Kloosterman paths of prime powers moduli

Emmanuel ROYER
in collaboration with Guillaume RICOTTA and igor SHPARLINSKI

Unless otherwise specified, p denotes a prime number other than 2.

Contents

Date: 2023, January 23rd.

1. Where are Kloosterman coming from?

1.1. **Poincaré series.**

Source: [Kow10, IK04]

If a group Γ acts on a set X, a general interesting problem is the construction of complex valued functions on X invariant under the action of Γ, in other words, functions $f : X \to \mathbb{C}$ such that

$$\forall \gamma \in \Gamma \ \ \forall x \in X \qquad f(\gamma x) = f(x).$$

Assume that we have at our disposal a normal subgroup B of Γ and a function $F : X \to \mathbb{C}$ that is invariant under the action of B, then the *averaging process* allow to build

$$x \mapsto \sum_{g \in B\backslash\Gamma} F(gx)$$

that is Γ-invariant... if the sum is actually convergent which is less likely the smaller B is, and therefore the easier it is to find F!

Let's be a bit more specific and take for X the upper-half plane $\mathcal{H}$, for Γ any congruence subgroup

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z}) : N \mid c \right\}.$$

acting on $\mathcal{H}$ by $z \mapsto \frac{az+b}{cz+d}$. For B take the stabilizer of the cusp $i\infty$ given by

$$\Gamma_{i\infty} = \left\{ \pm \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) : n \in \mathbb{Z} \right\}.$$

For any integer m, the function

$$\begin{array}{rccc} \mathrm{e}_m & : & \mathcal{H} & \to & \mathbb{C} \\ & & z & \mapsto & \mathrm{e}^{2\pi i m z} \end{array}$$

is invariant by $\Gamma_{i\infty}$. The averaging process would lead to consider

$$z \mapsto \sum_{g \in \Gamma_{i\infty}\backslash\Gamma_0(N)} \mathrm{e}_m(gz).$$

However, there is no value of m for which this function is absolutely convergent.

Poincaré got the intuition that it would be more easy to build automorphic functions of even weight k, meaning $f : \mathcal{H} \to \mathbb{C}$ such that

$$\forall g \in \Gamma_0(N) \ \ \forall z \in \mathcal{H} \qquad f(gz) = j(g,z)^k f(z) \qquad j\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z\right) = cz + d$$

and to deduce an invariant function by taking the quotient of two automorphic functions. The corresponding averaged function is the now names Poincaré series after he intriduced them in a paper (published in 1911, after his death):

$$P_m(z) = \sum_{g \in \Gamma_{i\infty} \backslash \Gamma_0(N)} j(g,z)^{-k}\, \mathrm{e}_m(gz).$$

For $m < 0$, the series does not converge, for $m = 0$ we get the important Eisenstein series (fully described by the Eisenstein series on $\mathrm{SL}(2,\mathbb{Z})$) but shall not focus on them and so we assume $m \geq 1$ and $k \geq 4$ also for convergence reasons.

The Poincaré series is automorphic of weight k. Its Fourier expansion is given by

$$P_m(z) = \sum_{n=1}^{+\infty} \widehat{P_m}(n)\, \mathrm{e}_n(z)$$

where

$$\widehat{P_m}(n) = \delta(m,n) + 2\pi \mathrm{i}^k \left(\frac{n}{m}\right)^{(k-1)/2} \sum_{\substack{c=1 \\ N|c}}^{+\infty} \frac{\mathrm{S}(m,n;c)}{c} J_{k-1}\left(4\pi \frac{\sqrt{mn}}{c}\right).$$

Here

- J_ℓ is the J Bessel function defined for example by $\sum_{r=0}^{+\infty} \frac{(-1)^r}{r!(r+\ell)!} \left(\frac{z}{2}\right)^{\ell+2r}$
- S is the Kloosterman sum

$$\mathrm{S}(m,n;c) = \sum_{\substack{d\,(c) \\ (d,c)=1 \\ d\overline{d}=1\,(c)}} \mathrm{e}\left(\frac{md + n\overline{d}}{c}\right) \qquad (\mathrm{e}(\ ) = \mathrm{e}_1(\ )).$$

This is essentially a consequence of the Poisson summation formula.

