

Equidistribution of Exponential Sums

Gabriel Ribeiro

École polytechnique

Summary

1. Exponential sums in nature
2. Cohomology to the rescue!
3. Deligne's equidistribution theorem
4. The general equidistribution result
5. Let's work out the case of Gauss' sums

Exponential sums in nature

Can we solve polynomial equations?

Foundational problem in NT: given $f \in \mathbb{Z}[x_1, \dots, x_n]$, describe the set of solutions (in \mathbb{Z} or \mathbb{Q}) of $f(x) = 0$.

Can we solve polynomial equations?

Foundational problem in NT: given $f \in \mathbb{Z}[x_1, \dots, x_n]$, describe the set of solutions (in \mathbb{Z} or \mathbb{Q}) of $f(x) = 0$. Is this set finite or infinite? If it is finite, what is its cardinality? If it's infinite, can we describe some numbers which "generate" all the solutions in some sense?

Can we solve polynomial equations?

Foundational problem in NT: given $f \in \mathbb{Z}[x_1, \dots, x_n]$, describe the set of solutions (in \mathbb{Z} or \mathbb{Q}) of $f(x) = 0$. Is this set finite or infinite? If it is finite, what is its cardinality? If it's infinite, can we describe some numbers which "generate" all the solutions in some sense?

Very often, these questions are way out of reach for our methods. This leads us to consider solutions mod p of the desired equations.

Can we solve polynomial equations?

Foundational problem in NT: given $f \in \mathbb{Z}[x_1, \dots, x_n]$, describe the set of solutions (in \mathbb{Z} or \mathbb{Q}) of $f(x) = 0$. Is this set finite or infinite? If it is finite, what is its cardinality? If it's infinite, can we describe some numbers which "generate" all the solutions in some sense?

Very often, these questions are way out of reach for our methods. This leads us to consider solutions mod p of the desired equations.

Let us then define a function $\text{Sol}(f, p, t)$ which counts the number of solutions to $f(x) \equiv t \pmod{p}$.

Taking a Fourier transform

We lose no information if we consider $t \mapsto \text{Sol}(f, p, t)$ as complex-valued and if we take its Fourier transform.

Taking a Fourier transform

We lose no information if we consider $t \mapsto \text{Sol}(f, p, t)$ as complex-valued and if we take its Fourier transform. This Fourier transform is given by

$$\psi \mapsto \sum_{t \in \mathbb{F}_p} \psi(t) \text{Sol}(f, p, t) = \sum_{x \in \mathbb{F}_p^n} \psi(f(x)).$$

Taking a Fourier transform

We lose no information if we consider $t \mapsto \text{Sol}(f, p, t)$ as complex-valued and if we take its Fourier transform. This Fourier transform is given by

$$\psi \mapsto \sum_{t \in \mathbb{F}_p} \psi(t) \text{Sol}(f, p, t) = \sum_{x \in \mathbb{F}_p^n} \psi(f(x)).$$

Since $\widehat{\mathbb{F}_p} = \mathbb{F}_p$, every character is of the form $\psi_a(x) := \exp(2\pi i ax/p)$.

Taking a Fourier transform

We lose no information if we consider $t \mapsto \text{Sol}(f, p, t)$ as complex-valued and if we take its Fourier transform. This Fourier transform is given by

$$\psi \mapsto \sum_{t \in \mathbb{F}_p} \psi(t) \text{Sol}(f, p, t) = \sum_{x \in \mathbb{F}_p^n} \psi(f(x)).$$

Since $\widehat{\mathbb{F}_p} = \mathbb{F}_p$, every character is of the form $\psi_a(x) := \exp(2\pi i ax/p)$. Via this identification, the function above is none other than

$$a \mapsto \sum_{x \in \mathbb{F}_p^n} \exp\left(\frac{2\pi i a f(x)}{p}\right);$$

an exponential sum!

Let's properly define ES

In order to deal systematically with exponential sums, let us give a proper definition which encompasses the previous sum and many interesting others.

Definition - Exponential sum

Let k be a finite field and X be a finite-type scheme over k . An **exponential sum** is a sum of the form

$$S(f, E, \chi) := \sum_{x \in X(E)} \chi(f(x)),$$

where E/k is a finite extension, G is a commutative algebraic group, χ is a character of $G(E)$, and $f : X \rightarrow G$ is a morphism of schemes.

We're still counting solutions!

As before, we remark that

$$\begin{aligned}\widehat{G}(E) &\rightarrow \mathbb{C} \\ \chi &\mapsto \sum_{x \in X(E)} \chi(f(x))\end{aligned}$$

is the Fourier transform of

$$\begin{aligned}G(E) &\rightarrow \mathbb{C} \\ t &\mapsto \#\{x \in X(E) \mid f(x) = t\}.\end{aligned}$$

This point of view also allows us to put numerous number-theoretic questions under the umbrella of exponential sums.

This point of view also allows us to put numerous number-theoretic questions under the umbrella of exponential sums.

The case where χ is the trivial character is already interesting and highly non-trivial.

Let's consider an example

Take X as the elliptic curve defined by $y^2 = 4x^3 - x - 1$. We denote by $N(X, q)$ the number of \mathbb{F}_q -points of X and wonder how the numbers $N(X, q)$ vary as a function of q .

Let's consider an example

Take X as the elliptic curve defined by $y^2 = 4x^3 - x - 1$. We denote by $N(X, q)$ the number of \mathbb{F}_q -points of X and wonder how the numbers $N(X, q)$ vary as a function of q .

In analytic number theory, we usually divide the analysis into two cases: either we consider only the cases where q varies between the prime numbers (which are not 2 or 13), or we fix one such prime p and make q vary among the numbers of the form p^n , for some n .

Vertical distribution

We begin with the latter. Ever since Artin's thesis in the 1920's, it is known that there exist two complex numbers α_p and β_p , satisfying $\alpha_p\beta_p = p$, such that

$$N(X, p^n) = p^n + 1 - \alpha_p^n - \beta_p^n$$

for all $n \geq 1$.

We begin with the latter. Ever since Artin's thesis in the 1920's, it is known that there exist two complex numbers α_p and β_p , satisfying $\alpha_p \beta_p = p$, such that

$$N(X, p^n) = p^n + 1 - \alpha_p^n - \beta_p^n$$

for all $n \geq 1$.

