 2$ be an integer. The sequence of $C^0([0,1],\mathbb{C})$-valued random variables $\mathsf{Kl}_{p^n}(*;(*,*))$ on the random space $(\mathbb{Z}/p^n\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z})^\times$ where p is an odd prime number is tight.*

Proof of Proposition 5.6. Let us show that if $0 \leq s,t \leq 1$ then

$$\frac{1}{\varphi(p^n)^2} \sum_{(a,b)\in(\mathbb{Z}/p^n\mathbb{Z})^\times\times(\mathbb{Z}/p^n\mathbb{Z})^\times} |\mathsf{Kl}_{p^n}(t;(a,b)) - \mathsf{Kl}_{p^n}(s;(a,b))|^4 \ll n|t-s|^2, \quad (5.5)$$

where the implied constant is absolute. The bound (5.5) is enough by Proposition A.1 to ensure the tightness of the sequence of $C^0([0,1],\mathbb{C})$-valued random variables $\mathsf{Kl}_{p^n}(*;(*,*))$ as p tends to infinity among the odd prime numbers. One can assume that $0 \leq s < t \leq 1$.

First range: $0 \leq t-s \leq 1/(\varphi(p^n)-1)$. So that

$$p^n \leq \frac{4}{t-s}. \quad (5.6)$$

Let us show that

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

which implies (5.5) in this range. Let us assume that

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

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

First case:

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

In this case,

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

by (2.2) and (5.6).

Second case:

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

where $2 \leq j \leq \varphi(p^n) - 1$. In this case,

$$|\mathsf{Kl}_{p^n}(t;(a,b)) - \mathsf{Kl}_{p^n}(s;(a,b))| \leq |\mathsf{Kl}_{p^n}(t;(a,b)) - z_j((a,b);p^n)| + |z_j((a,b);p^n) - \mathsf{Kl}_{p^n}(s;(a,b))|.$$

The first term is less than

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

whereas the second term is less than

$$|\alpha_{j-1}((a,b);p^n)|\Big(\frac{j-1}{\varphi(p^n)-1} - s\Big).$$

Altogether,

$$|\mathsf{Kl}_{p^n}(t;(a,b)) - \mathsf{Kl}_{p^n}(s;(a,b))| \leq \frac{\varphi(p^n)-1}{p^{n/2}}(t-s) \leq 2\sqrt{t-s}$$

by (2.2) and (5.6).

Second range: $t - s \geq 1/(\varphi(p^n) - 1)$. So that

$$p^n \geq \frac{1}{t-s}. \tag{5.7}$$

Let us assume that

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

where $1 \leq j \leq k-1 \leq \varphi(p^n) - 2$. In other words,

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

By (4.10) and Hölder's inequality,

$$\frac{1}{\varphi(p^n)^2} \sum_{(a,b)\in(\mathbb{Z}/p^n\mathbb{Z})^\times\times(\mathbb{Z}/p^n\mathbb{Z})^\times} |\mathsf{Kl}_{p^n}(t;(a,b)) - \mathsf{Kl}_{p^n}(s;(a,b))|^4 = \mathsf{M}_4(I_{s,t}) + O\Big(\frac{1}{p^{2n}}\Big) = \mathsf{M}_4(I_{s,t}) + O((t-s)^2),$$

where $I_{s,t}$ is the non-empty interval in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ given by

$$\big(x_j(s) = \varphi(p^n)s + j - 1., .x_k(t) = \varphi(p^n)t + k - 1\big] \cap (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Its length satisfies

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

since $(\varphi(p^n)-1)(t-s)\geq 1$. Proposition 5.5 implies (5.5). □

6. Proof of Theorem A and Theorem B

Let us prove Theorem A. By Proposition 3.1, the random variable Kl has moments to all orders. Thus, we are allowed to use the method of moments. Proposition 4.1 leads to the result.

Theorem B is implied by Theorem A.3, Theorem A and Proposition 5.6.

A. Probabilistic tools

This section contains some probabilistic results needed in this work. The main reference for both the statements and their proof is [10].

Let us say a few words about random variables with values in the Banach space $C^0([0,1],\mathbb{C})$ of $\mathbb{C}$-valued continuous function on $[0,1]$ endowed with the supremum norm. Confer [10, Section B.9] for more details. For each $n\geq 1$, let X_n be a random variable on the random space $(\Omega_n,\mathcal{A}_n,\mathbb{P}_n)$ with values in $C^0([0,1],\mathbb{C})$. Let X be a $C^0([0,1],\mathbb{C})$-valued random variable.

The sequence $(X_n)_{n\geq 1}$ converges to X in the sense of *finite distributions* if for all integers $k\geq 1$ and all k-tuples $(t_1,\dots,t_k)$ with

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

the sequence of $\mathbb{C}^k$-valued random vectors $(X_n(t_1),\dots,X_n(t_k))$ converge in law to the random vector $(X(t_1),\dots,X(t_k))$.