The Poincaré series are of crucial importance in the analytic number theory of modular forms since their set spans the finite dimensional space of the cuspidal modular forms of weight k over $\Gamma_0(N)$, thanks to the following formula: if f is a cuspidal modular form of weight k over

$\Gamma_0(N)$, then its Fourier expansion is

$$f(z) = \sum_{n=1}^{+\infty} \frac{(4\pi n)^{k-1}}{(k-2)!} \langle f, P_n \rangle \, \mathrm{e}_n(z) \qquad \langle f, P_n \rangle = \int_{\Gamma_0(N)\backslash\mathcal{H}} f(z)\overline{P_n(z)} y^k \frac{\mathrm{d}x\,\mathrm{d}y}{y^2}$$

($\langle\,,\,\rangle$ is the Petersson scalar product). By elementary linear algebra, a basis space of the space of cuspidal modular forms of weight k over $\Gamma_0(N)$ should exist made of Poincaré series. However, it is not even known if some Poincaré series are indeed identically vanishing. Nor a description of the linear relations between Poincaré series is known. These problems are mentionned by Iwaniec [Iwa97, p. 54]. Rhoades [Rho12] relates the question of the description of linear relations with the existence of a so-called weakly holomorphic forms with prescribed principal part. To my knowledge at least, no explicit linear relation between Poincaré series is however known yet (for general weight and N. For values of k sufficiently small so that no nonzero cuspidal form exist, the Poincaré series vanish identically ; see also [CS17, Theorem 8.2.3]).

The Fourier expansion of the Poincaré series and the expression of the Fourier implies the following so-called “Petersson trace formula" that is the departure point of most of the analytical studies of modular forms:

$$\frac{(k-2)!}{(4\pi\sqrt{mn})^{k-1}} \sum_{f\in H_k(N)} \frac{\widehat{f}(n)\overline{\widehat{f}(m)}}{\|f\|^2} = \delta(m,n) + 2\mathrm{i}\pi^{-k} \sum_{\substack{c=1\\ N|c}}^{+\infty} \frac{S(m,n;c)}{c} J_{k-1}\left(\frac{4\pi\sqrt{mn}}{c}\right).$$

where $H_k(N)$ is any orthonormal basis of the space of cuspidal forms of weight k over $\Gamma_0(N)$.

1.2. **Kloosterman variant of the circle method.**

Source: [Kow10, Iwa97]

In 1926, Kloosterman developed a version of the circle method to estimate the number of solutions $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ of the equation

$$a_1x_1^2 + a_1x_1^2 + a_1x_1^2 + a_1x_1^2 = n \qquad (a_1, a_2, a_3, a_4, n) \in \mathbb{Z}^5_{>0}. \qquad (1.1)$$

His estimation rely on a estimation of $S(m,n;c)$ that he deduced from an evaluation of the fourth moment

$$V_4(p)=\sum_{a\,(p)}^{\times} S(a,1;p)^4,\quad p \text{ prime}$$

He computed $V_4(p)=2p^3-3p^2-3p-1$ and got

$$|S(a,1;p)|<2p^{3/4}.$$

From this, he obtained that the number of solutions of (1.1) is

$$\frac{\pi^2}{\sqrt{a_1a_2a_3a_4}}nS(n)+O\left(n^{17/18+\varepsilon}\right)$$

where $S(n)$ is the so-called singular series whose size varies between $\log\log(n)^{-1}$ and $\log\log(n)$.

The computation of explicit forms of the moments of $S(a,1;p)$ is still an ongoing task. For a survey of what is knonwn and new results, see a recent work by Sayed & Kalita [SK23].

2. Bounds

If $c=\prod_{p|c}p^{v_p(c)}$, let $c_p=c/p^{v_p(c)}$, then we have a multiplicative relation

$$S(m,n;c)=\prod_{p|c}S\left(m\overline{c_p}^2,n;p^{v_p(c)}\right),\quad c_p\overline{c_p}=1\ (p^{v_p(c)}).$$

We now focus on $S(m,n;p^\alpha)$.

If m and n are coprime with p, if $c\geq 1$, then

$$S\left(p^am,p^bn,p^c\right)=\begin{cases}p^aS\left(mn,1;p^{c-a}\right) & \text{if } a=b<c\\ p^{\min(a,b,c)}\left(1-\frac{1}{p}\right)^{\delta(c\leq\min(a,b))}\mu\left(p^{c-\min(a,b,c)}\right) & \text{otherwise.}\end{cases}$$

We now focus on $S(m,1;p^\alpha)$.

Assume $a\geq 2$, then

$$S(m,1;p^a)=\sum_{x=1}^{p^a-1}{}^{\times}\,\mathrm{e}\left(\frac{mx+\overline{x}}{p^a}\right).$$

Write uniquely $x = h + jp^{a-1}$ with $0 \le j \le p-1$ and $1 \le h \le p^{a-1}-1$, we have $\overline{x} = \overline{h} - j\overline{h}^2 p^{a-1}$ (here, we use $a \ge 2$), and hence

$$S(m,1;p^a) = \sideset{}{^\times}\sum_{h=1}^{p^{a-1}-1} \mathrm{e}\left(\frac{mh+\overline{h}}{p^a}\right) \sum_{j=0}^{p-1} \mathrm{e}\left(\frac{m-\overline{h}^2}{p}\right)^j$$

$$= p \sideset{}{^\times}\sum_{\substack{h=1 \\ m=\overline{h}^2\ (p)}}^{p^{a-1}-1} \mathrm{e}\left(\frac{mh+\overline{h}}{p^a}\right)$$

In particular, $S(m,1;p^a)$ is zero if m is not a square modulo p.

