

Exponential sums over  
finite fields

8<sup>th</sup> ECM

E. Kowalski

(ETH  
Zürich)

23.6.2021

[Joint w. A. Forey and J. Fresán]

<https://www.math.ethz.ch/~kowalski/convolution-ecm-draft.pdf>

$$\sum_{x \in \mathbb{F}_q} \alpha(x)$$

$$\in \mathbb{C}$$

complex numbers  
of modulus  
1, "of  
algebraic  
nature"

finite field  
with  $q$  elements

$$(\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z})$$

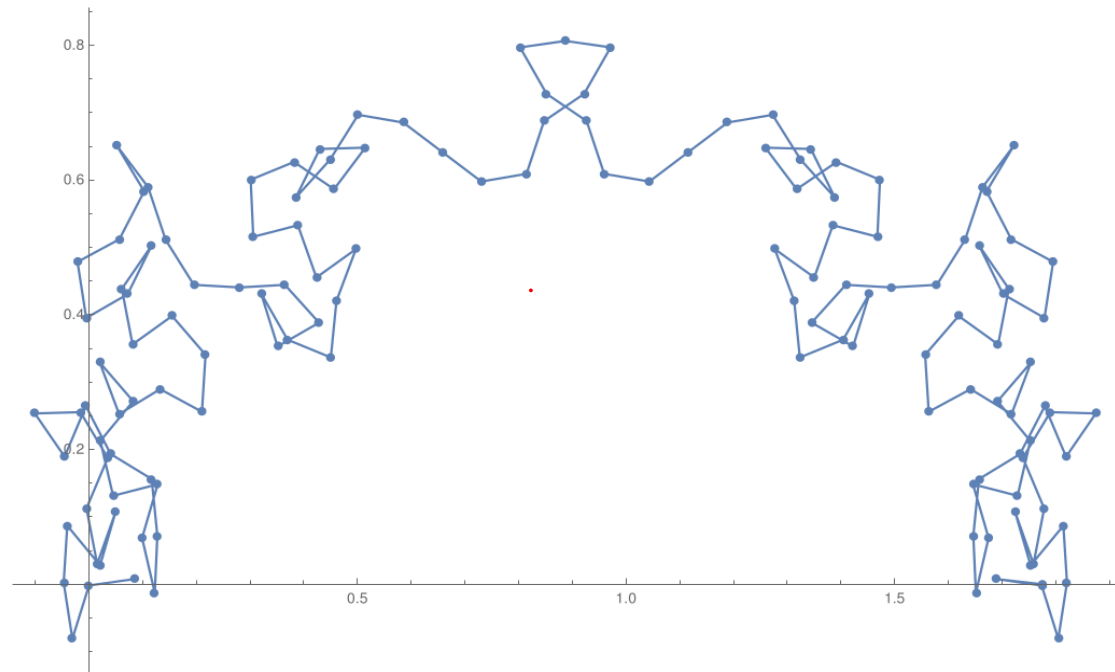
Ex.

$$2i\pi f(x)/p$$

$$\alpha(x) = e$$

$$\text{for } f \in \mathbb{Z}[x]$$

$$(x \in \mathbb{Z}/p\mathbb{Z})$$



History: (1) Lagrange resolvents (cyclotomy)

(2) Gauss sums:

$$\tau(\chi, a) = \sum_{x \in \mathbb{F}_p^\times} \chi(x) e\left(\frac{ax}{p}\right)$$

additive character

multiplicative character

(Gauss

$$\cong \mathbb{Z}/(p-1)\mathbb{Z})$$

$$\left\{ \begin{array}{l} \chi : \mathbb{F}_p^\times \longrightarrow \mathbb{S}^1 \\ e(z) = e^{2i\pi z} \end{array} \right.$$

multiplicative

Analogy:

$$\Gamma(s) = \int_0^{+\infty} \underbrace{e^{-x}}_{\text{additive}} \underbrace{x^s}_{\text{multiplicative}} \frac{dx}{x}$$

Euler : 
$$\frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)} = \int_0^1 x^{a-1} (1-x)^{b-1} dx$$

Jacobi : 
$$\frac{\tau(\chi_1)\tau(\chi_2)}{\tau(\chi_1\chi_2)} = \sum_{\substack{x \in \mathbb{F}_p^\times \\ x \neq 1}} \chi_1(x)\chi_2(1-x)$$

$$[\tau(\chi) = \tau(\chi, 1)]$$

" 
$$J(\chi_1, \chi_2)$$

Further examples : hypergeometric functions  
and sums (Katz, ...)