The sequence $(X_n)_{n\geq 1}$ converges in *law* to X if for any $\mathbb{C}$-valued continuous and bounded map φ on the Banach space $C^0([0,1],\mathbb{C})$, the sequence of complex numbers $(\mathbb{E}(\varphi(X_n)))_{n\geq 1}$ converges to $\mathbb{E}(\varphi(X))$.

Each X_n induces a probability measure μ_n on the Banach space by

$$\forall A\subset C^0([0,1],\mathbb{C}),\quad \mu_n(A)=\mathbb{P}_n(X_n^{-1}(A)).$$

The sequence $(X_n)_{n\geq 1}$ is said to be *tight* if for any $\epsilon>0$, there exists a compact subset K of $C^0([0,1],\mathbb{C})$ satisfying

$$\forall n\geq 1,\quad \mu_n(K)\geq 1-\epsilon.$$

A practical criterion for tightness is due to Kolmogorov.

Proposition A.1 (Kolmogorov's criterion for tightness). *If there exists* $\alpha > 0$ *and* $\delta > 0$ *so that*

$$\forall (s,t) \in [0,1]^2, \quad \mathbb{E}\big(|X_n(s) - X_n(t)|^\alpha\big) \ll |s-t|^{1+\delta}$$

then $(X_n)_{n\geq 1}$ *is tight.*

Remark A.2. This is [10, Proposition B.9.5, p. 82].

Last but not least, the main tool of this work is Prokhorov's criterion for convergence in law in $C^0([0,1],\mathbb{C})$.

Theorem A.3 (Prokhorov's criterion). *If* $(X_n)_{n\geq 1}$ *converges to* X *in the sense of finite distributions and* $(X_n)_{n\geq 1}$ *is tight then* $(X_n)_{n\geq 1}$ *converges in law in the sense of* $C^0([0,1],\mathbb{C})$*-valued random variables.*

Remark A.4. This is [10, Theorem B.9.4, p. 82].

References

[1] J. Bober, L. Goldmakher, A. Granville, and K. Soundararajan, The frequency and the structure of large character sums, *preprint*, 2013.

[2] J. W. Bober and L. Goldmakher, The distribution of the maximum of character sums, *Mathematika*, **59** (2013), no. 2, 427–442. Zbl 1316.11075 MR 3081779

[3] K. Gong, W. Veys, and D. Wan, Power moments of Kloosterman sums, *J. Number Theory*, **164** (2016), 103–126. Zbl 06568157 MR 3474381

[4] A. Granville and K. Soundararajan, Large character sums: pretentious characters and the Pólya-Vinogradov theorem, *J. Amer. Math. Soc.*, **20** (2007), no. 2, 357–384. Zbl 1210.11090 MR 2276774

[5] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, 53, American Mathematical Society, Providence, RI, 2004. Zbl 1059.11001 MR 2061214

[6] J.-P. Kahane, *Some random series of functions*, second edition, Cambridge Studies in Advanced Mathematics, 5, Cambridge University Press, Cambridge, 1985. Zbl 0571.60002 MR 833073

[7] N. M. Katz, *Sommes exponentielles*, Course taught at the University of Paris, Orsay, Fall 1979. With a preface by Luc Illusie. Notes written by Gérard Laumon, With an English summary, Astérisque, 79, Société Mathématique de France, Paris, 1980. Zbl 0469.12007 MR 617009

[8] D. Kelmer, Distribution of twisted Kloosterman sums modulo prime powers, *Int. J. Number Theory*, **6** (2010), no. 2, 271–280. Zbl 1217.11074 MR 2646758

[9] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second edition, Graduate Texts in Mathematics, 58, Springer-Verlag, New York, 1984. Zbl 0364.12015 MR 754003

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

[11] E. Kowalski and G. Ricotta, Fourier coefficients of $GL(N)$ automorphic forms in arithmetic progressions, *Geom. Funct. Anal.*, **24** (2014), no. 4, 1229–1297. Zbl 1307.11051 MR 3248485

[12] E. Kowalski and W. F. Sawin, Kloosterman paths and the shape of exponential sums, *Compos. Math.*, **152** (2016), no. 7, 1489–1516. Zbl 06619364 MR 3530449

[13] D. H. Lehmer, Incomplete Gauss sums, *Mathematika*, **23** (1976), no. 2, 125–135. Zbl 0346.10020 MR 429787

[14] J. H. Loxton, The graphs of exponential sums, *Mathematika*, **30** (1983), no. 2, 153–163 (1984). Zbl 0517.10040 MR 737174

[15] J. H. Loxton, The distribution of exponential sums, *Mathematika*, **32** (1985), no. 1, 16–25. Zbl 0574.10042 MR 817102

[16] H. Weyl, Zur Abschätzung von $\zeta(1 + ti)$, *Math. Z.*, **10** (1921), 88–101. Zbl 48.0346.01

Received November 06, 2016

G. 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

E. Royer, Laboratoire de Mathématiques, Campus universitaire des Cézeaux,
3 place Vasarely, TSA 60026, CS 60026, 63178 Aubière Cedex, France
E-mail: emmanuel.royer@uca.fr