Remark. Since the kernel of the homomorphism $x \mapsto x^2$ of $\left(\mathbb{Z}/p^a\right)^\times$ is $\{-1,1\}$, exactly half of the sums $S(m,1;p^a)$ vanish. These sums with a non square modulo p will be called *trivially vanishing*.

If m is a nonzero square modulo p (and hence also a square modulo p^a), let $m = s^2\ (p^a)$, we have

$$S(m,1;p^a) = 2\sqrt{p^a}\cos\left(4\pi\frac{s}{p^a} + \theta_{p,a}\right) \begin{cases} 1 & \text{if } a \text{ is even} \\ \left(\dfrac{s}{p}\right) & \text{if } a \text{ is odd} \end{cases}$$

where

$$\theta_{s,p} = \begin{cases} 0 & \text{if } a \text{ is even or } p = 1\ (4) \\ \dfrac{\pi}{2} & \text{if } a \text{ is odd and } p = 3\ (4). \end{cases}$$

In particular

$$\forall m\ \ \forall p \ne 2\ \ \forall a \ge 2 \qquad \left|S(m,1;p^a)\right| \le 2\sqrt{p^a}. \tag{2.1}$$

If $a = 1$, the situation is more complex. We note that

$$S(m,1;p) = \sum_{x \in \mathbb{F}_p^\times} \mathrm{e}\left(\frac{mx+\overline{x}}{p}\right) = \sum_{x \in \mathbb{F}_p^\times} \psi\left(mx+\overline{x}\right)$$

where $\psi : x \mapsto \mathrm{e}(x/p)$ is a character of the *additive* group $\mathbb{F}_p$ and we introduce

$$S(m,q) = \sum_{x \in \mathbb{F}_q} \Psi_{\mathbb{F}_q/\mathbb{F}_p}\left(mx+\overline{x}\right) \quad q \text{ power of } p$$

where $\Psi_{\mathbb{F}_q/\mathbb{F}_p} = \psi \circ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ is a character of the additive group $\mathbb{F}_q$. It follows from the proof by Weil of the Riemann hypothesis for curves over finite fields that

$$-\frac{S(m,q)}{\sqrt{q}} = \mathrm{Tr}\, D_{m,q} = 2\left(\alpha_{m,q} + \overline{\alpha_{m,q}}\right) \qquad \left(\left|\alpha_{m,q}\right| = 1\right)$$

for some conjuguacy class $D_{m,q}$ of $U_2(\mathbb{C})$; In particular, since $S(m,1;p) = S(m,p)$, we can remove the assumption on a in (2.1) and get

$$\forall m \ \ \forall p \neq 2 \ \ \forall a \geq 1 \qquad \left|S(m,1;p^a)\right| \leq 2\sqrt{p^a}.$$

Finally, we introduce the normalised Kloosterman sums

$$\mathrm{Kl}(a,b;q) = \frac{1}{\sqrt{q}} S(a,b;q) = \frac{1}{\sqrt{q}} \sum_{\substack{x\ (q) \\ x\overline{x}=1}} \mathrm{e}\left(\frac{ax+b\overline{x}}{q}\right)$$

for any power q of a prime number.

3. Kloosterman paths

We want to understand how the exponentials sum to the Kloosterman sum. A bit more precisely, if a and b are chosen randomly, how behave the sequence of partial sums that lead to $\mathrm{Kl}(a,b;p^n)$?

Enumerating the representatives of $\{x\ (p^n) : (x,p) = 1\}$ in $\{1,\dots,p^n-1\}$ with the usual order of $\mathbb{Z}$, we build a sequence

$$x_1 < \dots < x_{\varphi(p^n)}.$$

The corresponding polynomial path is the concatenation of the closed segments

$$\frac{1}{\sqrt{p^n}} \left[\sum_{\substack{x \leq x_1 \\ (x,p)=1}} \mathrm{e}\left(\frac{ax+b\overline{x}}{p^n}\right), \sum_{\substack{x \leq x_2 \\ (x,p)=1}} \mathrm{e}\left(\frac{ax+b\overline{x}}{p^n}\right) \right], \dots$$

$$\dots, \frac{1}{\sqrt{p^n}} \left[\sum_{\substack{x \leq x_{\varphi(p^n)-1} \\ (x,p)=1}} \mathrm{e}\left(\frac{ax+b\overline{x}}{p^n}\right), \sum_{\substack{x \leq x_{\varphi(p^n)} \\ (x,p)=1}} \mathrm{e}\left(\frac{ax+b\overline{x}}{p^n}\right) \right].$$