In particular, to determine $N(X, p^n)$ for all n , it suffices to know $N(X, p)$.

The former case is much harder. By the Hasse bound, we know that

$$|N(X, p) - (p + 1)| \leq 2\sqrt{p}$$

and so there exists a unique "angle" $\theta_p \in [0, \pi]$ such that

$$N(X, p) - (p + 1) = 2\sqrt{p} \cos(\theta_p).$$

How do the angles vary?

Our question is then: how the angles θ_p vary as a function of p .

How do the angles vary?

Our question is then: how the angles θ_p vary as a function of p .

If X is an elliptic curve with complex multiplication, it's known since Deuring's 1955 paper *Die Zetafunktion einer algebraischen Kurve von Geschlechte Eins* that the θ_p are uniformly distributed in $[0, \pi]$.

How do the angles vary?

Our question is then: **how the angles θ_p vary as a function of p .**

If X is an elliptic curve with complex multiplication, it's known since Deuring's 1955 paper *Die Zetafunktion einer algebraischen Kurve von Geschlechte Eins* that the θ_p are uniformly distributed in $[0, \pi]$.

Our elliptic curve, however, does not have complex multiplication (its j -invariant is not an algebraic integer, for example).

The distribution of angles θ_p for elliptic curves without complex multiplication was the subject of a famous conjecture of Sato and Tate, which says that the sequence (θ_p) is equidistributed in $[0, \pi]$ for the Sato-Tate measure $\mu_{ST} := (2/\pi) \sin^2 \theta \, d\theta$.

The distribution of angles θ_p for elliptic curves without complex multiplication was the subject of a famous conjecture of Sato and Tate, which says that the sequence (θ_p) is equidistributed in $[0, \pi]$ for the Sato-Tate measure $\mu_{ST} := (2/\pi) \sin^2 \theta \, d\theta$.

This conjecture very recently became a theorem by Clozel, Barnet-Lamb, Geraghty, Harris, Sheperd-Barron and Taylor, whose proof builds from all the arithmetic geometry used on the modularity theorem.

The distribution of angles θ_p for elliptic curves without complex multiplication was the subject of a famous conjecture of Sato and Tate, which says that the sequence (θ_p) is equidistributed in $[0, \pi]$ for the Sato-Tate measure $\mu_{ST} := (2/\pi) \sin^2 \theta \, d\theta$.

This conjecture very recently became a theorem by Clozel, Barnet-Lamb, Geraghty, Harris, Sheperd-Barron and Taylor, whose proof builds from all the arithmetic geometry used on the modularity theorem.

Several natural variants and generalizations remain wide-open.

Cohomology to the rescue!

The hero of our story is the theory of étale cohomology and, more precisely, Deligne's groundbreaking paper [La Conjecture de Weil II](#). Since this is a huge machinery, we will begin by explaining its main features.

The hero of our story is the theory of étale cohomology and, more precisely, Deligne's groundbreaking paper [La Conjecture de Weil II](#). Since this is a huge machinery, we will begin by explaining its main features.

- Let $k = \mathbb{F}_q$, where $q = p^n$;

The hero of our story is the theory of étale cohomology and, more precisely, Deligne's groundbreaking paper [La Conjecture de Weil II](#). Since this is a huge machinery, we will begin by explaining its main features.

- Let $k = \mathbb{F}_q$, where $q = p^n$;
- $\ell \neq p$ a prime number;

The hero of our story is the theory of étale cohomology and, more precisely, Deligne's groundbreaking paper [La Conjecture de Weil II](#). Since this is a huge machinery, we will begin by explaining its main features.

- Let $k = \mathbb{F}_q$, where $q = p^n$;
- $\ell \neq p$ a prime number;
- X a smooth geometrically connected variety over k .

The étale fundamental group

Since the Zariski topology is so coarse, lots of spaces of interest have a trivial fundamental group.

The étale fundamental group

Since the Zariski topology is so coarse, lots of spaces of interest have a trivial fundamental group. In other words, the usual tools from algebraic topology are not adapted to the study of these varieties.

The étale fundamental group

Since the Zariski topology is so coarse, lots of spaces of interest have a trivial fundamental group. In other words, the usual tools from algebraic topology are not adapted to the study of these varieties.

This led Grothendieck to define the **étale fundamental group** $\pi_1(X)$, a profinite group that classifies the finite étale covers of X .

The étale fundamental group is independent of a base point up to inner automorphism.

The étale fundamental group is independent of a base point up to inner automorphism. As in topology, a morphism of schemes $f : X \rightarrow Y$ induces a morphism

$$f_* : \pi_1(X) \rightarrow \pi_1(Y).$$

The étale fundamental group is independent of a base point up to inner automorphism. As in topology, a morphism of schemes $f : X \rightarrow Y$ induces a morphism

$$f_* : \pi_1(X) \rightarrow \pi_1(Y).$$

Moreover, if $X = \text{Spec } k$, its fundamental group is nothing but the absolute Galois group of k .

In our case, where k is \mathbb{F}_q , this is the free profinite group $\widehat{\mathbb{Z}}$ on one canonical generator given by

$$\overline{\mathbb{F}}_q \rightarrow \overline{\mathbb{F}}_q, \quad x \mapsto x^q.$$

In our case, where k is \mathbb{F}_q , this is the free profinite group $\widehat{\mathbb{Z}}$ on one canonical generator given by

$$\overline{\mathbb{F}}_q \rightarrow \overline{\mathbb{F}}_q, \quad x \mapsto x^q.$$

This is the so-called **arithmetic Frobenius**. As we'll see, its inverse, denoted by Frob_k and called **geometric Frobenius**, will play a key role in the theory.

In topology, the category of local systems is equivalent to the category of finite-dimensional representations of the fundamental group by taking the fiber of a local system on a fixed point.

In topology, the category of local systems is equivalent to the category of finite-dimensional representations of the fundamental group by taking the fiber of a local system on a fixed point. This suggests the following definition.

Definition - Local system

An ℓ -adic local system \mathcal{L} of rank r over X is a continuous representation $\rho : \pi_1(X) \rightarrow \mathrm{GL}_r(\overline{\mathbb{Q}}_\ell)$.

