A pot-pourri on Equidistribution

Ph. Michel, EPF Lausanne
NuTMiC 2024

June 26, 2024

Definition

A sequence of finite (multi-)sets $(X(N))_{N\geq 1},\ X(N) \subset \mathbb{R}/\mathbb{Z}$ becomes uniformly distributed modulo 1 if $\forall 0 \leq a < b \leq 1$,

$$\frac{|\{x \in X(N),\ x \in [a,b]\}|}{|X(N)|} \to b - a = \mu_{Leb}([a,b]).$$

Equivalently, for any $\varphi \in \mathcal{C}(\mathbb{R}/\mathbb{Z})$

$$\frac{1}{|X(N)|} \sum_{x \in X(N)} \varphi(x) \to \int_{\mathbb{R}/\mathbb{Z}} \varphi(u) du$$

Über die Gleichverteilung von Zahlen mod. Eins.*)

Von

Hermann Weyl in Zürich.

§ 1.

Grundlagen. Der lineare Fall.

Es seien auf der Geraden der reellen Zahlen unendlich viele Punkte

$$\alpha_1, \alpha_2, \alpha_3, \cdots$$

Weyl's equidistribution criterion

Theorem (H. Weyl)

Given $\alpha \in \mathbb{R} - \mathbb{Q}$ *(eg.* $\alpha = \sqrt{2}$*) the sequence*

$$X(\alpha; N) = \{\alpha \pmod 1,\ 2\alpha \pmod 1, \cdots, N\alpha \pmod 1\} \subset \mathbb{R}/\mathbb{Z}$$

becomes uniformly distributed modulo 1. *For any* $\varphi \in \mathcal{C}(\mathbb{R}/\mathbb{Z})$

$$W(\varphi; N) := \frac{1}{N}\sum_{n \leq N} \varphi(\alpha.n) \to \int_{\mathbb{R}/\mathbb{Z}} \varphi(t)dt. \qquad \text{(W)}$$

Weyl's equidistribution criterion

It is sufficient to prove (W) for φ of the form

$$\varphi(u) = \exp(2\pi iku),\ k \in \mathbb{Z}.$$

Definition

Given X loc. compact Hausdorff and μ a regular Borel probability measure.
A sequence of finite (multi-)sets $(X(N))_{N\geq 1}$, $X(N) \subset X$ becomes uniformly distributed wrt μ if for any $\varphi \in \mathcal{C}_c(X)$

$$W(\varphi; N) := \frac{1}{|X(N)|} \sum_{x \in X(N)} \varphi(x) \to \int_X \varphi(u) d\mu(u). \qquad \text{(W)}$$

Weyl's equidistribution criterion

It is sufficient to prove (W) for φ in an ONB of $L^2(X,\mu)$ contained in $\mathcal{C}(X)$

Equidistribution in Galois groups

Theorem (Dirichlet-Landau)

Given $q \geq 1$. The multiset

$$\mathcal{P}(N;q) = \{p \,(\mathrm{mod}\, q),\ p \leq N,\ (p,q)=1,\} \subset (\mathbb{Z}/q\mathbb{Z})^\times$$

becomes ed in $(\mathbb{Z}/q\mathbb{Z})^\times$ relative to the uniform probability measure: $\forall a \,(\mathrm{mod}\, q) \in (\mathbb{Z}/q\mathbb{Z})^\times$

$$\frac{|\{p \leq N,\ p \equiv a \,(\mathrm{mod}\, q)\}|}{|\{p \leq N,\ (p,q)=1,\}|} \to \frac{1}{\varphi(q)}$$

This is a special (initial case) of the

Equidistribution for Galois groups

Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group $G(K/\mathbb{Q})$ and $G(K/\mathbb{Q})^\natural$ the set of conjugacy classes equipped with the Sato-Tate probability measure μ_{ST}: for $\sigma^\natural \subset G(K/\mathbb{Q})^\natural$ be the conjugacy class of $\sigma \in G(K/\mathbb{Q})$

$$\mu_{ST}(\sigma^\natural) = \frac{|\sigma^\natural|}{|G(K/\mathbb{Q})|}.$$

Theorem (Chebotareff density Theorem)

The multisets

$$\mathrm{Frob}(N;K) = \{\mathrm{Frob}_p,\ p \leq N,\ (p, D_K) = 1\} \subset G(K/\mathbb{Q})^\natural$$

become ed in $G(K/\mathbb{Q})^\natural$ wrt μ_{ST}.