We compute an affine parametrisation of these segments and deduce a continuous map:

$$\begin{array}{ccc} [0,1] & \to & \mathbb{C} \\ t & \mapsto & \mathrm{Kl}_{p^n}(t;(a,b)). \end{array}$$

Note that $\mathrm{Kl}_{p^n}(0;(a,b)) = \frac{1}{\sqrt{p^n}}\mathrm{e}\left(\frac{a+b}{p^n}\right)$ and $\mathrm{Kl}_{p^n}(1;(a,b)) = \mathrm{Kl}(a,b;p^n)$.

The parameters a and b can be seen as living in $\left(\mathbb{Z}/p^n\right)^\times$ and we endow $\left(\mathbb{Z}/p^n\right)^\times \times \left(\mathbb{Z}/p^n\right)^\times$ with the uniform probability measure

$$\mathrm{Prob}(A) = \frac{1}{\varphi(p^n)^2}\#A \qquad A \subset \left(\mathbb{Z}/p^n\right)^\times \times \left(\mathbb{Z}/p^n\right)^\times.$$

For any a and b, the map $t \mapsto \mathrm{Kl}_{p^n}(t;(a,b))$ is in $\mathrm{C}^0([0,1],\mathbb{C})$. If this space is given the supremum norm, it can be seen as a Banach space.

Finally, we an consider the following *random variable*:

$$\begin{array}{rccc} \mathrm{Kl}_{p^n} : & \left(\mathbb{Z}/p^n\right)^\times \times \left(\mathbb{Z}/p^n\right)^\times & \to & \mathrm{C}^0([0,1],\mathbb{C}) \\ & (a,b) & \mapsto & t \mapsto \mathrm{Kl}_{p^n}(t;(a,b)). \end{array}$$

What can be said about the convergence of this random variable?

The question has been first studied by Kowalski & Sawin [KS16] for the case of prime modulus. Their proof involves Deligne's work on the Riemann hypothesis for finite fields as well as many additional results in algebraic and geometric number theory. With Ricotta [RR18], I extended the study to the cas of prime power modulus. Contrary to the prime case, we do not use deep results on algebraic geometry since we have at our disposal an explicit formula. The cost is however an important complexity on arithmetics, combinatorics and analysis.

We prove the following. Let $n \geq 2$ be fixed, as $p \to +\infty$ among prime numbers, the random variable Kl_{p^n} converges in law to an *explicit* $\mathrm{C}^0([0,1],\mathbb{C})$-valued random variable Kl_∞ that we shall described a bit latter.

It must be noted that the limit random variable does not depend on n. However, is is not the same than the one obtained by Kowalski

& Sawin. This is further evidence that Kloosterman sums behave differently depending on whether the module is prime or not.

An rephrasing of our result is the following: for any continuous bounded functions $\Psi\colon \mathrm{C}^0([0,1],\mathbb{C})\to\mathbb{C}$, we have

$$\lim_{p\to+\infty}\frac{1}{\varphi(p^n)^2}\sum_{(a,b)\in\left(\mathbb{Z}/p^n\right)^\times\times\left(\mathbb{Z}/p^n\right)^\times}\Psi\left(t\mapsto \mathrm{Kl}_{p^n}(t;(a,b))\right)=\mathbb{E}(\Psi(\mathrm{Kl}_\infty)).$$

For example, fix $g\in\mathrm{C}^0(\mathbb{C},\mathbb{C})$ bounded and consider

$$\begin{array}{rccc}\Psi_g & : & \mathrm{C}^0([0,1],\mathbb{C}) & \to & \mathbb{C}\\ & & f & \to & g(f(1))\end{array}$$

then

$$\lim_{p\to+\infty}\frac{1}{\varphi(p^n)^2}\sum_{(a,b)\in\left(\mathbb{Z}/p^n\right)^\times\times\left(\mathbb{Z}/p^n\right)^\times}g\left(\mathrm{Kl}(a,b;p^n)\right)=\mathbb{E}(g(\mathrm{Kl}_\infty(1))).$$

Let us describe the limit variable Kl_∞. Let $\left(U_q\right)_q$ be a sequence of independent identically distributed random variables of probability law

$$\begin{aligned}\forall f\in\mathrm{C}^0([0,1],\mathbb{C})\quad \mu(f)&=\frac{1}{2}\delta_0(f)+\mu_1(f)\\ &=\frac{1}{2}f(0)+\frac{1}{2\pi}\int_{-2}^{2}f(x)\frac{\mathrm{d}x}{\sqrt{4-x^2}}\end{aligned}$$

then, Kl_∞ is the $\mathrm{C}^0([0,1],\mathbb{C})$-random variable defined by the almost convergent (and hence in law) random series:

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

In the case of prime modulus considered by Kowalski & Sawin, the result is the same with $\left(U_q\right)_q$ replaced by a sequence of independent identically distributed random variables of probability law

$$\forall f\in\mathrm{C}^0([0,1],\mathbb{C})\quad \mu_{\mathrm{ST}}(f)=\frac{1}{2\pi}\int_{-2}^{2}f(x)\sqrt{4-x^2}\,\mathrm{d}x.$$

Let us continue our example. We have $\mathbb{E}\big(\Psi_g(\mathrm{Kl}_\infty)\big) = \mathbb{E}\,(g\,(\mathrm{Kl}_\infty(1)))$. We compute

$$\mathrm{Kl}_\infty(1) = U_0 + \sum_{h\in\mathbb{Z}^*} \underbrace{\frac{\mathrm{e}(ht)-1}{2\pi i h}}_{=0} U_h = U_0$$

so $\mathbb{E}\big(\Psi_g(\mathrm{Kl}_\infty)\big) = \mathbb{E}\,(g(U_0))$ and finally

$$\lim_{p\to+\infty} \frac{1}{\varphi\,(p^n)^2} \sum_{(a,b)\in\left(\mathbb{Z}/p^n\right)^\times\times\left(\mathbb{Z}/p^n\right)^\times} g\big(\mathrm{Kl}(a,b;p^n)\big)$$
$$= \frac{1}{2}g(0) + \frac{1}{2\pi}\int_{-2}^{2} g(t)\frac{\mathrm{d}t}{\sqrt{4-t^2}}.$$

In other words, we recover a result essentially found by Kelmer [Kel10]. again, the case of prime moduli is a consequence of Deligne's theory and is due to Katz. Note that the dual equidistribution problem:

$$\text{fix } a \text{ and } b \text{ and compute } \lim_{x\to+\infty} \frac{1}{\#\{p^n\le x\}} \sum_{p^n\le x} g\big(\mathrm{Kl}(a,b;p^n)\big)$$

remains an open problem.

We have considered a random variable on $\left(\mathbb{Z}/p^n\right)^\times \times \left(\mathbb{Z}/p^n\right)^\times$, that is on the two parameters a and b. However, we have seen in the introduction that the Kloosterman sums are essentially described by a single parameter. A natural question is then to fix the parameter b, let us say to the value b_0 and to consider the random variable

$$\begin{array}{rccc} \mathrm{Kl}_{b_0,p^n} & : & \left(\mathbb{Z}/p^n\right)^\times & \to & \mathrm{C}^0\,([\,0,1],\mathbb{C}) \\ & & a & \mapsto & t\mapsto \mathrm{Kl}_{p^n}\,(t;(a,b_0))\,. \end{array}$$

We prove with Ricotta & Shparlinski [RRS20] the following. Let $n\ge 31$ be fixed, as $p\to+\infty$ among prime numbers, the random variable Kl_{b_0,p^n} converges in law to Kl_∞. This is indeed to be considered as a substantial strengthening since, for example, the case when $n=1$ remains open: Kowalski & Sawin can only prove, for $\mathrm{Kl}_{b_0,p}$ a weaker convergence (convergence in the sense of finite distributions).

In our results, we fixed n and let p grow. We could consider the situation when p is fixed and n grows. We wrote in our papers "the problem, both theoretically and numerically, seems to be of a completely different nature" which we saw as a politically correct way to say we thought it was impossible to do. It appears we were wrong since, Milićević

& Zhang [MZ23] proved last year the following: let p be a fixed odd prime, let a_0 and b_0 be fixed. Then as $n \to +\infty$ among prime numbers, the random variable $\mathrm{Kl}_{a_0,b_0,p^n}$, which is Kl_{b_0,p^n} restricted to

$$\left\{a \in \left(\mathbb{Z}/p^n\right)^\times : a = a_0 \ (p)\right\},$$

converges in law to a limit random variable $\mathrm{Kl}_{a_0,b_0,p,\infty}$ defined the following way:

$$\mathrm{Kl}_{a_0,b_0,p,\infty} = \sum_{\substack{h\in\mathbb{Z}\\ \mathrm{cond}}} \frac{\mathrm{e}(ht)-1}{2\pi \mathrm{i} h} U_h^\sharp$$

where cond is the following " $(a_0-h)b_0$ is an inversible square modulo p", each $U_h^\sharp$ being distributed with respect to the μ_1 measure.