Given a finite extension E of k , we may define a **trace function** $\mathrm{tr}_{\mathcal{L}} : X(E) \rightarrow \overline{\mathbb{Q}_\ell}$ in the following way:

Given a finite extension E of k , we may define a **trace function** $\mathrm{tr}_{\mathcal{L}} : X(E) \rightarrow \overline{\mathbb{Q}_\ell}$ in the following way: a point $x \in X(E)$ is a morphism $\mathrm{Spec} E \rightarrow X$, and so induces a map

$$\mathrm{Gal}(E) \rightarrow \pi_1(X).$$

Given a finite extension E of k , we may define a **trace function** $\mathrm{tr}_{\mathcal{L}} : X(E) \rightarrow \overline{\mathbb{Q}}_{\ell}$ in the following way: a point $x \in X(E)$ is a morphism $\mathrm{Spec} E \rightarrow X$, and so induces a map

$$\mathrm{Gal}(E) \rightarrow \pi_1(X).$$

We denote by $\mathrm{Frob}_{E,x}$ the image of Frob_E through this morphism.

Given a finite extension E of k , we may define a **trace function** $\text{tr}_{\mathcal{L}} : X(E) \rightarrow \overline{\mathbb{Q}}_{\ell}$ in the following way: a point $x \in X(E)$ is a morphism $\text{Spec } E \rightarrow X$, and so induces a map

$$\text{Gal}(E) \rightarrow \pi_1(X).$$

We denote by $\text{Frob}_{E,x}$ the image of Frob_E through this morphism. It follows that $\rho(\text{Frob}_{E,x})$ is a conjugation class in $\text{GL}_r(\overline{\mathbb{Q}}_{\ell})$, and we may take its trace.

Trace functions

Given a finite extension E of k , we may define a **trace function** $\mathrm{tr}_{\mathcal{L}} : X(E) \rightarrow \overline{\mathbb{Q}}_{\ell}$ in the following way: a point $x \in X(E)$ is a morphism $\mathrm{Spec} E \rightarrow X$, and so induces a map

$$\mathrm{Gal}(E) \rightarrow \pi_1(X).$$

We denote by $\mathrm{Frob}_{E,x}$ the image of Frob_E through this morphism. It follows that $\rho(\mathrm{Frob}_{E,x})$ is a conjugation class in $\mathrm{GL}_r(\overline{\mathbb{Q}}_{\ell})$, and we may take its trace.

This number is the image of x by $\mathrm{tr}_{\mathcal{L}}$.

The Lang isogeny

Let G be a (nice) commutative group scheme over k . We consider the **absolute Frobenius** $F_G : G \rightarrow G$.

The Lang isogeny

Let G be a (nice) commutative group scheme over k . We consider the absolute Frobenius $F_G : G \rightarrow G$. The Lang isogeny

$$\mathrm{id}_G - F_G : G \rightarrow G$$

is a finite étale cover, which is also Galois with group $G(k)$.

Since $\pi_1(G)$ is the limit of the Galois groups of all finite étale Galois covers, we obtain a natural surjection $\pi_1(G) \rightarrow G(k)$.

Since $\pi_1(G)$ is the limit of the Galois groups of all finite étale Galois covers, we obtain a natural surjection $\pi_1(G) \rightarrow G(k)$. Now, if $\chi : G(k) \rightarrow \overline{\mathbb{Q}}_\ell^\times$ is a character, we may compose those morphisms to obtain a representation

$$\pi_1(G) \rightarrow G(k) \rightarrow \overline{\mathbb{Q}}_\ell^\times,$$

corresponding to a rank one local system over G ; denoted \mathcal{L}_χ .

More generally, given a morphism $f : X \rightarrow G$ of k -schemes, we compose the morphism above with f_* to obtain a rank one local system $f^* \mathcal{L}_\chi$, commonly denoted $\mathcal{L}_{\chi(f)}$.

More generally, given a morphism $f : X \rightarrow G$ of k -schemes, we compose the morphism above with f_* to obtain a rank one local system $f^* \mathcal{L}_\chi$, commonly denoted $\mathcal{L}_{\chi(f)}$.

Its trace at a point $x \in X(E)$ is given by $\chi(\mathrm{tr}_{E/k}^G f(x))$, where $\mathrm{tr}_{E/k}^G : G(E) \rightarrow G(k)$ sends $g \in G(E)$ to $g + \mathrm{Frob}_E(g) + \dots + \mathrm{Frob}_E^{n-1}(g)$ for $n = [E : k]$.

To go further into the world of étale cohomology, we need to expand our category of ℓ -adic local systems to the so-called **constructible sheaves**, which behave much better functorially.

To go further into the world of étale cohomology, we need to expand our category of ℓ -adic local systems to the so-called **constructible sheaves**, which behave much better functorially.

In topology, the constructible sheaves are those that restrict to local systems on a given stratification.

To go further into the world of étale cohomology, we need to expand our category of ℓ -adic local systems to the so-called **constructible sheaves**, which behave much better functorially.

In topology, the constructible sheaves are those that restrict to local systems on a given stratification. Up to some minor technical details, the same definition works in the ℓ -adic setting.

The six-functors on étale cohomology

We can define the **derived category** $D_c^b(X, \overline{\mathbb{Q}}_\ell)$ of constructible sheaves.

The six-functors on étale cohomology

We can define the **derived category** $D_c^b(X, \overline{\mathbb{Q}}_\ell)$ of constructible sheaves. These categories possess a rich functoriality!

- We have tensor products \otimes and inner homs RHom.

The six-functors on étale cohomology

We can define the **derived category** $D_c^b(X, \overline{\mathbb{Q}}_\ell)$ of constructible sheaves. These categories possess a rich functoriality!

- We have tensor products \otimes and inner homs RHom.

The six-functors on étale cohomology

We can define the **derived category** $D_c^b(X, \overline{\mathbb{Q}}_\ell)$ of constructible sheaves. These categories possess a rich functoriality!

- We have tensor products \otimes and inner homs RHom.

For a morphism $f : X \rightarrow Y$,

- we have a direct image and a compactly supported direct image functor $Rf_*, Rf_! : D_c^b(X, \overline{\mathbb{Q}}_\ell) \rightarrow D_c^b(Y, \overline{\mathbb{Q}}_\ell)$;

The six-functors on étale cohomology

We can define the **derived category** $D_c^b(X, \overline{\mathbb{Q}}_\ell)$ of constructible sheaves. These categories possess a rich functoriality!

