Equidistribution of exponential sums

Théo Untrau

Under the supervision of Florent Jouve and Guillaume Ricotta

1. Introduction

Exponential sums are sums of roots of unity which can be defined in a very elementary way. As sums of complex numbers of absolute value 1, they can always be trivially bounded by their number of terms. However, in most situations one expects the arguments of the complex numbers involved in the sum to cancel, so that the absolute value of the resulting sum is smaller than the trivial bound. Finding a non-trivial bound can be a very difficult question, but it often comes with a concrete number theoretic result such as the ones we present below. The many applications to concrete problems in number theory serve as a strong motivation for a refined study of exponential sums. Beyond the question of finding upper or lower bounds for their absolute value, there are many questions one can ask about the asymptotic distribution of exponential sums (possibly after some rescaling), and which have led to beautiful results during the last decades.

2. Some number theoretic applications of exponential sums

Let p be a prime number. In this poster, we will define *exponential sums* over the finite field $\mathbf{F}_p$ as sums of the form

$$\sum_{\substack{x\in\mathbf{F}_p\\ g(x)\not\equiv 0 \bmod p}} e_p\left(\frac{f(x)}{g(x)}\right), \tag{1}$$

where $f, g \in \mathbf{Z}[X]$ are two fixed polynomials, and $e_p(z)$ denotes $\exp\left(\frac{2i\pi}{p}z\right)$ for all $z \in \mathbf{C}$.

Gauss sums and quadratic reciprocity

Recall the definition of the Legendre symbol modulo a prime p: for all $x \in \mathbf{F}_p$,

$$\left(\frac{x}{p}\right) := \begin{cases} 0 \text{ if } x = 0 \\ 1 \text{ if there exists } y \in \mathbf{F}_p \text{ such that } x = y^2 \\ -1 \text{ if there does not exist } y \in \mathbf{F}_p \text{ such that } x = y^2. \end{cases}$$

If one takes $f(X) = X^2$ and $g(X) = 1$ in (1) one obtains the so-called *Gauss sums*:

$$\sum_{x\in\mathbf{F}_p} e_p\left(x^2\right).$$

Considerations on these sums lead to a proof of the *quadratic reciprocity law*, which states that if p and q are two distinct odd prime numbers, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Point counting on varieties defined over finite fields

For any prime p and any $a \in \mathbf{F}_p$, consider the following "sphere modulo p":

$$S(a,p) := \left\{(x,y,z) \in \mathbf{F}_p^3 \mid x^2 + y^2 + z^2 = a\right\}.$$

Then writing

$$\mathbb{1}_{S(a,p)}(x,y,z) = \frac{1}{p}\sum_{b\in\mathbf{F}_p} e_p\left(b\left(x^2+y^2+z^2-a\right)\right)$$

and summing over x, y, z gives:

$$|S(a,p)| = \frac{1}{p}\sum_{b\in\mathbf{F}_p} \tau(b)^3 e_p(-ab),$$

where $\tau(b) = \sum_{x\in\mathbf{F}_p} e_p\left(bx^2\right)$. The equality $|\tau(b)| = \sqrt{p}$, which holds as soon as $b \not\equiv 0 \bmod p$, allows one to obtain the following asymptotic:

$$|S(a,p)| \underset{p\to\infty}{=} p^2 + O\left(p^{\frac{3}{2}}\right).$$

This example illustrates how exponential sums can be related to point counting problems over finite fields.