Equidistribution in Galois groups

Chebotareff density theorem admits extensions to not necessarily finite Galois groups over *global fields*. In the number field case most are still conjectures but one is the (feu) Sato-Tate conjecture for elliptic curves: given $E/\mathbb{Q}$ an elliptic curve of discriminant D_E, for $p \nmid D_E$ let

$$a_p(E) := p + 1 - |E(\mathbb{F}_p)|; \text{ one has } |a_p(E)| \leq 2\sqrt{p}.$$

Theorem (Clozel/Harris/Shepherd-Barron/Taylor+...)

Suppose that $E/\mathbb{Q}$ is non-CM; the multisets

$$A(N; E) := \{\frac{a_p(E)}{\sqrt{p}},\ p \leq N,\ (p, D_E) = 1\} \subset [-2, 2]$$

becomes ed wrt the Sato-Tate measure

$$\mu_{ST}(u) = \frac{1}{2\pi}\sqrt{4 - u^2}du$$

Equidistribution for algebraic exponential sums

Over function fields (ie. $\mathbb{F}_q[U]$), many cases have been established by Deligne (on proving the Weil's conjecture) and in the subsequent work of Katz.

Given $q > 2$ a prime and $\chi \in \widehat{\mathbb{F}_q^\times}$ a non trivial multiplicative character modulo q, its normalized Gauss is

$$\varepsilon(\chi) := \frac{1}{q^{1/2}} \sum_{a \in \mathbb{F}_q} \chi(a) e_q(a),\ \ e_q(\bullet) = \exp(2\pi i \frac{\bullet}{q}).$$

One has

$$\varepsilon(\chi) = e^{i\theta_\chi},\ \ \theta_\chi \in \mathbb{R}/2\pi\mathbb{Z}.$$

Theorem (Deligne)

As $q \to \infty$ the multiset of angles

$$\Xi(q) := \{\theta_\chi,\ \chi \,(\mathrm{mod}\, q),\ \chi \neq 1\} \subset \mathbb{R}/2\pi\mathbb{Z}$$

becomes uniformly distributed.

Equidistribution for algebraic exponential sums

By Weyl's criterion is suffice to prove that for $k \in \mathbb{Z} - \{0\}$

$$W(k;q) := \frac{1}{q-2} \sum_{\chi \neq 1} \varepsilon(\chi)^k \overset{?}{\to} 0.$$

One has

$$W(k;q) = \frac{q-1}{q-2} \frac{1}{q^{1/2}} \mathrm{Kl}_{|k|}(\pm 1; q) - \frac{(-1)^k}{q^{k/2}}.$$

with for $u \in \mathbb{F}_q^\times$ and $k \geq 1$

$$\mathrm{Kl}_k(u;q) := \frac{1}{q^{\frac{k-1}{2}}} \sum_{x_1.\cdots.\mathbf{x}_k = u} e_q(x_1 + \cdots + x_k)$$

is the hyper-Kloosterman sum in $k-1$ variables.

Equidistribution for algebraic exponential sums

Theorem (Deligne)

One has for $k \geq 1$

$$|\mathrm{Kl}_k(u;q)| \leq k+1.$$

In particular for $k \in \mathbb{Z} - \{0\}$

$$|W(k;q)| \leq 2\frac{|k|+1}{q^{1/2}} \to 0.$$

When $k = 2$,

$$\mathrm{Kl}_2(u;q) := \frac{1}{q^{1/2}} \sum_{x_1.x_2=u} e_q(x_1+x_2)$$

is the usual Kloosterman sum which is ubiquitous in the theory of modular forms.