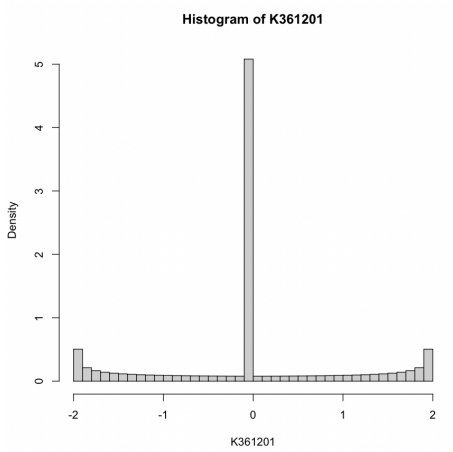
4. A repulsion phenomenon

The result with Shparlinsky implies that

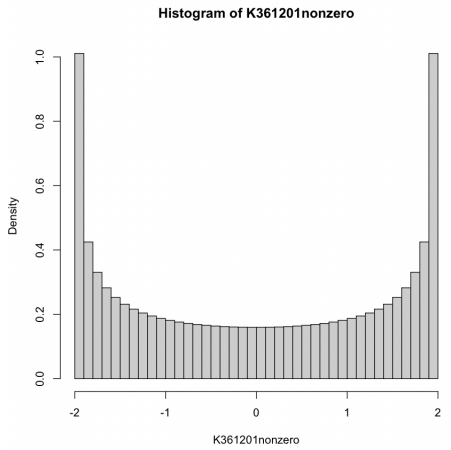
$$\lim_{p\to+\infty} \frac{1}{\varphi(p^n)} \sum_{a\in\left(\mathbb{Z}/p^n\right)^\times} g\left(\mathrm{Kl}(a,1;p^n)\right) = \frac{1}{2}g(0) + \frac{1}{2\pi}\int_{-2}^{2} g(t)\frac{\mathrm{d}t}{\sqrt{4-t^2}}.$$

Half of the values of a lead to a zero Kloosterman sum (see Remark 2), and this is the reason of the term $\frac{1}{2}g(0)$ (or equivalently of the $\frac{1}{2}\delta_0$ in the definition of μ. In other word the Kloosterman sums that do not trivially vanish (*i.e.* corresponding to a squares modulo p) distribute according to the measure $\frac{1}{\pi}\frac{\mathrm{d}t}{\sqrt{4-t^2}}$. Equivalently

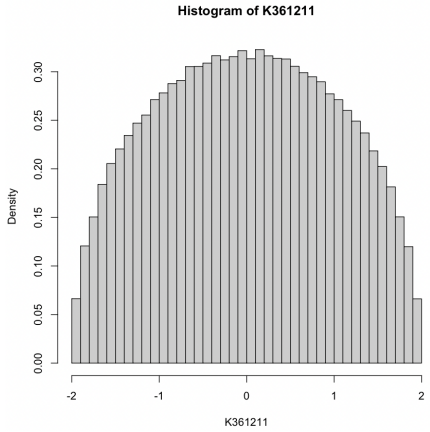
$$\lim_{p\to+\infty} \frac{1}{\#\left\{a \in \left(\mathbb{Z}/p^n\right)^\times : a = \square \ (\mathrm{mod}\ p)\right\}} \sum_{\substack{a\in\left(\mathbb{Z}/p^n\right)^\times\\ a=\square\ (\mathrm{mod}\ p)}} g\left(\mathrm{Kl}(a,1;p^n)\right) = \frac{1}{\pi}\int_{-2}^{2} g(t)\frac{\mathrm{d}t}{\sqrt{4-t^2}}.$$



(a) $q = 361201 = 601^2$



(b) $q = 601^2$ nonsquare a removed



(c) $q = 361211$

Figure 1. Distribution of $a \mapsto \mathrm{Kl}(a, 1; q)$

If we compare this by the distribution of $a \mapsto \mathrm{Kl}(a, 1; p)$ due to Katz:

$$\lim_{p \to +\infty} \frac{1}{\#\left\{a \in \left(\mathbb{Z}/p^n\right)^\times\right\}} \sum_{a \in \left(\mathbb{Z}/p^n\right)^\times} g\left(\mathrm{Kl}(a, 1; p^n)\right) = \frac{1}{\pi} \int_{-2}^{2} g(t) \frac{\mathrm{d}t}{\sqrt{4 - t^2}}.$$

we see that, for prime levels, the Kloosterman sums tend to concentrate around 0, whereas for prime-power levels, they tend to concentrate around ± 2. In the case of prime-power level, the trivially vanishing sums have a repulsion effect on the others. See figures 1.

5. Ideas of proof

We give ideas of proof for the first result, the one where the random variable depends on the two parameters a and b.

To prove the convergence in law, we use the following criterion due to Prokhorov: a sequence $(X_q)_q$ of $\mathrm{C}^0([0,1],\mathbb{C})$-random variables that converges to X in the *sense of finite distribution* and *tight* converges in law.