Representation of integers by diagonal quadratic forms

It is known since Lagrange that every natural number can be represented as the sum of four integer squares. In other words, the quadratic form $X^2 + Y^2 + Z^2 + T^2$ represents any natural number. However, is it still true if one introduces some positive integer coefficients, thus turning the quadratic form into one of the form $Q(X,Y,Z,T) = aX^2 + bY^2 + cZ^2 + dT^2$? Of course, if a, b, c and d are simultaneously even, $Q(x,y,z,t)$ is even for any $(x,y,z,t) \in \mathbf{Z}^4$, but unless there is such a congruence obstruction, can any integer be represented by Q? This question was addressed by Kloosterman in [4], and he proved an asymptotic formula for the number of representations of a sufficiently large integer n by Q, that is: the number of $(x,y,z,t) \in \mathbf{Z}^4$ such that $Q(x,y,z,t) = n$. The proof relies on a variant of the *circle method* developed by Hardy, Ramanujan and Littlewood a few years before in the context of Waring's problem. Some exponential sums which are now named after Kloosterman play a key role in the proof, and we present them in the next section.

3. Bounds on the absolute value of Kloosterman sums

The exponential sums which appear in [4] are defined for any prime p and any integers a and b as

$$\mathrm{K}_p(a,b) := \sum_{x\in\mathbf{F}_p^\times} e_p\left(ax + bx^{-1}\right). \tag{2}$$

They correspond to the choice of $f(X) = aX^2 + b$ and $g(X) = X$ in equation (1). These sums are real numbers, and the triangle inequality gives the estimate $|\mathrm{K}_p(a,b)| \leqslant p - 1$.

Kloosterman's bound

By considerations on the 4th moment of the family $\{\mathrm{K}_p(a,b);\ a,b \in \mathbf{F}_p\}$, Kloosterman was able to reduce the question of finding an upper bound for these sums to an elementary counting problem. He obtained the following bound:

$$|\mathrm{K}_p(a,b)| \leqslant 2p^{\frac{3}{4}} \quad \text{for all } a,b \in \mathbf{F}_p^\times.$$

This power saving of $1/4$ compared to the trivial bound was sufficient to conclude on his question. However, this bound is now known not to be optimal.

Weil's bound

A consequence of Weil's work on the Riemann hypothesis for curves over finite fields is the upper bound

$$\left|\mathrm{K}_p(a,b)\right| \leqslant 2\sqrt{p} \quad \text{for all } a,b \in \mathbf{F}_p^\times. \tag{3}$$

4. A note on probabilistic aspects

The picture obtained when drawing the path connecting the successive partial sums of the Kloosterman sum (2) suggests that the map $x \mapsto ax + bx^{-1}$ behaves quite randomly at the level of representatives of $\mathbf{F}_p^\times$ in $\{0, \dots, p-1\}$.