- We have tensor products \otimes and inner homs RHom.

For a morphism $f : X \rightarrow Y$,

- we have a direct image and a compactly supported direct image functor $Rf_*, Rf_! : D_c^b(X, \overline{\mathbb{Q}}_\ell) \rightarrow D_c^b(Y, \overline{\mathbb{Q}}_\ell)$;
- we have an inverse image and an exceptional inverse image functor $f^*, f^! : D_c^b(Y, \overline{\mathbb{Q}}_\ell) \rightarrow D_c^b(X, \overline{\mathbb{Q}}_\ell)$.

The six-functors on étale cohomology

We can define the **derived category** $D_c^b(X, \overline{\mathbb{Q}}_\ell)$ of constructible sheaves. These categories possess a rich functoriality!

- We have tensor products \otimes and inner homs RHom.

For a morphism $f : X \rightarrow Y$,

- we have a direct image and a compactly supported direct image functor $Rf_*, Rf_! : D_c^b(X, \overline{\mathbb{Q}}_\ell) \rightarrow D_c^b(Y, \overline{\mathbb{Q}}_\ell)$;
- we have an inverse image and an exceptional inverse image functor $f^*, f^! : D_c^b(Y, \overline{\mathbb{Q}}_\ell) \rightarrow D_c^b(X, \overline{\mathbb{Q}}_\ell)$.

The six-functors on étale cohomology

We can define the **derived category** $D_c^b(X, \overline{\mathbb{Q}}_\ell)$ of constructible sheaves. These categories possess a rich functoriality!

- We have tensor products \otimes and inner homs RHom.

For a morphism $f : X \rightarrow Y$,

- we have a direct image and a compactly supported direct image functor $Rf_*, Rf_! : D_c^b(X, \overline{\mathbb{Q}}_\ell) \rightarrow D_c^b(Y, \overline{\mathbb{Q}}_\ell)$;
- we have an inverse image and an exceptional inverse image functor $f^*, f^! : D_c^b(Y, \overline{\mathbb{Q}}_\ell) \rightarrow D_c^b(X, \overline{\mathbb{Q}}_\ell)$.

These functors satisfy a large number of compatibility relations which are encapsulated in the designation **six-functor formalism**.

The trace formula

Since constructible sheaves “locally” are local systems, we may extend trace functions to objects of $D_c^b(X, \overline{\mathbb{Q}}_\ell)$.

The trace formula

Since constructible sheaves “locally” are local systems, we may extend trace functions to objects of $D_c^b(X, \overline{\mathbb{Q}}_\ell)$. It satisfies the so-called **trace formula**

$$\mathrm{tr}_{Rf_!M}(t) = \sum_{f(x)=t} \mathrm{tr}_M(x).$$

The trace formula

Since constructible sheaves “locally” are local systems, we may extend trace functions to objects of $D_c^b(X, \overline{\mathbb{Q}}_\ell)$. It satisfies the so-called **trace formula**

$$\mathrm{tr}_{Rf_!M}(t) = \sum_{f(x)=t} \mathrm{tr}_M(x).$$

In particular, our exponential sums may be written as

$$\begin{aligned} S(f, E, \chi) &= \sum_{x \in X(E)} \chi(f(x)) = \sum_{t \in G(E)} \chi(t) \#\{x \in X(E) \mid f(x) = t\} \\ &= \sum_{t \in G(E)} \chi(t) \mathrm{tr}_{Rf_! \overline{\mathbb{Q}}_\ell}(t). \end{aligned}$$

The trace formula

Since constructible sheaves “locally” are local systems, we may extend trace functions to objects of $D_c^b(X, \overline{\mathbb{Q}}_\ell)$. It satisfies the so-called **trace formula**

$$\mathrm{tr}_{Rf_!M}(t) = \sum_{f(x)=t} \mathrm{tr}_M(x).$$

In particular, our exponential sums may be written as

$$\begin{aligned} S(f, E, \chi) &= \sum_{x \in X(E)} \chi(f(x)) = \sum_{t \in G(E)} \chi(t) \#\{x \in X(E) \mid f(x) = t\} \\ &= \sum_{t \in G(E)} \chi(t) \mathrm{tr}_{Rf_! \overline{\mathbb{Q}}_\ell}(t). \end{aligned}$$

Believe it or not, **this is a tremendous simplification!**

Deligne's equidistribution theorem

Our sums $S(f, E, \chi)$ are Fourier transforms of traces of Frobenius acting on complexes of ℓ -adic sheaves.

Fourier-Deligne transform

Our sums $S(f, E, \chi)$ are Fourier transforms of traces of Frobenius acting on complexes of ℓ -adic sheaves. Is it possible to do this Fourier transform in a *sheaf-theoretic* way?

Fourier-Deligne transform

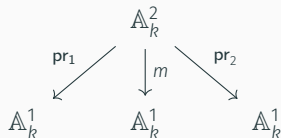
Our sums $S(f, E, \chi)$ are Fourier transforms of traces of Frobenius acting on complexes of ℓ -adic sheaves. Is it possible to do this Fourier transform in a *sheaf-theoretic* way? **At least when $G = \mathbb{G}_a$, yes!**

Fourier-Deligne transform

Our sums $S(f, E, \chi)$ are Fourier transforms of traces of Frobenius acting on complexes of ℓ -adic sheaves. Is it possible to do this Fourier transform in a *sheaf-theoretic* way? **At least when $G = \mathbb{G}_a$, yes!**

Consider the diagram on the right, where $m : (x, y) \mapsto xy$ is the multiplication map. The **Fourier-Deligne** transform is the functor

$$\begin{aligned} \mathrm{FT}_\chi : D_c^b(\mathbb{A}_k^1, \overline{\mathbb{Q}}_\ell) &\rightarrow D_c^b(\mathbb{A}_k^1, \overline{\mathbb{Q}}_\ell) \\ M &\mapsto R\mathrm{pr}_{2,!}(\mathrm{pr}_1^* M \otimes \mathcal{L}_{\chi(m)}). \end{aligned}$$



Recall that, if we fix a character $\tilde{\chi}$ of $k = \mathbb{A}^1(k)$, all $\chi \in \hat{E}$ are of the form $t \mapsto \tilde{\chi}(\text{tr}_{E/k}(tx))$ for a unique $x \in E$.