The sequence $(X_q)_q$ converges to X in the *sense of finite distribution* if:

$$\forall k\ \ \forall 0 \leq t_1 < \ldots < t_k \leq 1\ \ \underbrace{\big(X_q(t_1),\ldots,X_q(t_k)\big)}_{\substack{\text{sequence of } \mathbb{C}^k\text{-}\\ \text{valued random}\\ \text{variables}}} \xrightarrow[q\to+\infty]{\text{law}} (X(t_1),\ldots,X(t_k))$$

or, rephrased,

$$\forall k\ \ \forall 0 \leq t_1 < \ldots < t_k \leq 1\ \ \forall h \in \mathrm{C}^0\left(\mathbb{C}^k,\mathbb{C}\right)$$
$$\mathbb{E}\left(h\left(X_q(t_1)\right),\ldots,h\left(X_q(t_k)\right)\right) \xrightarrow[q\to+\infty]{} \mathbb{E}\left(h\left(X(t_1)\right),\ldots,h\left(X(t_k)\right)\right).$$

For the tightness we give only a criterion due to Kolmogorov: if there exist $\alpha > 0$, $\delta > 0$ and $C > 0$ such that

$$\forall q\ \ \forall (s,t) \in [0,1]^2 \quad \mathbb{E}\left(\left|X_q(s) - X_q(t)\right|^{\alpha}\right) \leq C|s-t|^{1+\delta}$$

then $(X_q)_q$ is *tight*.

To prove the tightness of Kl_{p^n}, we prove that

$$\frac{1}{\varphi(p^n)^2} \sum_{(a,b)\in\left(\mathbb{Z}/p^n\right)^\times\times\left(\mathbb{Z}/p^n\right)^\times} \left|\mathrm{Kl}_{p^n}(t;(a,b)) - \mathrm{Kl}_{p^n}(s;(a,b))\right|^4 \leq Cn|t-s|^2$$

where C is some constant independent on any of the variables. This inequality is proved by careful explicit computation and does not present extraordinary difficulties. This is however deeply related to the fact that we have indeed an explicit expression of the Kloosterman sum.

The main part is the proof of the convergence in the sense of finite distribution, and we can even prove the convergence in the sense

of finite distribution for the one parameter random variable (which implies the one for the two parameters random variable). We use the method of moments, that is we prove the equivalent:

$$\lim_{p\to+\infty}\frac{1}{\varphi(p^n)}\sum_{a\in(\mathbb{Z}/p^n)^\times}\prod_{j=1}^{k}\overline{\mathrm{Kl}_{p^n}\left(t_j;(a,b_0)\right)^{m_j}}\,\mathrm{Kl}_{p^n}\left(t_j;(a,b_0)\right)^{n_j}$$
$$=\mathbb{E}\left(\prod_{j=1}^{k}\overline{\mathrm{Kl}_\infty(t_j)^{m_j}}\,\mathrm{Kl}_\infty(t_j)^{n_j}\right).$$

The first step in the proof is to replace the segments of the Kloosterman paths by a constant function, replacing the continuous function by a step function: we prove that, up to an admissible error term, $\mathrm{Kl}_{p^n}(t;(a,b))$ can be replaced by

$$\widetilde{\mathrm{Kl}_{p^n}}(t;(a,b)):=\sum_{h\in\mathbb{Z}/p^n}\underbrace{\alpha_{p^n}}_{\frac{\mathrm{e}(ht)-1}{2\pi ih}+O\left(\frac{1}{p^n}\right)}\mathrm{Kl}_{p^n}(a-h,b;p^n)$$

So, our proof reduces to the evaluation of

$$\frac{1}{\varphi(p^n)}\sum_{a\in(\mathbb{Z}/p^n)^\times}\prod_{j=1}^{k}\overline{\widetilde{\mathrm{Kl}_{p^n}}\left(t_j;(a,b_0)\right)^{m_j}}\widetilde{\mathrm{Kl}_{p^n}}\left(t_j;(a,b_0)\right)^{n_j}.$$

6. Computing the moments

Our objective is to prove that

$$\frac{1}{\varphi(p^n)}\sum_{a\in(\mathbb{Z}/p^n)^\times}\prod_{j=1}^{k}\overline{\widetilde{\mathrm{Kl}_{p^n}}\left(t_j;(a,b_0)\right)^{m_j}}\widetilde{\mathrm{Kl}_{p^n}}\left(t_j;(a,b_0)\right)^{n_j}$$
$$=\mathbb{E}\left(\prod_{j=1}^{k}\overline{\mathrm{Kl}_\infty(t_j)^{m_j}}\,\mathrm{Kl}_\infty(t_j)^{n_j}\right)+\text{error}.$$

