27.5.21
(restart)

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_p} \chi_1(x)\, \chi_2(1-x)$$

$$J(\chi_1, \chi_2) = \frac{\tau(\chi_1)\,\tau(\chi_2)}{\tau(\chi_1\chi_2)}$$

Cor. $p \equiv 1 \bmod 4 \Rightarrow p = a^2 + b^2$ for some a, b in $\mathbb{Z}$.

Proof. Since $p \equiv 1 \bmod 4$,

$\mathbb{F}_p^\times \simeq \mathbb{Z}/4q\mathbb{Z}$ for some $q \geq 1$

so there exists

(1) $\chi_1 \neq 1$, $\chi_1^2 = 1$

$$\left[\mathbb{F}_p^\times \xrightarrow{\sim} \mathbb{Z}/4q\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \simeq \{\pm 1\} \right]$$

(2) $\chi_2 \neq 1$, $\chi_2^2 \neq 1$, $\chi_2^4 = 1$

$$\left[\mathbb{F}_p^\times \xrightarrow{\sim} \mathbb{Z}/4q\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \simeq \{\pm 1, \pm i\} \right]$$

Now consider

$$J(\chi_1, \chi_2) = \frac{\tau(\chi_1)\,\tau(\chi_2)}{\tau(\chi_1\chi_2)}$$

$\chi_1\chi_2 \neq 1$ since $\chi_1 \neq \chi_2^{-1}$

Since χ_1 takes values $0, 1, -1$

χ_2 ——————— $0, \pm 1, \pm i$

the Jacobi sum has the form

$$a + ib$$

with a, b in $\mathbb{Z}$; then

$$a^2 + b^2 = |J(\chi_1, \chi_2)|^2$$

$$= \frac{|\tau(\chi_1)\,\tau(\chi_2)|^2}{|\tau(\chi_1\chi_2)|^2}$$

$$= \frac{p \cdot p}{p} = p$$

□

N.B. There exist polynomial-time algorithms to compute a_p and b_p (Schoof).

Proof of the formula for $J(\chi_1, \chi_2)$

$$J(\chi_1, \chi_2) = (\chi_1\chi_2(1)\chi_1\chi_2(1)) \cdot \sum_{x} \chi_1(x)\chi_2(1-x) \sum_{y \neq 0} \chi_1\chi_2(y) e\left(\frac{y}{p}\right)$$

$\chi_1\chi_2(1) = 1 \neq 0$

$$= \sum_{x, y \neq 0} \chi_1(xy)\chi_2(y(1-x)) e\left(\frac{y}{p}\right)$$

$z = xy$

$$\begin{cases} z = y \\ w = xy \end{cases} \iff \begin{cases} y = z \\ x = wz^{-1} \end{cases}$$

$$= \sum_{w, z \neq 0} \chi_1(w)\chi_2(z-w) e\left(\frac{z}{p}\right)$$

$$\begin{cases} u = w \\ v = z - w \end{cases} \iff \begin{cases} w = u \\ z = v + u \end{cases}$$

$$= \sum_{u,v} \chi_1(u)\,\chi_2(v)\, e\left(\frac{u}{p}\right) e\left(\frac{v}{p}\right)$$

$$= \tau(\chi_1)\ \tau(\chi_2)$$

□

2 - Kloosterman paths

Kloosterman sums : (Poincaré, 1912

Kloosterman, 1924)

p prime

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

$$Kl_2(a,b;p) = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p^\times} e\left(\frac{ax + b\bar{x}}{p}\right)$$

(where $x\bar{x} \equiv 1 \bmod p$)

Easy fact: $Kl_2(a,b;p) \in \mathbb{R}$

$$\overline{Kl_2(a,b;p)} = \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p^\times} e\left(\frac{-ax - b\bar{x}}{p}\right)$$

$$= \frac{1}{\sqrt{p}} \sum_{y \in \mathbb{F}_p^\times} e\left(\frac{ay + b\bar{y}}{p}\right)$$

$y = -x$

$\bar{y} = -\bar{x}$

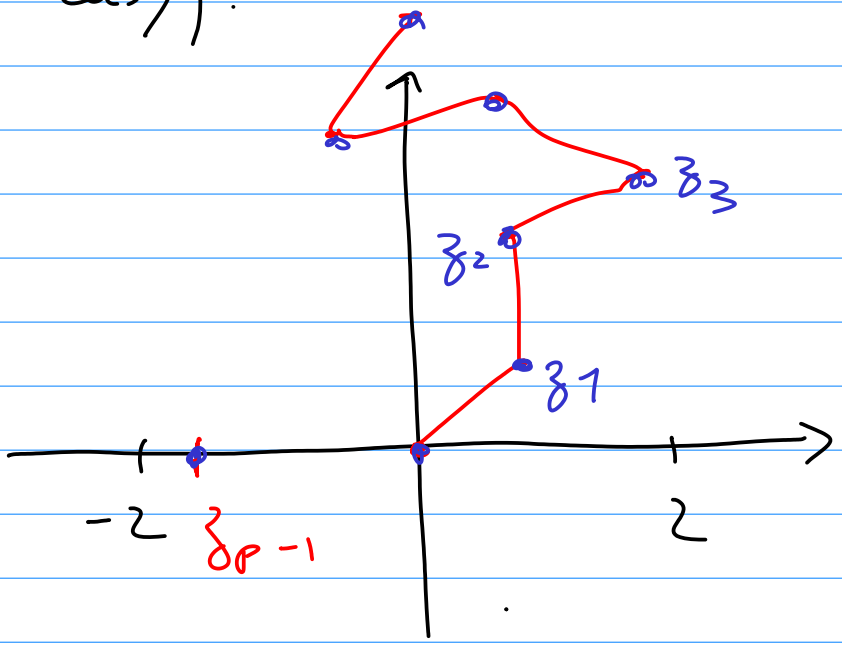
$$= Kl_2(a, b; p) \Big]$$

Hard fact: (Weil, 1948)

$$|Kl_2(a, b; p)| \leq 2$$

(confirming again the CLT heuristic for exponential sums).

