Equidistribution of exponential sums indexed by roots of polynomials

Théo Untrau (joint work with Emmanuel Kowalski)

Journées Arithmétiques, Nancy 2023

Plan of the talk

1. Motivation: distribution of the classical Kloosterman sums

2. The case of exponential sums over the roots of $X^d - 1$

3. The case of exponential sums over the roots of an arbitrary polynomial

Notation: $e(t) := e^{2i\pi t}$

Motivation: distribution of the classical Kloosterman sums

Motivation: distribution of the classical Kloosterman sums

For a prime number p, we define Kloosterman sums modulo p as follows:

$$K_p(a,b) = \sum_{x \in \mathbf{F}_p^\times} e\left(\frac{ax + bx^{-1}}{p}\right) \quad \text{for any } a, b \in \mathbf{F}_p.$$

Motivation: distribution of the classical Kloosterman sums

For a prime number p, we define Kloosterman sums modulo p as follows:

$$K_p(a,b) = \sum_{x \in \mathbf{F}_p^\times} e\left(\frac{ax + bx^{-1}}{p}\right) \quad \text{for any } a, b \in \mathbf{F}_p.$$

Examples of applications in number theory

- Kloosterman's variant of the circle method to tackle the problem of representations of large integers by quadratic forms of the form $aX^2 + bY^2 + cZ^2 + dT^2$;
- Fourier coefficients of modular forms, trace formulas.

Motivation: distribution of the classical Kloosterman sums

For a prime number p, we define Kloosterman sums modulo p as follows:

$$K_p(a,b) = \sum_{x \in \mathbf{F}_p^\times} e\left(\frac{ax + bx^{-1}}{p}\right) \qquad \text{for any } a, b \in \mathbf{F}_p.$$

Examples of applications in number theory

- Kloosterman's variant of the circle method to tackle the problem of representations of large integers by quadratic forms of the form $aX^2 + bY^2 + cZ^2 + dT^2$;
- Fourier coefficients of modular forms, trace formulas.

These sums are real numbers, satisfying $|K_p(a,b)| \leqslant p - 1$.

Motivation: distribution of the classical Kloosterman sums

For a prime number p, we define Kloosterman sums modulo p as follows:

$$K_p(a,b) = \sum_{x \in \mathbf{F}_p^\times} e\left(\frac{ax + bx^{-1}}{p}\right) \qquad \text{for any } a, b \in \mathbf{F}_p.$$

Examples of applications in number theory

- Kloosterman's variant of the circle method to tackle the problem of representations of large integers by quadratic forms of the form $aX^2 + bY^2 + cZ^2 + dT^2$;
- Fourier coefficients of modular forms, trace formulas.

These sums are real numbers, satisfying $|K_p(a,b)| \leqslant p-1$.

Weil's bound

If $a, b \in \mathbf{F}_p^\times$,

$$|K_p(a,b)| \leqslant 2p^{1/2}$$

Motivation: distribution of the classical Kloosterman sums

Theorem (Katz, 1988)

The sets of normalized Kloosterman sums $\left\{ \frac{1}{\sqrt{p}} K_p(a,1);\ a \in \mathbf{F}_p^\times \right\}$ become equidistributed in $[-2,2]$ with respect to the Sato–Tate measure

$$\mathrm{d}\mu_{\mathrm{ST}}(x) := \frac{1}{2\pi}\sqrt{4-x^2}\mathrm{d}x$$

as p goes to $+\infty$.

Motivation: distribution of the classical Kloosterman sums

Theorem (Katz, 1988)

The sets of normalized Kloosterman sums $\left\{ \frac{1}{\sqrt{p}} K_p(a,1);\ a \in \mathbf{F}_p^\times \right\}$ become equidistributed in $[-2,2]$ with respect to the Sato–Tate measure

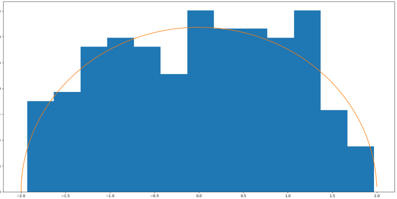
$$\mathrm{d}\mu_{\mathrm{ST}}(x) := \frac{1}{2\pi}\sqrt{4-x^2}\,\mathrm{d}x$$

as p goes to $+\infty$.