We replace $\widetilde{\mathrm{Kl}_{p^n}}$ by its definition, expand the powers and are led to evaluate sums of terms having the following shape:

$$\frac{1}{\varphi(p^n)}\sum_{a\in(\mathbb{Z}/p^n)^\times}\prod_{\tau\in\mathbb{Z}/p^n}\mathrm{Kl}(a+\tau,b;p^n)^{\mu(\tau)}$$

for some non negative integers $\mu(\tau)$ with bounded sum. We get a principal term

$$\frac{\sharp A_{p^n}(\mu)}{\varphi(p^n)} \prod_{\tau \in \mathbb{Z}/p^n} \delta_{2|\mu(\tau)} \binom{\mu(\tau)}{\mu(\tau)/2}$$

where

$$A_{p^n} = \left\{ a \in \left(\mathbb{Z}/p^n\right)^\times : \forall \tau \in \mathbb{Z}/p^n,\ \mu(\tau) \geq 1 \Rightarrow a + \tau \text{ is a square mod } p^n \right\}.$$

In particular, we find

$$\frac{1}{\varphi(p^n)} \sum_{a \in \left(\mathbb{Z}/p^n\right)^\times} \mathrm{Kl}(a, b; p^n)^m = \underbrace{\frac{\delta_{2|m}}{2} \binom{m}{m/2}}_{\substack{\text{Moment of any real variable of law } \mu}} + \text{error.}$$

Ultimately, the evaluation of $\sharp A_{p^n}(\mu)$ requires the estimation of the number of x (p) such that $x, x+1, \ldots, x+k$ are square modulo p. An estimation has been given by Davenport (1931) [Kat80, §1.4.2] using Weil's proof of the Riemann's hypothesis for curves in its following corollary: let $f \in \mathbb{Z}[X]$, and for $p \neq 2$, consider the following sum of Legendre symbols:

$$S_p(f) = \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p} \right).$$

Assume that f is unitary, without multiple roots in $\mathbb{C}$ and such that its reduction modulo p has no multiple roots in $\overline{\mathbb{F}_p}$. Then

$$\left| S_p(f) \right| \leq (\deg(f) - 1)\sqrt{p}.$$

References

[CS17] Henri Cohen and Fredrik Strömberg. *Modular forms: a classical approach*, volume 179 of *Grad. Stud. Math.* Providence, RI: American Mathematical Society (AMS), 2017.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *Colloq. Publ., Am. Math. Soc.* Providence, RI: American Mathematical Society (AMS), 2004.

[Iwa97] Henryk Iwaniec. *Topics in classical automorphic forms*, volume 17 of *Grad. Stud. Math.* Providence, RI: American Mathematical Society, 1997.

[Kat80] Nicholas M. Katz. *Sommes exponentielles. Cours à Orsay, automne 1979. Redige par Gerard Laumon, preface par Luc Illusie*, volume 79 of *Astérisque*. Société Mathématique de France (SMF), Paris, 1980.

[Kel10] Dubi Kelmer. Distribution of twisted Kloosterman sums modulo prime powers. *Int. J. Number Theory*, 6(2):271–280, 2010.

[Kow10] Emmanuel Kowalski. Poincaré and analytic number theory. In *The scientific legacy of Poincaré. Transl. from the French by Joshua Bowman*, pages 73–85. Providence, RI: American Mathematical Society (AMS); London: London Mathematical Society (LMS), 2010.

[KS16] Emmanuel Kowalski and William F. Sawin. Kloosterman paths and the shape of exponential sums. *Compos. Math.*, 152(7):1489–1516, 2016.

[MZ23] Djordje Milićević and Sichen Zhang. Distribution of Kloosterman paths to high prime power moduli. *Trans. Am. Math. Soc., Ser. B*, 10:636–669, 2023.

[Rho12] Robert C. Rhoades. Linear relations among Poincaré series via harmonic weak Maass forms. *Ramanujan J.*, 29(1-3):311–320, 2012.

[RR18] Guillaume Ricotta and Emmanuel Royer. Kloosterman paths of prime powers moduli. *Comment. Math. Helv.*, 93(3):493–532, 2018.

[RRS20] Guillaume Ricotta, Emmanuel Royer, and Igor Shparlinski. Kloosterman paths of prime powers moduli. II. *Bull. Soc. Math. Fr.*, 148(1):173–188, 2020.

[SK23] Fahim Sayed and Gautam Kalita. Moments of Kloosterman sums, super-characters, and elliptic curves. *Indian J. Pure Appl. Math.*, 54(1):200–209, 2023.

Emmanuel Royer, Université Clermont Auvergne – CNRS, Institut CNRS Pauli – IRL2842, A-1090 WIEN, Autriche

Email address: emmanuel.royer@math.cnrs.fr