Equidistribution for algebraic exponential sums

One may then look as the distribution of these exponentiel sums: for instance for $k=2$ (then $\mathrm{Kl}_2(u;q)\in\mathbb{R}$) one has

Theorem (Katz)

The multiset

$$\mathrm{KL}_2(q)=\{\mathrm{Kl}_2(u;q),\ u\in\mathbb{F}_q^\times\}\subset[-2,2]$$

becomes ed wrt the Sato-Tate measure

$$\mu_{ST}(u)=\frac{1}{2\pi}\sqrt{4-u^2}du$$

Similar Sato-Tate equidistribution laws exist for the $\{\mathrm{Kl}_k(u;q),\ u\in\mathbb{F}_q^\times\}$.

Equidistribution for algebraic exponential sums

The key concept for the proof is the existence of an ℓ-adic sheaf ($\ell \neq q$), the Kloosterman sheaf, a Galois representation of the function field $\mathbb{F}_q(U)$

$$\mathcal{K}\ell_2 : \mathsf{Gal}(\mathbb{F}_q(U)^{sep}/\mathbb{F}_q(U)) \to \mathsf{SL}_2(\overline{\mathbb{Q}_\ell}) \hookrightarrow \mathsf{SL}_2(\mathbb{C})$$

with trivial determinant, unramified outside 0 and ∞ and such that

- $\forall u \in \mathbb{F}_q^\times$
$$\mathrm{tr}(\mathrm{Frob}_{(U-u)}|\mathcal{K}\ell_2) = \mathrm{Kl}_2(u;q);$$
- (Katz) its geometric monodromy group is as big as possible:
$$G^{geom}(\mathcal{K}\ell_2) := \mathcal{K}\ell_2(\mathsf{Gal}(\mathbb{F}_q(U)^{sep}/\overline{\mathbb{F}_q}(U)))^{Zar} = \mathsf{SL}_2(\overline{\mathbb{Q}_\ell})$$

Equidistribution for algebraic exponential sums

The Sato-Tate measure μ_{ST} is the push-forward of the Haar measure $\mu_{\mathsf{SU}_2(\mathbb{C})}$ by the trace map

$$\mathsf{tr} : \mathsf{SU}_2(\mathbb{C}) \to [-2, 2] \subset \mathbb{R}.$$

For Hyper-Kloosterman sums $\mathrm{Kl}_k(u; q)$, there exists a similar hyper-Kloosterman Galois representation with trivial determinant such that

- $\forall u \in \mathbb{F}_q^\times$
$$\mathsf{tr}(\mathrm{Frob}_{(U-u)} | \mathcal{K}\ell_k) = \mathrm{Kl}_k(u; q);$$
- (Katz) its geometric monodromy group is as big as possible:
$$G^{geom}(\mathcal{K}\ell_k) = \mathsf{SL}_k(\overline{\mathbb{Q}_\ell}).$$

Equidistribution over short intervals

Combining methods from analytic number theory and ℓ-adic cohomology it is possible to obtain further refinements of the above: for instance given $1 \leq N \leq q-1$ one can consider the truncated set of Kloosterman sums

$$\mathrm{KL}_2(N;q) = \{\mathrm{Kl}_2(n;q) = \mathrm{Kl}_2(n \pmod q; q),\ 1 \leq n \leq N\} \subset [-2,2].$$

Theorem (M.)

For any $N \geq q^{1/2}\log^2 q$ the multiset $\mathrm{KL}_2(N;q)$ becomes equidistributed on $[-2,2]$ wrt the Sato-Tate measure μ_{ST}.

Joint Equidistribution

Another refinement is to consider joint equidistribution; for instance for $a \neq 1$, the distribution of the pairs

$$\mathrm{KL}_{2,(1,a)}(q) := \{(\mathrm{Kl}_2(u;q), \mathrm{Kl}_2(au;q)),\ u \in \mathbb{F}_q^\times\} \subset [-2,2]^2.$$

Theorem

As $q \to \infty$ and $a = a_q \in \mathbb{F}_q^\times - \{\pm 1\}$, the set $\mathrm{KL}_{2,(1,a)}(q)$ becomes equidistributed in $[-2,2] \times [-2,2]$ relative to the product measure $\mu_{ST} \otimes \mu_{ST}$

The proof builds in a Goursat type argument (Goursat-Kolchin-Ribet criterion) applied to the Galois representation (sheaf)

$$\mathcal{K}\ell_2 \oplus [\times a]^* \mathcal{K}\ell_2$$

to show that its geometric monodromy group is as big as possible ($\mathrm{SL}_2 \times \mathrm{SL}_2$).