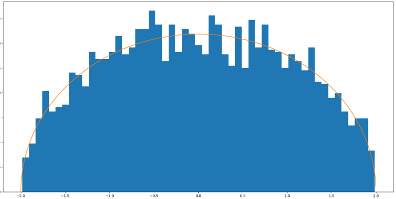
In other words, for any $[c,d] \subseteq [-2,2]$,

$$\frac{\left|\left\{ a \in \mathbf{F}_p^\times;\ \frac{1}{\sqrt{p}} K_p(a,1) \in [c,d] \right\}\right|}{\left|\mathbf{F}_p^\times\right|} \underset{p\to\infty}{\longrightarrow} \frac{1}{2\pi}\int_c^d \sqrt{4-x^2}\,\mathrm{d}x.$$

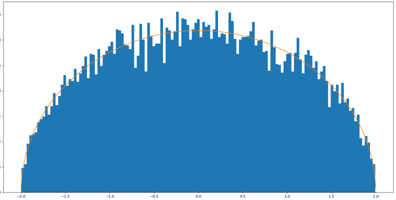
Motivation: distribution of the classical Kloosterman sums



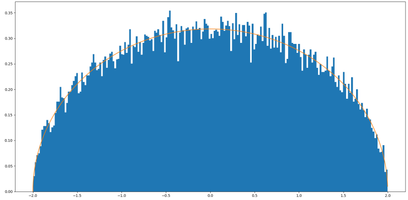
$p = 191$



$p = 2887$



$p = 18367$



$p = 45989$

Distribution of the sums $\frac{1}{\sqrt{p}} K_p(a, 1)$ in $[-2, 2]$ as a varies in $\mathbf{F}_p^\times$, for several values of p.

The case of exponential sums over the roots of $X^d - 1$

Sums over the roots of $X^5 - 1$

Let us consider the following exponential sums

$$\sum_{\substack{x \in \mathbf{F}_p \\ x^5 = 1}} e\left(\frac{ax}{p}\right)$$

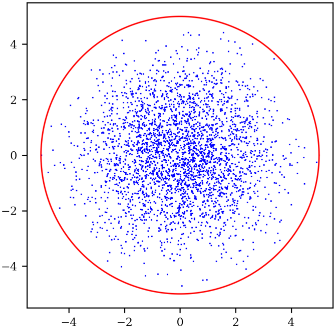
parametrized by $a \in \mathbf{F}_p$, for a prime number $p \equiv 1 \pmod 5$. Which one of the following pictures represents them?

Sums over the roots of $X^5 - 1$

Let us consider the following exponential sums

$$\sum_{\substack{x \in \mathbf{F}_p \\ x^5 = 1}} e\left(\frac{ax}{p}\right)$$

parametrized by $a \in \mathbf{F}_p$, for a prime number $p \equiv 1 \pmod 5$. Which one of the following pictures represents them?

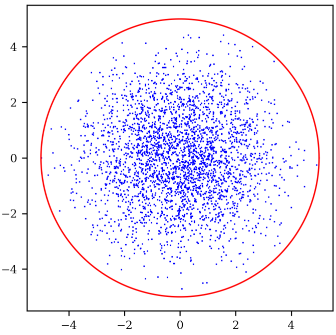


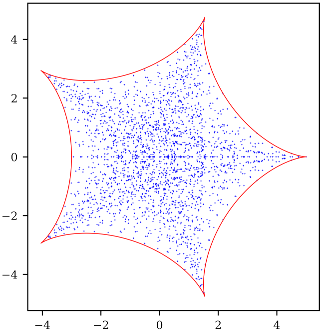
Sums over the roots of $X^5 - 1$

Let us consider the following exponential sums

$$\sum_{\substack{x \in \mathbf{F}_p \\ x^5 = 1}} e\left(\frac{ax}{p}\right)$$

parametrized by $a \in \mathbf{F}_p$, for a prime number $p \equiv 1 \pmod 5$. Which one of the following pictures represents them?