(Elementary proofs are known, but not easy).



We consider how the full sum is obtained as last step of the sequence of partial sums

$$z_0 = 0, \quad z_j = \frac{1}{\sqrt{p}} \sum_{1 \le x \le j} e\left(\frac{ax+b\bar{x}}{p}\right)$$

$$(1 \le j \le p-1)$$

so that $z_{p-1} = Kl_2(a,b;p)$.

Q: (1) what shapes do we see ?

(2) do these sequences behave like a "random walk" ?

we link successive partial sums with line segments

The pictures certainly look quite "random" ...

To state the main theorem:

p prime $(\to \infty)$

$\Omega_p = \mathbb{F}_p^\times \times \mathbb{F}_p^\times$, with uniform prob. measure

$$C([0,1]) = \{ f : [0,1] \to \mathbb{C} \mid f \text{ continuous} \}$$

sep. Banach space with

$$\|f\| = \sup_{x \in [0,1]} |f(x)|$$

Define random variables

$$Kl_p : \Omega_p \to C([0,1])$$

by

$Kl_p(a,b) =$ the continuous function such that

$$j/p-1 \longmapsto Z_j(a,b)$$

$$= \frac{1}{\sqrt{p}} \sum_{1 \le x \le j} e\left(\frac{ax + b\bar{x}}{p}\right)$$

for $0 \leq j \leq p-1$

and is defined by linear interpola-

-tion for $\frac{j}{p-1} \leq t \leq \frac{j+1}{p-1}$.

The image $Kl_p(a,b)([0,1])$ of this function is the path we see in pictures.

[6.1.1]

Theorem (K. - Sawin, 2016)

As $p \to +\infty$, the r.v. Kl_p converge in law (as $C([0,1])$-valued r.v.) to the random "Fourier series"

$$K(t) = t\,ST_0 + \sum_{\substack{h \neq 0 \\ h \in \mathbb{Z}}} \frac{e(ht)-1}{2i\pi h} ST_h$$

$\uparrow$ $[0,1]$

where $(ST_h)_{h \in \mathbb{Z}}$ is a family

of i.i.d random variables with law

$$\mu_{ST} = \frac{1}{\pi}\sqrt{1-\frac{x^2}{4}}\,dx$$

on $[-2,2]$.

"Sato-Tate measure; semi-circle law"

Remarks:

(1) The series is interpreted as

$$\lim_{H\to+\infty} \sum_{1\le|h|\le H} (\dots)$$

and we will see that this series converges a.s. uniformly on $[0,1]$, so defines a $C([0,1])$-valued r.v.

(2) The same limit holds for normalized Birch sums, i.e. partial sums

$$\frac{1}{\sqrt{p}} \sum_{0 \le x \le j} e\left(\frac{ax+x^3}{p}\right)$$

for $a \in \mathbb{F}_p^\times$ (with uniform measure).

(3) As a corollary, we obtain by evaluating at $r=1$ the distribution of $Kl_2(a,b;p)$ as r.v. on Ω_p:

Th. (Katz; 1988)

The r.v. $(a,b) \longmapsto Kl_2(a,b;p)$ on Ω_p converge in law to

$$K(1) = ST_0 + \sum \frac{e(h)-1}{2i\pi h} ST_h \quad (\text{with } e(h)-1 = 0)$$

$$= ST_0, \text{ a Sato-Tate r.v.}$$

Cor. The constant 2 in Weil's

L bound cannot be improved

[because $\mathrm{Supp}(\mu_{ST}) = [-2, 2]$,

so

$$\liminf_{p \to \infty} \frac{1}{(p-1)^2} \left| \{ (a,b) \mid Kl_2(a,b;p) \geq 2 - \varepsilon \} \right| > 0$$

for all fixed $\varepsilon > 0$.]

3 - Outline of the proof

Step 0 - Motivation for the limit.

Step 1 - Prove some basic properties of the limit (e.g. $K(H)$ is well-defined as r.v. with values in $C([0,1])$).

Step 2 - Proof of convergence of finite distributions / proof of

convergence of Fourier coefficients

[i.e. for $0 \leq t_1 < t_2 < \cdots < t_h \leq 1$, want

$$\left(Kl_p(t_1), \ldots, Kl_p(t_h)\right) \xrightarrow[\text{in } \mathbb{C}^h]{\text{law}} \left(K(t_1), \ldots, K(t_h)\right)$$

(or

show that the sequence of "Fourier coefficients" of Kl_p converges in law to that of K]

Step 3 - Prove "tightness" of the sequence $(Kl_p)_{p \text{ prime}}$, which turns out to depend on arithmetic properties of the Kloosterman sums.

Note: Steps 0, 1, 2 can be generalized to many more sums (using deep results of Deligne and Katz on the Riemann Hypothesis over finite fields), but our proof of Step 3 really depends on special features which do not hold for all sums.