Equidistribution along the primes

Combining the two results above along with sieve techniques, one can then show that

Theorem (M.)

As $q \to \infty$ the multiset

$$\{\mathrm{Kl}_2(p; q),\ 1 \leq p \leq q-1,\ p \textit{ prime}\} \subset [-2, 2]$$

becomes equidistributed on $[-2, 2]$ wrt the Sato-Tate measure μ_{ST}.

Such results with further strenghtenings have applications to the study of the low-lying zeros in families of automorphic L-functions.

Summing trace function over short intervals

Hyper-Kloosterman sums

$$\mathrm{Kl}_k(\bullet; q) : u \in \mathbb{F}_q^\times \mapsto \mathrm{Kl}_k(u; q)$$

are example of trace functions and occur regularly in analytic number theory when studying congruence classes.
Given such a trace function $K : u \mapsto K(u)$ one would like to be able to evaluate its sum over intervals and typically prove that

$$\sum_{n \leq N} K(n) \stackrel{?}{=} o(N) \qquad \text{(sub-PV)}$$

for N as small compared to q as possible.

Summing trace function over short intervals

Under relatively simple, generic, assumptions on the underlying sheaf $\mathcal{K}$ (being a *Fourier* sheaf), one can show that the above holds as long as $N \geq q^{1/2} \log^2(q)$: this is the Polya-Vinogradov range. Going below the PV range is a major problem solved only in a very limited number of cases.

Theorem (Burgess)

For $K(u) = \chi(u)$, (Sub-PV) holds for $N \geq q^{1/4} \log^A q$.

Also recent techniques from additive combinatorics allow to pass below the PV range but for very special K.

Summing trace function over short intervals

Using joint equidistribution results for large tuples of exponential sums such as

$$(\mathrm{Kl}_k(a_1 u + b_1), \cdots, \mathrm{Kl}_k(a_{2d} u + b_{2d})) \in [-2, 2]^{2d}$$

for $(a_1, \cdots a_{2b})$, $(b_1, \cdots b_{2b})$ in "general" position allow to pass the PV range "on average":

Theorem (Kowalski-M.-Sawin)

Given $1 \leq M, N \leq q$ such that $MN^2 \geq q^{1+\varepsilon}$ for some $\varepsilon > 0$, one has

$$\sum_{m \leq M} \Big| \sum_{n \leq N} \mathrm{Kl}_k(mn; q) \Big| = o(MN).$$

For instance if $M = N \geq q^{1/3+\varepsilon}$.

Equidistribution and modular forms

Another important context where equidistribution is ubiquitous are spaces associated with modular forms (more generaly automorphic forms) such as the modular surface

$$X_0(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \simeq \mathrm{SL}_2(\mathbb{Z})\backslash \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}),$$

$$\mathbb{H} = \{z = x + iy \in \mathbb{C},\ y > 0\}$$

and more generally modular curves $X_0(N)$ that parametrize elliptic curves equipped with a level N structure.
A basic example of equidistribution is that for orbits of Hecke operators.

Equidistribution and modular forms: Hecke orbits

Given $z \in \mathbb{H}$ and q a prime, the q-Hecke orbit of $\mathrm{SL}_2(\mathbb{Z}).z$ is

$$T_q(z) := \mathrm{SL}_2(\mathbb{Z})\backslash\{\frac{z+b}{q},\ 0 \leq b \leq q-1,\ qz\} \subset X_0(1).$$

Theorem

As $q \to \infty$, the Hecke orbit $T_q(z)$ becomes equidistributed towards the hyperbolic measure $d\mu_{Hyp} := \frac{3}{\pi}\frac{dxdy}{y^2}$: for any $\varphi \in \mathcal{C}_c(X_0(1))$

$$\frac{1}{q+1}\Big(\sum_{b \,(\mathrm{mod}\, q)} \varphi(\frac{z+b}{q}) + \varphi(qz)\Big) \to \int_{X_0(1)} \varphi(z) d\mu_{Hyp}(z)$$