Sums over the roots of $X^d - 1$

Let us consider the following sums

$$S_p(a,d) := \sum_{\substack{x\in\mathbf{F}_p \\ x^d=1}} e\left(\frac{ax}{p}\right)$$

for a fixed integer d and $p \equiv 1 \pmod d$ going to $+\infty$. These sums were studied in two articles of 2015:

Theorem[1,2]

There exists a Laurent polynomial $g_d\colon (\mathbf{S}^1)^{\varphi(d)} \to \mathbf{C}$ such that the sets of sums $\{S_p(a,d);\ a \in \mathbf{F}_p\}$ become equidistributed in the image of g_d with respect to the pushforward measure via g_d of the Haar measure on $(\mathbf{S}^1)^{\varphi(d)}$, as $p \equiv 1 \pmod d$ goes to $+\infty$.

[1] William Duke, Stephan Ramon Garcia and Bob Lutz. The graphic nature of Gaussian periods, Proc. Amer. Math. Soc. 2015.

[2] Stephan Ramon Garcia, Trevor Hyde and Bob Lutz. Gauss's hidden menagerie: from cyclotomy to supercharacters, Notices Amer. Math. Soc. 2015.

Sums over the roots of $X^d - 1$

Summary of the proof

- Pick a generator w_p of the unique subgroup of order d and rewrite the sum in terms of this generator.

Sums over the roots of $X^d - 1$

Summary of the proof

- Pick a generator w_p of the unique subgroup of order d and rewrite the sum in terms of this generator.
- Use the linear relations between powers of w_p to write the sums as a Laurent polynomial g_d in fewer variables, more precisely $\varphi(d)$.

Summary of the proof

- Pick a generator w_p of the unique subgroup of order d and rewrite the sum in terms of this generator.
- Use the linear relations between powers of w_p to write the sums as a Laurent polynomial g_d in fewer variables, more precisely $\varphi(d)$.
- Show the uniform distribution of the remaining $\varphi(d)$ variables in a torus of dimension $\varphi(d)$.

Sums over the roots of $X^d - 1$

Summary of the proof

- Pick a generator w_p of the unique subgroup of order d and rewrite the sum in terms of this generator.
- Use the linear relations between powers of w_p to write the sums as a Laurent polynomial g_d in fewer variables, more precisely $\varphi(d)$.
- Show the uniform distribution of the remaining $\varphi(d)$ variables in a torus of dimension $\varphi(d)$.
- Find a geometric interpretation of the image of $(\mathbf{S}^1)^{\varphi(d)}$ via g_d. For instance when d is prime, the image of g_d is the region of the complex plane delimited by a d-cusp hypocycloid.

The case of exponential sums over the roots of an arbitrary polynomial

Modifying the previous approach

Let us rephrase the key argument of the previous case:

- $\left\{ \left(e\left(\frac{aw_p^k}{p}\right)\right)_{0\leqslant k<\varphi(d)} \;;\; a\in\mathbf{F}_p \right\}$ become equidistributed in $(\mathbf{S}^1)^{\varphi(d)}$.

Modifying the previous approach

Let us rephrase the key argument of the previous case:

- $\left\{ \left(e\left(\frac{aw_p^k}{p}\right)\right)_{0\leqslant k<\varphi(d)} \ ; \ a \in \mathbf{F}_p \right\}$ become equidistributed in $(\mathbf{S}^1)^{\varphi(d)}$.
- $\left\{ \left(e\left(\frac{aw_p^k}{p}\right)\right)_{0\leqslant k<d} \ ; \ a \in \mathbf{F}_p \right\}$ become equidistributed in $\mathrm{H}_d \subseteq (\mathbf{S}^1)^d$.