Recall that, if we fix a character $\tilde{\chi}$ of $k = \mathbb{A}^1(k)$, all $\chi \in \hat{E}$ are of the form $t \mapsto \tilde{\chi}(\mathrm{tr}_{E/k}(tx))$ for a unique $x \in E$. This, along with the trace formula, implies that

$$\{S(f, E, \chi)\}_{\chi \in \hat{E}} = \left\{ \mathrm{tr}_{\mathrm{FT}_{\tilde{\chi}}(\mathrm{Rf}_! \overline{\mathbb{Q}}_\ell)}(x) \right\}_{x \in E}.$$

ES as a *single* trace function

Recall that, if we fix a character $\tilde{\chi}$ of $k = \mathbb{A}^1(k)$, all $\chi \in \hat{E}$ are of the form $t \mapsto \tilde{\chi}(\mathrm{tr}_{E/k}(tx))$ for a unique $x \in E$. This, along with the trace formula, implies that

$$\{S(f, E, \chi)\}_{\chi \in \hat{E}} = \left\{ \mathrm{tr}_{\mathrm{FT}_{\tilde{\chi}}(\mathrm{Rf}_! \overline{\mathbb{Q}}_\ell)}(x) \right\}_{x \in E}.$$

In particular, we may focus our study in the distribution of a **single** trace function.

Now, let's understand the complex $M := \mathrm{FT}_{\tilde{\chi}}(\mathrm{R}f_! \overline{\mathbb{Q}}_\ell)$.

Now, let's understand the complex $M := \mathrm{FT}_{\tilde{\chi}}(\mathrm{Rf}_! \overline{\mathbb{Q}}_\ell)$. A priori, we have a tough problem:

- neither $\mathrm{Rf}_!$ nor $\mathrm{FT}_{\tilde{\chi}}$ preserve constructible sheaves (in degree 0).

Now, let's understand the complex $M := \mathrm{FT}_{\tilde{\chi}}(\mathrm{R}f_1 \overline{\mathbb{Q}}_\ell)$. A priori, we have a tough problem:

- neither $\mathrm{R}f_1$ nor $\mathrm{FT}_{\tilde{\chi}}$ preserve constructible sheaves (in degree 0).

Now, let's understand the complex $M := \mathrm{FT}_{\tilde{\chi}}(\mathrm{R}f_! \overline{\mathbb{Q}}_\ell)$. A priori, we have a tough problem:

- neither $\mathrm{R}f_!$ nor $\mathrm{FT}_{\tilde{\chi}}$ preserve constructible sheaves (in degree 0).

Luckily, there is another abelian subcategory of $D_c^b(\mathbb{A}_k^1, \overline{\mathbb{Q}}_\ell)$ which works much better; the category of **perverse sheaves**!

Let us recall a couple of facts about perverse sheaves:

Let us recall a couple of facts about perverse sheaves:

- If \mathcal{L} is a local system, \mathcal{L} is also a perverse sheaf;

Let us recall a couple of facts about perverse sheaves:

- If \mathcal{L} is a local system, \mathcal{L} is also a perverse sheaf;
- (Artin vanishing) If f is affine and quasi-finite, $Rf_!$ preserves perversity;

Let us recall a couple of facts about perverse sheaves:

- If \mathcal{L} is a local system, \mathcal{L} is also a perverse sheaf;
- (Artin vanishing) If f is affine and quasi-finite, $Rf_!$ preserves perversity;
- The Fourier-Deligne transform preserves perversity.

Let us recall a couple of facts about perverse sheaves:

- If \mathcal{L} is a local system, \mathcal{L} is also a perverse sheaf;
- (Artin vanishing) If f is affine and quasi-finite, $Rf_!$ preserves perversity;
- The Fourier-Deligne transform preserves perversity.

Let us recall a couple of facts about perverse sheaves:

- If \mathcal{L} is a local system, \mathcal{L} is also a perverse sheaf;
- (Artin vanishing) If f is affine and quasi-finite, $Rf_!$ preserves perversity;
- The Fourier-Deligne transform preserves perversity.

In particular, for finite f , $M = \mathbf{FT}_{\tilde{\chi}}(Rf_! \overline{\mathbb{Q}}_\ell)$ is a perverse sheaf.

Let us recall a couple of facts about perverse sheaves:

- If \mathcal{L} is a local system, \mathcal{L} is also a perverse sheaf;
- (Artin vanishing) If f is affine and quasi-finite, $Rf_!$ preserves perversity;
- The Fourier-Deligne transform preserves perversity.

In particular, for finite f , $M = \mathbf{FT}_{\tilde{\chi}}(Rf_! \overline{\mathbb{Q}}_\ell)$ is a perverse sheaf.

Moreover, there's an open subscheme $U \hookrightarrow \mathbb{A}_k^1$ such that $M|_U$ is a local system \mathcal{L} .

The previous discussion allows us to focus on the traces of a rank r local system \mathcal{L} , which is given by a representation ρ .

Monodromy groups

The previous discussion allows us to focus on the traces of a rank r local system \mathcal{L} , which is given by a representation ρ . By a result of Grothendieck, the natural map $\pi_1(X_{\bar{k}}) \rightarrow \pi_1(X)$ is injective, and therefore we may associate two algebraic groups to \mathcal{L} :

- the arithmetic monodromy group $G_{\text{arith}, \mathcal{L}}$, which is the Zariski closure of $\rho(\pi_1(X))$ inside $\text{GL}_r(\overline{\mathbb{Q}}_\ell)$;

Monodromy groups

The previous discussion allows us to focus on the traces of a rank r local system \mathcal{L} , which is given by a representation ρ . By a result of Grothendieck, the natural map $\pi_1(X_{\bar{k}}) \rightarrow \pi_1(X)$ is injective, and therefore we may associate two algebraic groups to \mathcal{L} :

- the arithmetic monodromy group $G_{\text{arith}, \mathcal{L}}$, which is the Zariski closure of $\rho(\pi_1(X))$ inside $\text{GL}_r(\overline{\mathbb{Q}}_\ell)$;
- the geometric monodromy group $G_{\text{geom}, \mathcal{L}}$, which is the Zariski closure of $\rho(\pi_1(X_{\bar{k}}))$ inside $\text{GL}_r(\overline{\mathbb{Q}}_\ell)$.