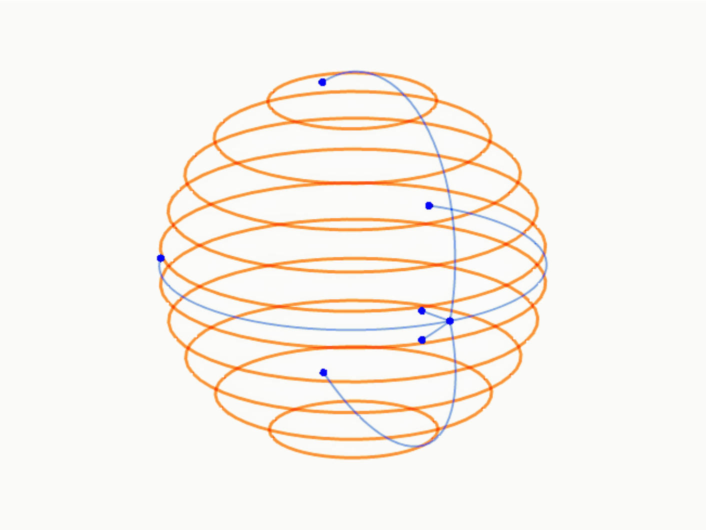
The proof is a consequence of the Petersson-Kuznetsov formula and the Weil's bound for Kloosterman sum

$$|\mathrm{Kl}_2(n;q)| \leq 2(\ll q^{1/2-\delta})$$

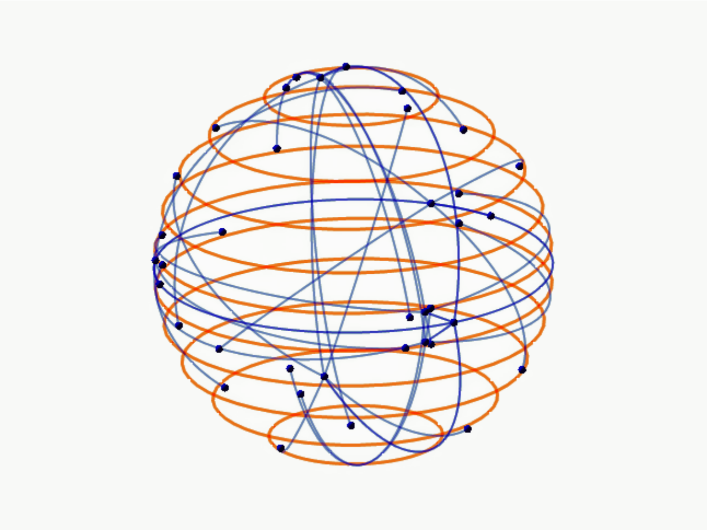
Equidistribution of Hecke orbits

Also q could be composite (for instance a power of a fixed prime q, say $q = 5$) which corresponds to iterating T_q several times; moreover via the Jacquet-Langlands correspondence there exists similar versions of the equidistribution of Hecke orbits for arithmetic quotients attached to other quaternion algebras/$\mathbb{Q}$