Modifying the previous approach

Let us rephrase the key argument of the previous case:

- $\left\{ \left(e\left(\frac{aw_p^k}{p}\right)\right)_{0\leqslant k<\varphi(d)} \; ; \; a \in \mathbf{F}_p \right\}$ become equidistributed in $(\mathbf{S}^1)^{\varphi(d)}$.
- $\left\{ \left(e\left(\frac{aw_p^k}{p}\right)\right)_{0\leqslant k<d} \; ; \; a \in \mathbf{F}_p \right\}$ become equidistributed in $\mathrm{H}_d \subseteq (\mathbf{S}^1)^d$.
- The random variable

$$\begin{array}{ccc} \mathbf{F}_p & \to & (\mathbf{S}^1)^d \\ a & \mapsto & \left(e\left(\frac{aw_p^k}{p}\right)\right)_{0\leqslant k<d} \end{array}$$

converges in law to the uniform distribution on H_d.

Modifying the previous approach

Trying not to use the notion of primitive root, let us modify the random variable

$$\begin{array}{rcc} \mathbf{F}_p & \to & (\mathbf{S}^1)^d \\ a & \mapsto & \left(e\left(\frac{aw_p^k}{p}\right)\right)_{0\leqslant k<d} \end{array}$$

Modifying the previous approach

Trying not to use the notion of primitive root, let us modify the random variable

$$\begin{array}{rcc} \mathbf{F}_p & \to & (\mathbf{S}^1)^d \\ a & \mapsto & \left(e\left(\frac{aw_p^k}{p}\right)\right)_{0\leqslant k<d} \end{array}$$

Step 1:

$$\begin{array}{rcc} \mathbf{F}_p & \to & \mathrm{C}(\mu_d(\mathbf{F}_p), \mathbf{S}^1) \\ a & \mapsto & \left| \begin{array}{ccc} \mu_d(\mathbf{F}_p) & \to & \mathbf{S}^1 \\ x & \mapsto & e\left(\frac{ax}{p}\right) \end{array} \right. \end{array}$$

Modifying the previous approach

Trying not to use the notion of primitive root, let us modify the random variable

$$\begin{array}{rcl} \mathbf{F}_p & \to & (\mathbf{S}^1)^d \\ a & \mapsto & \left(e\left(\frac{aw_p^k}{p}\right)\right)_{0\leqslant k<d} \end{array}$$

Step 1:

$$\begin{array}{rcl} \mathbf{F}_p & \to & \mathrm{C}(\mu_d(\mathbf{F}_p), \mathbf{S}^1) \\ a & \mapsto & \left| \begin{array}{rcl} \mu_d(\mathbf{F}_p) & \to & \mathbf{S}^1 \\ x & \mapsto & e\left(\frac{ax}{p}\right) \end{array} \right. \end{array}$$

- Advantage: we no longer use the ordering of the roots!

Modifying the previous approach

Trying not to use the notion of primitive root, let us modify the random variable

$$\begin{array}{rcl} \mathbf{F}_p & \to & (\mathbf{S}^1)^d \\ a & \mapsto & \left(e\left(\frac{aw_p^k}{p}\right)\right)_{0\leqslant k<d} \end{array}$$

Step 1:

$$\begin{array}{rcl} \mathbf{F}_p & \to & \mathrm{C}(\mu_d(\mathbf{F}_p), \mathbf{S}^1) \\ a & \mapsto & \left| \begin{array}{rcl} \mu_d(\mathbf{F}_p) & \to & \mathbf{S}^1 \\ x & \mapsto & e\left(\frac{ax}{p}\right) \end{array} \right. \end{array}$$

- Advantage: we no longer use the ordering of the roots!
- Drawback: These random variables take values in a space that depends on p.

Modifying the previous approach

Step 2: To modify

$$\begin{array}{ccc} \mathbf{F}_p & \to & \mathrm{C}(\mu_d(\mathbf{F}_p), \mathbf{S}^1) \\ a & \mapsto & \left| \begin{array}{ccc} \mu_d(\mathbf{F}_p) & \to & \mathbf{S}^1 \\ x & \mapsto & e\left(\frac{ax}{p}\right) \end{array} \right. \end{array}$$

let us consider

$$\begin{array}{ccc} \mathbf{F}_p & \to & \mathrm{C}(\mu_d(\mathbf{C}), \mathbf{S}^1) \\ a & \mapsto & \left| \begin{array}{ccc} \mu_d(\mathbf{C}) & \to & \mathbf{S}^1 \\ x & \mapsto & e\left(\frac{a\varpi_{\mathfrak{p}}(x)}{p}\right) \end{array} \right. \end{array}$$