Monodromy groups

The previous discussion allows us to focus on the traces of a rank r local system \mathcal{L} , which is given by a representation ρ . By a result of Grothendieck, the natural map $\pi_1(X_{\bar{k}}) \rightarrow \pi_1(X)$ is injective, and therefore we may associate two algebraic groups to \mathcal{L} :

- the arithmetic monodromy group $G_{\text{arith}, \mathcal{L}}$, which is the Zariski closure of $\rho(\pi_1(X))$ inside $\text{GL}_r(\overline{\mathbb{Q}}_\ell)$;
- the geometric monodromy group $G_{\text{geom}, \mathcal{L}}$, which is the Zariski closure of $\rho(\pi_1(X_{\bar{k}}))$ inside $\text{GL}_r(\overline{\mathbb{Q}}_\ell)$.

Monodromy groups

The previous discussion allows us to focus on the traces of a rank r local system \mathcal{L} , which is given by a representation ρ . By a result of Grothendieck, the natural map $\pi_1(X_{\bar{k}}) \rightarrow \pi_1(X)$ is injective, and therefore we may associate two algebraic groups to \mathcal{L} :

- the arithmetic monodromy group $G_{\text{arith}, \mathcal{L}}$, which is the Zariski closure of $\rho(\pi_1(X))$ inside $\text{GL}_r(\overline{\mathbb{Q}}_\ell)$;
- the geometric monodromy group $G_{\text{geom}, \mathcal{L}}$, which is the Zariski closure of $\rho(\pi_1(X_{\bar{k}}))$ inside $\text{GL}_r(\overline{\mathbb{Q}}_\ell)$.

Clearly $G_{\text{geom}, \mathcal{L}}$ is a subgroup of $G_{\text{arith}, \mathcal{L}}$. Moreover, Deligne proved that, in our case, $G_{\text{geom}, \mathcal{L}}$ is reductive.

Deligne's equidistribution theorem

Fix an embedding $\overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$, and let K be a maximal compact subgroup of $G_{\text{geom}, \mathcal{L}}(\mathbb{C})$.

Deligne's equidistribution theorem

Fix an embedding $\overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$, and let K be a maximal compact subgroup of $G_{\text{geom}, \mathcal{L}}(\mathbb{C})$.

Theorem (Deligne)

Suppose that $G_{\text{geom}, \mathcal{L}} = G_{\text{arith}, \mathcal{L}}$. Then the sums

$$\left\{ \frac{(-1)^d}{|E|^{d/2}} \sum_{x \in X(E)} \tilde{\chi}(\text{tr}_{E/k}(tf(x))) \right\}_{t \in U(E)}$$

are distributed as traces of random matrices in K as the degree of E/k tends to infinity.

Deligne's equidistribution theorem

Fix an embedding $\overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$, and let K be a maximal compact subgroup of $G_{\text{geom}, \mathcal{L}}(\mathbb{C})$.

Theorem (Deligne)

Suppose that $G_{\text{geom}, \mathcal{L}} = G_{\text{arith}, \mathcal{L}}$. Then the sums

$$\left\{ \frac{(-1)^d}{|E|^{d/2}} \sum_{x \in X(E)} \tilde{\chi}(\text{tr}_{E/k}(tf(x))) \right\}_{t \in U(E)}$$

are distributed as traces of random matrices in K as the degree of E/k tends to infinity.

More generally, we have equidistribution results for sums of the form

$$\sum_{x \in E} \tilde{\chi}(\text{tr}_{E/k}(tx)) \text{tr}_M(x),$$

where M is a “nice” (= pure of weight 0) perverse sheaf.

The general equidistribution result

Why generalizing Deligne's result is hard

One crucial point in the discussion leading to Deligne's theorem is that, when $G = \mathbb{G}_a$, there's an algebraic variety (\mathbb{A}^1 itself) over k whose E -points parameterize the characters of $G(E)$.

Why generalizing Deligne's result is hard

One crucial point in the discussion leading to Deligne's theorem is that, when $G = \mathbb{G}_a$, there's an algebraic variety (\mathbb{A}^1 itself) over k whose E -points parameterize the characters of $G(E)$. This fails already for $G = \mathbb{G}_m$.

Why generalizing Deligne's result is hard

One crucial point in the discussion leading to Deligne's theorem is that, when $G = \mathbb{G}_a$, there's an algebraic variety (\mathbb{A}^1 itself) over k whose E -points parameterize the characters of $G(E)$. This fails already for $G = \mathbb{G}_m$.

N. Katz had a brilliant idea: instead of considering a Fourier transform, we should consider a convolution of sheaves.

Why generalizing Deligne's result is hard

One crucial point in the discussion leading to Deligne's theorem is that, when $G = \mathbb{G}_a$, there's an algebraic variety (\mathbb{A}^1 itself) over k whose E -points parameterize the characters of $G(E)$. This fails already for $G = \mathbb{G}_m$.

N. Katz had a brilliant idea: instead of considering a Fourier transform, we should consider a convolution of sheaves. If $m : G \times G \rightarrow G$ is the multiplication map, and M, N are objects of $D_c^b(G, \overline{\mathbb{Q}}_\ell)$, the complex $M *_1 N := Rm_{!}(\text{pr}_1^* M \otimes \text{pr}_2^* N)$ satisfies

$$\text{tr}_{M *_1 N}(x) = (\text{tr}_M * \text{tr}_N)(x) = \sum_{t \in G(E)} \text{tr}_M(t) \text{tr}_N(xt^{-1}).$$

Tannakian categories

The so-called formalism of *Tannakian categories* gives conditions on an abelian symmetric monoidal category that forces it to be equivalent to $\text{Rep}(H)$, for some group scheme H .

Tannakian categories

The so-called formalism of *Tannakian categories* gives conditions on an abelian symmetric monoidal category that forces it to be equivalent to $\text{Rep}(H)$, for some group scheme H .

We want to use it to construct our “monodromy groups” that govern the distribution of exponential sums.