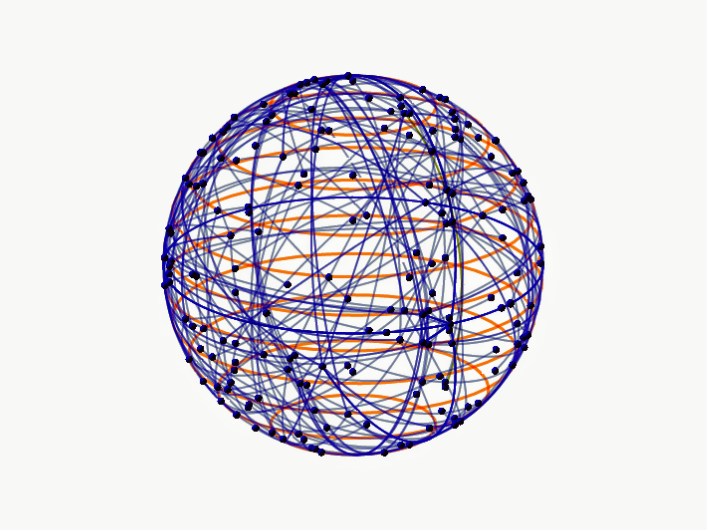
$q = 5$



$q = 5^2$



$q = 5^3$



Algebraically twisted Hecke orbits

Observe that for q a prime, a Hecke orbit is parametrized by the curve $\mathbb{P}^1(\mathbb{F}_q)$.

Combining the above with techniques from ℓ-adic cohomology, it is possible to impose further "algebraic" conditions on $b \pmod q$.

For instance (an example amongst many) is:

Theorem (Fouvry-Kowalski-M.)

Let $P(X) \in \mathbb{Z}[X]$ be non-constant. As $q \to \infty$, the algebraically twisted Hecke orbit

$$T_{q,P}(z) := \mathrm{SL}_2(\mathbb{Z})\backslash\{\frac{z+P(b)}{q},\ 0 \le b \le q-1\} \subset X_0(1)$$

becomes equidistributed wrt the hyperbolic measure $d\mu_{Hyp}$: for any $\varphi \in \mathcal{C}_c(X_0(1))$

$$\frac{1}{q}\sum_{b \pmod q} \varphi(\frac{z+P(b)}{q}) \to \int_{X_0(1)} \varphi(z)d\mu_{Hyp}(z)$$

Prime Hecke orbits

Another possible variant is to impose on b to be a *prime*:

Theorem (Ubis-Sarnak)

Assume the Ramanujan-Petterson conjecture for GL_2*.*
As $q \to \infty$*, the "prime" Hecke orbit*

$$T_{q,\mathcal{P}}(z) := \mathrm{SL}_2(\mathbb{Z})\backslash\{\frac{z+p}{q},\ 0 \leq p \leq q-1\} \subset X_0(1)$$

becomes dense in $X_0(1)$*. More precisely, any "nice" compact set* $\mathcal{K} \subset X_0(1)$ *contains at least a proportion of* $(\frac{1}{6} + o(1)\mu_{Hyp}(\mathcal{K})$ *of the "prime" Hecke points* $\mathrm{SL}_2(\mathbb{Z}).\frac{z+p}{q}$.

In the proof, prime detecting methods lead naturally to the following joint equidistribution problem.

Joint Hecke orbits

Question

Given $a \pmod q \in \mathbb{F}_q^\times$ (possibly varying with q); what is the distribution in $X_0(1) \times X_0(1)$ of the set of Hecke pairs

$$T_{q,(1,a)}(z) := \mathrm{SL}_2(\mathbb{Z})^2 \backslash \{(\frac{z+b}{q}, \frac{z+ab}{q}),\ 0 \leq b \leq q-1\}$$

as $q \to \infty$?

Obviously if $a = 1$, $T_{q,(1,1)}(z)$ equidistribute along the diagonal $X_0(1)^\Delta \subset X_0(1) \times X_0(1)$ toward the diagonal measure μ_{Hyp}^Δ; more generally, if a is constant with q, $T_{q,(1,a)}(z)$ will equidistribute along the graph of the Hecke correspondence T_a.

Equidistribution and modular forms

Let

$$m(q;a) := \min \Lambda_{q,a} \geq 1$$

where

$$\Lambda_{q,a} = \{(m,n) \in \mathbb{Z}^2,\ m - an \equiv 0 \pmod{q}\} \subset \mathbb{Z}^2.$$

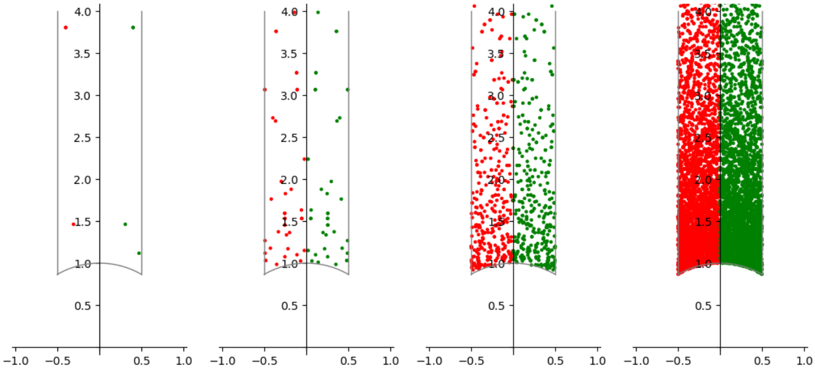
Theorem (Blomer-M.)