Modifying the previous approach

Step 2: To modify

$$\begin{array}{ccc} \mathbf{F}_p & \to & \mathrm{C}(\mu_d(\mathbf{F}_p), \mathbf{S}^1) \\ a & \mapsto & \left| \begin{array}{ccc} \mu_d(\mathbf{F}_p) & \to & \mathbf{S}^1 \\ x & \mapsto & e\left(\frac{ax}{p}\right) \end{array} \right. \end{array}$$

let us consider

$$\begin{array}{ccc} \mathbf{F}_p & \to & \mathrm{C}(\mu_d(\mathbf{C}), \mathbf{S}^1) \\ a & \mapsto & \left| \begin{array}{ccc} \mu_d(\mathbf{C}) & \to & \mathbf{S}^1 \\ x & \mapsto & e\left(\frac{a\varpi_{\mathfrak{p}}(x)}{p}\right) \end{array} \right. \end{array}$$

for all ideals $\mathfrak{p}$ of $K := \mathbf{Q}(\zeta_d)$ lying above p (the condition $p \equiv 1 \pmod{d}$ ensures that $\mathcal{O}_K/\mathfrak{p} \simeq \mathbf{F}_p$).

Modifying the previous approach

Step 2: To modify

$$\begin{array}{ccc} \mathbf{F}_p & \to & \mathrm{C}(\mu_d(\mathbf{F}_p), \mathbf{S}^1) \\ a & \mapsto & \left| \begin{array}{ccc} \mu_d(\mathbf{F}_p) & \to & \mathbf{S}^1 \\ x & \mapsto & e\left(\frac{ax}{p}\right) \end{array} \right. \end{array}$$

let us consider

$$\begin{array}{ccc} \mathbf{F}_p & \to & \mathrm{C}(\mu_d(\mathbf{C}), \mathbf{S}^1) \\ a & \mapsto & \left| \begin{array}{ccc} \mu_d(\mathbf{C}) & \to & \mathbf{S}^1 \\ x & \mapsto & e\left(\frac{a\varpi_{\mathfrak{p}}(x)}{p}\right) \end{array} \right. \end{array}$$

for all ideals $\mathfrak{p}$ of $K := \mathbf{Q}(\zeta_d)$ lying above p (the condition $p \equiv 1 \pmod d$ ensures that $\mathcal{O}_K/\mathfrak{p} \simeq \mathbf{F}_p$).

Conclusion: We no longer use the ordering of the roots, and our random variables take values in the same space.

A well suited framework

Let $g \in \mathbf{Z}[X]$ be a monic and separable polynomial. We introduce the following notations:

- Z_g is the set of complex roots of g;
- $K_g := \mathbf{Q}(\mathrm{Z}_g)$ its splitting field, with ring of integers $\mathbf{O}_g$.
- $\mathcal{S}_g$ is the set of prime ideals of $\mathbf{O}_g$ with residual degree 1 and not dividing the discriminant of g.

Definition of the unitary random variables

For all $\mathfrak{p} \in \mathcal{S}_g$ (lying above p say) we define the random variable

$$U_{\mathfrak{p}} \; : \; \mathbf{O}_g/\mathfrak{p} \to \mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1), \qquad a \mapsto \left| \begin{array}{ccc} \mathrm{Z}_g & \to & \mathbf{S}^1 \\ x & \mapsto & e\left(\frac{a\varpi_{\mathfrak{p}}(x)}{p}\right) \end{array} \right.$$

Convergence in law of the unitary random variables

Theorem (Kowalski–U. 2023)

As $\|\mathfrak{p}\|$ goes to infinity, the random variables $U_{\mathfrak{p}}$ converge in law to the uniform distribution on a certain subgroup H_g of $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$, orthogonal to the $\mathbf{Z}$-module of additive relations between the roots of g.

Convergence in law of the unitary random variables

Theorem (Kowalski–U. 2023)

As $\|\mathfrak{p}\|$ goes to infinity, the random variables $U_{\mathfrak{p}}$ converge in law to the uniform distribution on a certain subgroup H_g of $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$, orthogonal to the $\mathbf{Z}$-module of additive relations between the roots of g.