Tannakian categories

The so-called formalism of *Tannakian categories* gives conditions on an abelian symmetric monoidal category that forces it to be equivalent to $\text{Rep}(H)$, for some group scheme H .

We want to use it to construct our “monodromy groups” that govern the distribution of exponential sums. However, we don’t have a good candidate category...

- Convolution defines a symmetric monoidal operation on $D_c^b(G, \overline{\mathbb{Q}}_\ell)$, but this category is not abelian;

Tannakian categories

The so-called formalism of *Tannakian categories* gives conditions on an abelian symmetric monoidal category that forces it to be equivalent to $\text{Rep}(H)$, for some group scheme H .

We want to use it to construct our “monodromy groups” that govern the distribution of exponential sums. However, we don’t have a good candidate category...

- Convolution defines a symmetric monoidal operation on $D_c^b(G, \overline{\mathbb{Q}}_\ell)$, but this category is not abelian;
- $\text{Perv}(G, \overline{\mathbb{Q}}_\ell)$ is abelian, but perverse sheaves are not preserved by convolution.

Negligible objects

Gabber and Loeser had the idea to quotient $\text{Perv}(G, \overline{\mathbb{Q}}_\ell)$ by a Serre subcategory composed of *negligible objects*.

Negligible objects

Gabber and Loeser had the idea to quotient $\text{Perv}(G, \overline{\mathbb{Q}}_\ell)$ by a Serre subcategory composed of *negligible objects*. Our convolution functor should descend to the quotient, making

$$\text{Perv}(G, \overline{\mathbb{Q}}_\ell)/\text{Neg}$$

a tannakian category.

Negligible objects

Gabber and Loeser had the idea to quotient $\text{Perv}(G, \overline{\mathbb{Q}}_\ell)$ by a Serre subcategory composed of *negligible objects*. Our convolution functor should descend to the quotient, making

$$\text{Perv}(G, \overline{\mathbb{Q}}_\ell)/\text{Neg}$$

a tannakian category.

When $G = \mathbb{G}_m$, the negligible objects are precisely those with zero Euler characteristic.

Negligible objects

Gabber and Loeser had the idea to quotient $\text{Perv}(G, \overline{\mathbb{Q}}_\ell)$ by a Serre subcategory composed of *negligible objects*. Our convolution functor should descend to the quotient, making

$$\text{Perv}(G, \overline{\mathbb{Q}}_\ell)/\text{Neg}$$

a tannakian category.

When $G = \mathbb{G}_m$, the negligible objects are precisely those with zero Euler characteristic. This allowed Katz to prove an equidistribution theorem similar to the previous one.

Generic vanishing of cohomology

For higher-dimensional groups, the proof that a reasonable choice of negligible objects indeed yields a Tannakian category rests on a difficult cohomology vanishing theorem.

Generic vanishing of cohomology

For higher-dimensional groups, the proof that a reasonable choice of negligible objects indeed yields a Tannakian category rests on a difficult cohomology vanishing theorem.

Such a result was not known before the very recent preprint *Arithmetic Fourier Transforms over Finite Fields* by A. Forey, J. Fresán, and E. Kowalski, which uses as a fundamental tool the *Quantitative Sheaf Theory* of W. Sawin.

The general equidistribution theorem

Let M be a *semiperverse* sheaf on G , *mixed of weights* ≤ 0 . The Tannakian formalism gives a “arithmetic monodromy group” G_{arith} .

The general equidistribution theorem

Let M be a *semiperverse* sheaf on G , *mixed of weights* ≤ 0 . The Tannakian formalism gives a “arithmetic monodromy group” G_{arith} . We denote by ν the direct image of the normalized Haar measure μ on a maximal compact subgroup of $G_{\text{arith}}(\mathbb{C})$ by the trace function.

The general equidistribution theorem

Let M be a *semiperverse* sheaf on G , *mixed of weights* ≤ 0 . The Tannakian formalism gives a “arithmetic monodromy group” G_{arith} . We denote by ν the direct image of the normalized Haar measure μ on a maximal compact subgroup of $G_{\text{arith}}(\mathbb{C})$ by the trace function.

Theorem (Forey, Fresán, Kowalski)

The exponential sums $S(M, E, \chi) := \sum_{x \in G(E)} \chi(x) \text{tr}_M(x)$, for $\chi \in \widehat{G(E)}$, become ν -equidistributed *on average* as the degree of E/k tends to infinity.

The general equidistribution theorem

Let M be a *semiperverse* sheaf on G , *mixed of weights* ≤ 0 . The Tannakian formalism gives a “arithmetic monodromy group” G_{arith} . We denote by ν the direct image of the normalized Haar measure μ on a maximal compact subgroup of $G_{\text{arith}}(\mathbb{C})$ by the trace function.

Theorem (Forey, Fresán, Kowalski)

The exponential sums $S(M, E, \chi) := \sum_{x \in G(E)} \chi(x) \text{tr}_M(x)$, for $\chi \in \widehat{G(E)}$, become ν -equidistributed *on average* as the degree of E/k tends to infinity. In other words,

$$\int_K f(\text{tr}(x)) d\mu(x) = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{[E:k] \leq n} \frac{1}{|G(E)|} \sum_{\chi \in \widehat{G(E)}} f(S(M, E, \chi)).$$

for every bounded continuous function $f : \mathbb{C} \rightarrow \mathbb{C}$.

Let's work out the case of Gauss' sums

The Gauss sum $g(\psi, \chi)$ is defined as

$$g(\psi, \chi) := \sum_{x \in \mathbb{F}_q^\times} \psi(x)\chi(x),$$

where ψ is an additive and χ is a multiplicative character of \mathbb{F}_q .

The Gauss sum $g(\psi, \chi)$ is defined as

$$g(\psi, \chi) := \sum_{x \in \mathbb{F}_q^\times} \psi(x)\chi(x),$$

where ψ is an additive and χ is a multiplicative character of \mathbb{F}_q .

Fix a nontrivial additive character ψ of \mathbb{F}_p and denote by ψ_q the character of \mathbb{F}_q obtained by composing with the trace.

If χ is trivial, $g(\psi_q, \chi)$ is simply -1 .