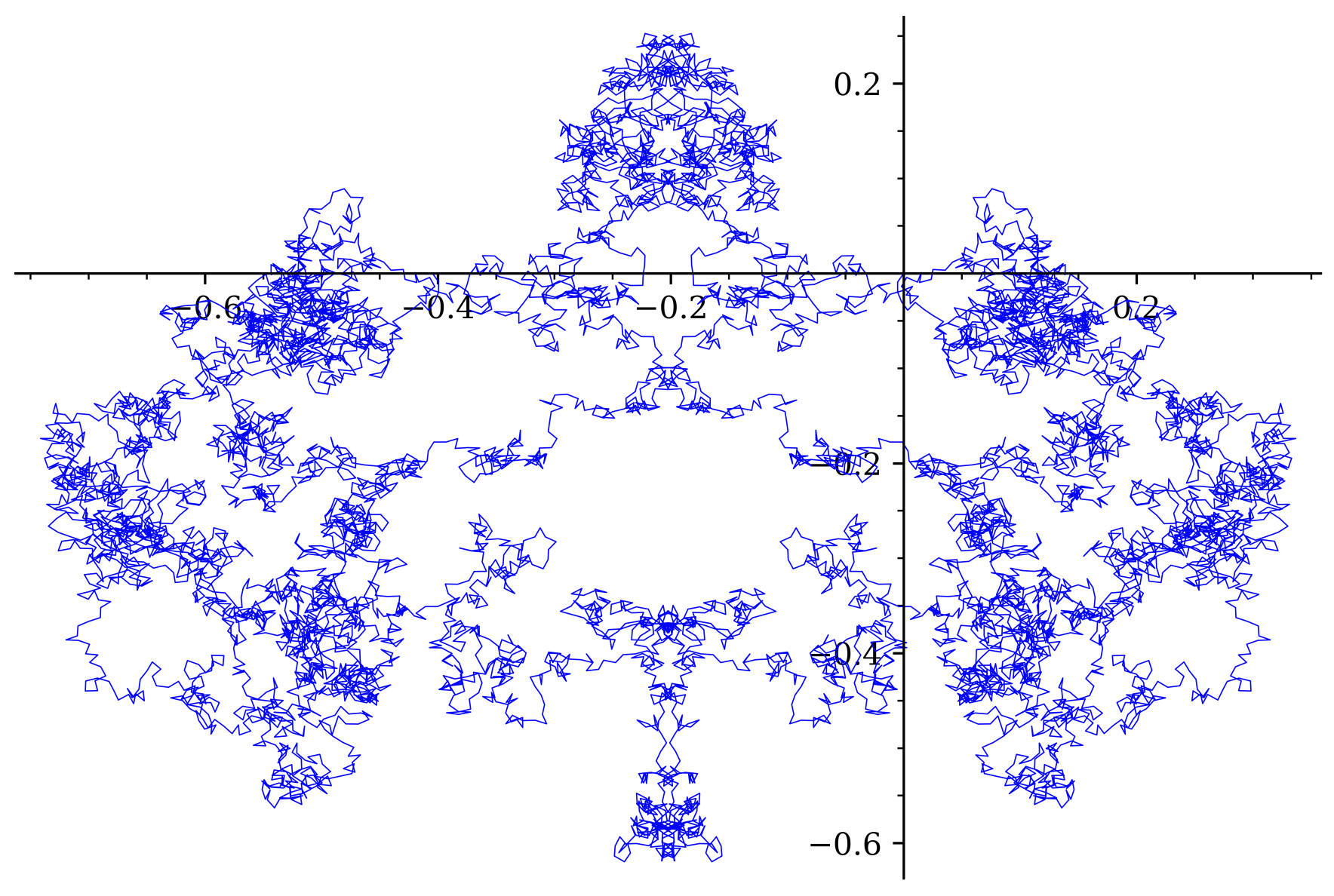

Figure 1: The path between the successive partial sums of $\frac{1}{\sqrt{p}}\mathrm{K}_p(1,1)$ for $p = 9001$.

Therefore, it is tempting to try to model $\mathrm{K}_p(a,b)$ by a sum

$$S_p := \sum_{j=1}^{p-1} X_j \tag{4}$$

of independent random variables X_j, where each of them is uniformly distributed on $\mathbf{S}^1$. Then the central limit theorem tells us that $S_p/\sqrt{p}$ converges in law to a Gaussian random variable, so that $|S_p|$ is "typically of size $\sqrt{p}$". Therefore, the *square root cancellation* encapsulated in Weil's bound is expected from a probabilistic point of view. However, the fact that $\frac{1}{\sqrt{p}}|\mathrm{K}_p(a,b)|$ is *always* less than or equal to 2 tells us that the random walk in the above picture is not so well approximated by the path connecting partial sums of a sum of type (4), and that the algebraic definition of the Kloosterman sums eventually impose constraints on the walk.

There is actually an equidistribution result for the paths connecting partial sums of Kloosterman sums. In [5], Kowalski and Sawin proved the convergence in law of these paths (viewed as random variables taking values in a space of continuous functions) towards an explicit random series.