Definition (module of additive relations)

$$\mathrm{R}_g := \left\{ \alpha \colon \mathrm{Z}_g \to \mathbf{Z} \;\middle|\; \sum_{x \in \mathrm{Z}_g} \alpha(x) x = 0 \right\}$$

Convergence in law of the unitary random variables

Theorem (Kowalski–U. 2023)

As $\|\mathfrak{p}\|$ goes to infinity, the random variables $U_{\mathfrak{p}}$ converge in law to the uniform distribution on a certain subgroup H_g of $\mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$, orthogonal to the $\mathbf{Z}$-module of additive relations between the roots of g.

Definition (module of additive relations)

$$\mathrm{R}_g := \left\{ \alpha\colon \mathrm{Z}_g \to \mathbf{Z} \;\middle|\; \sum_{x \in \mathrm{Z}_g} \alpha(x) x = 0 \right\}$$

Example: If $\mathrm{R}_g = \{0\}$, then $\mathrm{H}_g = \mathrm{C}(\mathrm{Z}_g, \mathbf{S}^1)$.

Equidistribution of exponential sums over roots

Corollary (Kowalski–U. 2023)

As p goes to infinity among the prime numbers totally split in K_g, the sums

$$\sum_{\substack{x \in \mathbf{F}_p \\ g(x) \equiv 0 \pmod{p}}} e\left(\frac{ax}{p}\right);$$

become equidistributed in $\mathbf{C}$ with respect to a measure μ_g that is related to the module of additive relations between the roots of g.

Equidistribution of exponential sums over roots

Corollary (Kowalski–U. 2023)

As p goes to infinity among the prime numbers totally split in K_g, the sums

$$\sum_{\substack{x \in \mathbf{F}_p \\ g(x) \equiv 0 \pmod{p}}} e\left(\frac{ax}{p}\right);$$

become equidistributed in $\mathbf{C}$ with respect to a measure μ_g that is related to the module of additive relations between the roots of g.

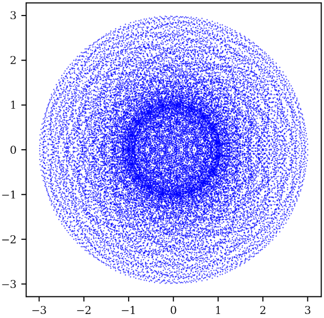
Example: If $\mathrm{R}_g = \{0\}$, then the sums above become equidistributed with respect ot the law of the sum of $\deg(g)$ independent Steinhaus random variables.

Illustration

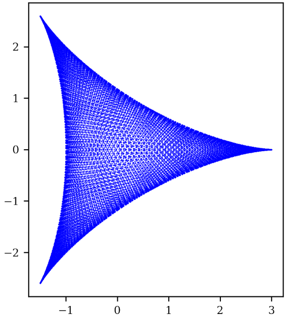
The two pictures below represent

$$\left\{ \sum_{x \in \mathrm{Z}_g(\mathbf{F}_p)} e\left(\frac{ax}{p}\right) ;\ a \in \mathbf{F}_p \right\}$$

for two different choices of polynomial g of degree 3.

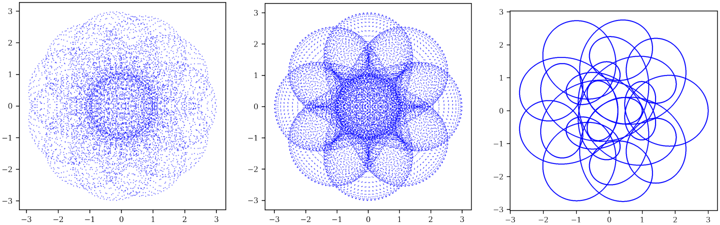


$g = X^3 + 2X^2 + 3$
$p = 30113$



$g = X^3 + X + 3$
$p = 30223$

Thank you for your attention!



- Emmanuel Kowalski and Théo Untrau, Ultra-short sums of trace functions, available on arXiv.