If χ is trivial, $g(\psi_q, \chi)$ is simply -1 . Else, its absolute value is \sqrt{q} and we find $q - 2$ points

$$\theta_{q,\chi} := \frac{g(\psi_q, \chi)}{\sqrt{q}} \in S^1,$$

one for each nontrivial multiplicative character.

How do these angles are distributed?

As in Sato-Tate's conjecture, we may wonder how do these “angles” are distributed on the unit circle as q tends *vertically* to infinity.

How do these angles are distributed?

As in Sato-Tate's conjecture, we may wonder how do these “angles” are distributed on the unit circle as q tends *vertically* to infinity.

Theorem (Deligne)

As q tends to infinity, the angles $\{\theta_{q,\chi}\}_{\chi \neq 1}$ become equidistributed on S^1 with respect to its normalized Haar measure.

How do these angles are distributed?

As in Sato-Tate's conjecture, we may wonder how do these “angles” are distributed on the unit circle as q tends *vertically* to infinity.

Theorem (Deligne)

As q tends to infinity, the angles $\{\theta_{q,x}\}_{x \neq 1}$ become equidistributed on S^1 with respect to its normalized Haar measure. In other words, the equation

$$\frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta}) d\theta = \lim_{q \rightarrow \infty} \frac{1}{q-2} \sum_{x \neq 1} f(\theta_{q,x})$$

is satisfied for all continuous functions $f : S^1 \rightarrow \mathbb{C}$.

Using our formalism

Our goal is to calculate

$$\lim_{q \rightarrow \infty} \frac{1}{q-2} \sum_{\chi \neq 1} f(\theta_{q,\chi}).$$

We begin by generalizing the statement to all *bounded* continuous functions $f : \mathbb{C} \rightarrow \mathbb{C}$.

Using our formalism

Our goal is to calculate

$$\lim_{q \rightarrow \infty} \frac{1}{q-2} \sum_{\chi \neq 1} f(\theta_{q,\chi}).$$

We begin by generalizing the statement to all *bounded* continuous functions $f : \mathbb{C} \rightarrow \mathbb{C}$. Since the trivial character amounts to nothing in the limit, we may also consider all characters.

Using our formalism

Our goal is to calculate

$$\lim_{q \rightarrow \infty} \frac{1}{q-2} \sum_{\chi \neq 1} f(\theta_{q,\chi}).$$

We begin by generalizing the statement to all *bounded* continuous functions $f : \mathbb{C} \rightarrow \mathbb{C}$. Since the trivial character amounts to nothing in the limit, we may also consider all characters.

If $j : \mathbb{G}_m \hookrightarrow \mathbb{A}^1$ is the natural inclusion, our perverse sheaf is $M = \mathcal{L}_{\psi(j)}(1/2)[1]$.

Using our formalism

Our goal is to calculate

$$\lim_{q \rightarrow \infty} \frac{1}{q-2} \sum_{\chi \neq 1} f(\theta_{q,\chi}).$$

We begin by generalizing the statement to all *bounded* continuous functions $f : \mathbb{C} \rightarrow \mathbb{C}$. Since the trivial character amounts to nothing in the limit, we may also consider all characters.

If $j : \mathbb{G}_m \hookrightarrow \mathbb{A}^1$ is the natural inclusion, our perverse sheaf is $M = \mathcal{L}_{\psi(j)}(1/2)[1]$. Its Tannakian dimension is 1, and so $G_{\text{geom}} \subseteq G_{\text{arith}} \subseteq \text{GL}_1$.

Using our formalism

Our goal is to calculate

$$\lim_{q \rightarrow \infty} \frac{1}{q-2} \sum_{\chi \neq 1} f(\theta_{q,\chi}).$$

We begin by generalizing the statement to all *bounded* continuous functions $f : \mathbb{C} \rightarrow \mathbb{C}$. Since the trivial character amounts to nothing in the limit, we may also consider all characters.

If $j : \mathbb{G}_m \hookrightarrow \mathbb{A}^1$ is the natural inclusion, our perverse sheaf is $M = \mathcal{L}_{\psi(j)}(1/2)[1]$. Its Tannakian dimension is 1, and so $G_{\text{geom}} \subseteq G_{\text{arith}} \subseteq \mathbf{GL}_1$. But no convolution power of $M_{\bar{k}}$ is the identity, and so $G_{\text{geom}} = G_{\text{arith}} = \mathbf{GL}_1$.

Using our formalism

Our goal is to calculate

$$\lim_{q \rightarrow \infty} \frac{1}{q-2} \sum_{\chi \neq 1} f(\theta_{q,\chi}).$$

We begin by generalizing the statement to all *bounded* continuous functions $f : \mathbb{C} \rightarrow \mathbb{C}$. Since the trivial character amounts to nothing in the limit, we may also consider all characters.

If $j : \mathbb{G}_m \hookrightarrow \mathbb{A}^1$ is the natural inclusion, our perverse sheaf is $M = \mathcal{L}_{\psi(j)}(1/2)[1]$. Its Tannakian dimension is 1, and so $G_{\text{geom}} \subseteq G_{\text{arith}} \subseteq \mathbf{GL}_1$. But no convolution power of $M_{\bar{k}}$ is the identity, and so $G_{\text{geom}} = G_{\text{arith}} = \mathbf{GL}_1$. The maximal compact subgroup is $K = S^1$ and the result follows.

Using our formalism

Our goal is to calculate

$$\lim_{q \rightarrow \infty} \frac{1}{q-2} \sum_{\chi \neq 1} f(\theta_{q,\chi}).$$

We begin by generalizing the statement to all *bounded* continuous functions $f : \mathbb{C} \rightarrow \mathbb{C}$. Since the trivial character amounts to nothing in the limit, we may also consider all characters.

If $j : \mathbb{G}_m \hookrightarrow \mathbb{A}^1$ is the natural inclusion, our perverse sheaf is $M = \mathcal{L}_{\psi(j)}(1/2)[1]$. Its Tannakian dimension is 1, and so $G_{\text{geom}} \subseteq G_{\text{arith}} \subseteq \mathbf{GL}_1$. But no convolution power of $M_{\bar{k}}$ is the identity, and so $G_{\text{geom}} = G_{\text{arith}} = \mathbf{GL}_1$. The maximal compact subgroup is $K = S^1$ and the result follows.

Thank you!