# Th. (Fermat)

Let  $p$  be a prime  $\equiv 1 \pmod{4}$ .  
There exist  $a, b$  in  $\mathbb{Z}$  with  
$$p = a^2 + b^2.$$

## Proof. (Jacobi (?))

①  $\left. \begin{array}{l} \mathbb{F}_p^\times \text{ is cyclic} \\ 4 \mid p-1 \end{array} \right\} \Rightarrow \begin{array}{l} \exists \chi_2 : \mathbb{F}_p^\times \rightarrow \{\pm 1\} \\ \chi_4 : \mathbb{F}_p^\times \rightarrow \{\pm 1, \pm i\} \end{array}$

$\Rightarrow \exists \mathcal{J}(\chi_2, \chi_4) = a + ib$

②  $|\tau(\chi)|^2 = p \Rightarrow a^2 + b^2 = |\mathcal{J}(\chi_2, \chi_4)|^2 = p$

□

# Kloosterman sums

$$x\bar{x} \equiv 1 \pmod{p}$$

$$Kl(a, b; p) = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p^*} e\left(\frac{ax + b\bar{x}}{p}\right)$$

$a, b \in \mathbb{F}_p^*$

Occurs in

\* Fourier expansion of Poincaré series  
(Poincaré 1912)  $\rightarrow$  modular forms

\* Solutions of  $a_1 x_1^2 + \dots + a_4 x_4^2 = N$

(Kloosterman 1924)

$\rightarrow$  circle method (6)

# Distribution of values

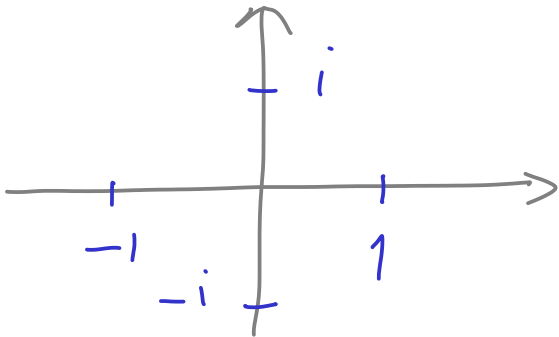
$p$  odd prime ;  $\chi_2 : \mathbb{F}_p^\times \longrightarrow \{\pm 1\}$

Easy:

( $\chi_2(x) = 1 \iff x$  is a square in  $\mathbb{F}_p^\times$ )

$$\tau(\chi_2) = \varepsilon_p \sqrt{p},$$

$$\varepsilon_p = \begin{cases} \pm 1 & \text{if } p \equiv 1 \pmod{4} \\ \pm i & \text{if } p \equiv 3 \pmod{4} \end{cases}$$



Th. (Gauss) - The sign is always  $\oplus$   
 $\tau(\chi_2) = \sqrt{p}$  or  $i\sqrt{p}$ .

Most other exponential sums cannot be computed so easily!

But: (1) they satisfy strong structural properties (Weil, Grothendieck, Deligne...)

(2) "families" of exponential sums have regular statistical behavior.

(Deligne, Katz,

Forey - Fresán - K.)

$\tau(x, a)$   
 $J(x_1, x_2)$   
 $\kappa(a, b; p)$

# Structural properties

Consider the examples

$$S(f; p) = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} e\left(\frac{f(x)}{p}\right), \quad f \in \mathbb{F}_p[x], \quad \deg(f) = d < p$$

[Weil] There are (algebraic) numbers  $\alpha_1, \dots, \alpha_{d-1}$  s.t.

$$\begin{cases} S(f, p) = -(\alpha_1 + \dots + \alpha_{d-1}) \\ |\alpha_i| = 1 \end{cases}$$

(Riemann Hypothesis for curves)

[Cor.  $|S(f, p)| \leq d-1$ ].

More generally: "every" exponential sum has similar properties

# Distribution properties

Deligne (1980): "Any family of exponential sums parameterized by an algebraic variety

[ex.  $Kl(a, b; p)$ , parameterized by  $(a, b)$ ] is

distributed statistically like the trace of a "random matrix in some compact group  $K \subset U_n(\mathbb{C})$ .