5. Katz equidistribution theorem

Thanks to Weil's bound (3), we know that for any prime p, the set $\left\{\frac{1}{\sqrt{p}}\mathrm{K}_p(a,1);\ a \in \mathbf{F}_p^\times\right\}$ is contained in $[-2,2]$. The question of the distribution of the normalized Kloosterman sums in this interval was answered by Katz in [3], and the precise result he obtained is the following:

As $p \to \infty$, the sets $\left\{\frac{1}{\sqrt{p}}\mathrm{K}_p(a,1);\ a \in \mathbf{F}_p^\times\right\}$ become equidistributed in $[-2,2]$ with respect to the Sato-Tate measure:

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

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

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

Figure 2 below illustrates this asymptotic behaviour (the red curve is the graph of $x \mapsto \frac{1}{2\pi}\sqrt{4-x^2}$).

6. Exponential sums indexed by a subgroup

For a fixed integer d and primes $p \equiv 1 \bmod d$, one can define the Kloosterman sums *restricted to the subgroup of order* d as

$$\mathrm{K}_p(a,b,d) := \sum_{\substack{x\in\mathbf{F}_p\\ x^d=1}} e_p\left(ax + bx^{-1}\right).$$

These sums, viewed as a family with varying parameters a and b, have striking visual features which have been partially investigated in [1]. They proved equidistribution results in a d-cusp hypocycloid when d is a prime number (see Figure 3). Similar statements are also proved in [2], where $e_p\left(ax + bx^{-1}\right)$ is replaced by $e_p(ax)$. Sums indexed by the subgroup of order d of $(\mathbf{Z}/p^\alpha\mathbf{Z})^\times$ for $\alpha \geqslant 2$ also satisfy the same properties, provided $p \equiv 1 \bmod d$.

The subject of my thesis is the study of such equidistribution questions for families of "short exponential sums" (meaning exponential sums restricted to specific subsets of $\mathbf{F}_p$ or $\mathbf{Z}/p^\alpha\mathbf{Z}$).

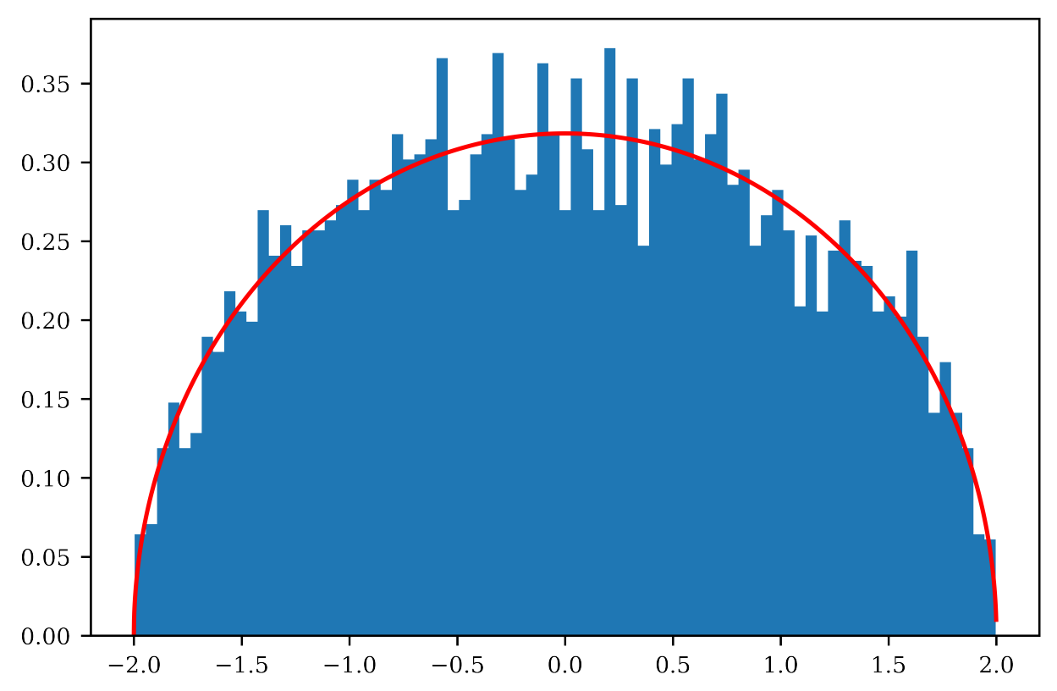

Figure 2: Distribution of the values $\frac{1}{\sqrt{6007}}\mathrm{K}_{6007}(a,1)$ in $[-2,2]$ as a ranges in $\mathbf{F}_{6007}^\times$.