[Originally: consider parameters over extensions of the base field of degree  $\rightarrow +\infty$ ]  
[ $SL_2(p)$ ;  $n = d - 1$ ]

Key Tool: Riemann Hypothesis over finite fields

Ex:  $\text{Kl}(a, b; p) = \text{Tr } \Theta_p(a, b),$   
 with  $\Theta_p(a, b) \in \text{SU}_2(\mathbb{F})$   
 (Katz) distributed like  $\text{Tr}(\Theta), \Theta$   
 random in  $\text{SU}_2(\mathbb{F})$ .

Concretely: for any continuous function  
 $f: [-2, 2] \longrightarrow \mathbb{C}$

we have

$$\int_{-2}^2 f(t) \frac{1}{\pi} \sqrt{1 - \frac{t^2}{4}} dt = \lim_{p \rightarrow \infty} \frac{1}{(p-1)^2} \sum_{a, b \in \mathbb{F}_p^\times} f(\text{Kl}(a, b; p)).$$

Katz (2012) : "same" result  
of "universal equidistribution" for all  
families parameterized by multiplicative

characters  $\chi: \mathbb{F}_q^\times \rightarrow \mathbb{S}^1$ .

Ex.  $S(\chi) = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p^\times} \chi(x) e\left(\frac{f(x)}{p}\right)$

*fixed pol.*

Key Tools : (1) Deligne's work again  
(2) Tannakian categories

Forey - Fresán - K. <sup>(7, 2021)</sup> : extend "universal"  
equidistribution to any family parameter-  
-rized by characters

$$\chi : G(\mathbb{F}_q) \longrightarrow \mathbb{S}^1$$

for  $G$  connected commutative algebraic group.

Ex.  $S(\chi, a) = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} \chi(x) e\left(\frac{ax + \bar{x}}{p}\right)$

Ex. More variables:

$$S(\chi_1, \chi_2) = \frac{1}{p} \sum_{x, y} \chi_1(x) \chi_2(y) e\left(\frac{f(x, y)}{p}\right)$$

# Key Tools

- (1) Deligne ...
- (2) Tannakian categories
- (3) "Vanishing theorems"

(4) Sawin's quantitative sheaf theory

→ Associate to algebraic objects a "complexity" measure and show that "all" algebraic operations do not increase complexity too much.

# The recognition problem

For a concrete family

$$\left[ S(x, a) = \frac{1}{\sqrt{p}} \sum \chi(x) e\left(\frac{ax}{p}\right) e\left(\frac{f(x)}{p}\right) \right]$$

the "universal" theorem does not tell us what the distribution looks like until

we compute the group  $\mathbb{K}$  ("Monodromy group",

$$\mathbb{K} \subset U_n(\mathbb{C})$$

Q. How can we do this?

# Ex. 1 - ("Larsen's Alternative")

$$M_{2m}(K) = \int_{K} |\text{Tr}(g)|^{2m} \quad K \subset U_n(\mathbb{C})$$

can sometimes be computed using the equidistribution. Sometimes this is enough.

Ex.

$$\frac{1}{p(p-1)} \sum_{\substack{a, x \\ \equiv \equiv}} \left| \frac{1}{\sqrt{p}} \sum_x \chi(x) e\left(\frac{ax}{p}\right) e\left(\frac{f(x)}{p}\right) \right|^4$$

$\xrightarrow{p \rightarrow \infty} 2$

$\rightsquigarrow M_4(K) \neq 2 \xrightarrow[\text{(almost)}]{\text{(Larsen)}} K \supset SU_n(\mathbb{C}).$

Ex. 2 (Krämer, F-F-K)

$X$  smooth cubic hypersurface in  $\mathbb{P}^4$   
over  $\mathbb{F}_p$

(ex. (Klein))

$$v^2w + w^2x + x^2y + y^2z + z^2v = 0$$

$F = \{ \text{lines } \subset X \}$ ; smooth surface

"Fano"

$A = \text{Pic}(F)$  [intermediate jacobian]

alg. group, dimension 5 [so about  
 $p^5$  characters mod  $p$ ]

$i: F \hookrightarrow A$  immersion

$$S(\chi) = \frac{1}{p} \sum_{\ell \in F(\mathbb{F}_p)} \chi(\ell)$$

└ char. of  $A(\mathbb{F}_p)$

"Th". The group  $K$  has connected  
└ component of exceptional type  $E_6$ .

Criterion: if  $K \subset U_{27}(\mathbb{F})$  is:

(1) not self-dual  
(2) connected

(3) finite center  
(4)  $M_4(K) = 3$

then  $K$  has type  $E_6$ .