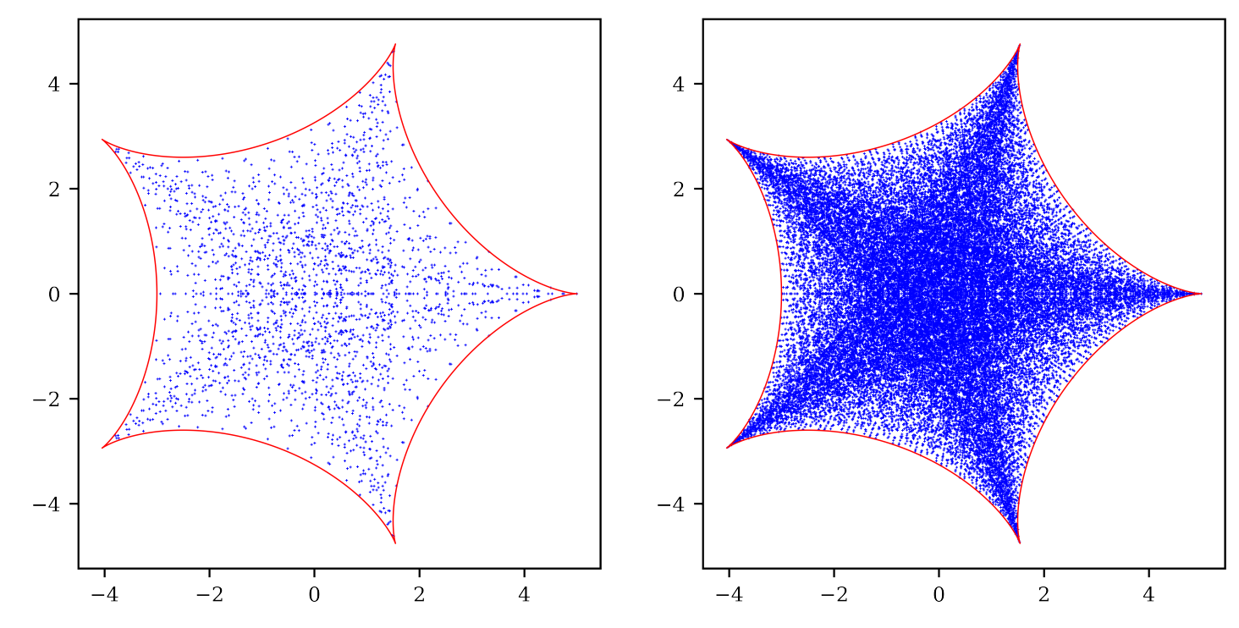

Figure 3: The sets $\left\{\mathrm{K}_p(a,b,5);\ a,b \in \mathbf{F}_p\right\}$ for $p = 151$ and $p = 631$.

References

[1] Paula Burkhardt, Alice Zhuo-Yu Chan, Gabriel Currier, Stephan Ramon Garcia, Florian Luca, and Hong Suh. Visual properties of generalized Kloosterman sums. *J. Number Theory*, 2016.

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

[3] Nicholas M. Katz. *Gauss sums, Kloosterman sums, and monodromy groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1988.

[4] H. D. Kloosterman. On the Representation of Numbers in the Form $ax^2 + by^2 + cz^2 + dt^2$. *Proc. London Math. Soc.*, 1926.

[5] Emmanuel Kowalski and William F. Sawin. Kloosterman paths and the shape of exponential sums. *Compos. Math.*, 2016.