If $m(q;a) \to \infty$, the "joint" Hecke orbit $T_{q,(1,a)}(z)$ equidistribute in $X_0(1) \times X_0(1)$ relative to the product of hyperbolic measures $\mu_{Hyp} \otimes \mu_{Hyp}$.

An example when $m(q;a) \to \infty$ is for $3|q-1$ and

$$a^3 \equiv 1 \pmod{q},\ a \neq 1$$

$$q = 19,\ 199,\ 1997,\ 19997$$



Joint equidistribution of Hecke orbits

The Goursat type argument is replaced by a, recent, deep and general classification result due to Einsiedler-Lindenstrauss for joinings on products of S-arithmetic quotients (here $\mathrm{PGL}_2(\mathbb{Z}[1/S])^2 \backslash \mathrm{PGL}_2(\mathbb{Q}_S)^2$ for suitable S) which are invariant under a diagonalizable rank 2 action.

Definition

Given a group A and two measure preserving actions $A \curvearrowright (X, \mu_X)$, $A \curvearrowright (Y, \mu_Y)$. A joining between μ_X and μ_Y is an A-invariant measure μ on $X \times Y$ whose projections to X and Y are μ_X and μ_Y respectively.

Joint equidistribution of Hecke orbits

- The EL classification theorem is applied to any weak-$\star$ limit of the uniform probability measures supported at

$$\{\mathrm{SL}_2(\mathbb{Z})^2(\frac{z+b}{q}, \frac{z+ab}{q}),\ b \pmod q\}.$$

- Any such limit is invariant under the action of the two diagonal matrices (in diagonal position)

$$\begin{pmatrix} p_1 & 0 \\ 0 & p_1^{-1} \end{pmatrix}^{\Delta} \in \mathrm{PGL}_2(\mathbb{Q}_{p_1})^2,\ \begin{pmatrix} p_2 & 0 \\ 0 & p_2^{-1} \end{pmatrix}^{\Delta} \in \mathrm{PGL}_2(\mathbb{Q}_{p_2})^2$$

for two distinct fixed primes p_1, p_2 coprime with q: this reflect the simple fact that for $i = 1, 2$

$$\{(b, ab),\ b \pmod q\} = \{(p_i^2 b, a p_i^2 b),\ b \pmod q\} \in (\mathbb{Z}/q\mathbb{Z})^2.$$

Joint equidistribution of Hecke orbits

- In this situation, the EL classification theorem says that any weak-$\star$ limit is a convex combination of the full measure $\mu_{Hyp} \otimes \mu_{Hyp}$ and of "diagonal" measures.
- To eliminate the "diagonal" measures, we compute the limit

$$\frac{1}{q} \sum_{b \pmod q} \varphi_1(\frac{z+b}{q})\varphi_2(\frac{z+ab}{q})$$

for $m(q;a) \to \infty$ and for judiciously chosen Hecke eigenforms: eg. to rule out the pure diagonal measure μ^{Δ}_{Hyp} we take $\varphi_2 = \overline{\varphi}_1$ and show that the above limit is

$$0 = |\int_{X_0(1)} \varphi_1(u) d\mu_{Hyp}(u)|^2$$

which is distinct from

$$\mu^{\Delta}_{Hyp}(\varphi_1 \otimes \overline{\varphi}_1) = \int_{X_0(1)} |\varphi_1(u)|^2 d\mu_{Hyp}(u) > 0.$$

Joint equidistribution of Hecke orbits

- To prove that

$$\frac{1}{q}\sum_{b \pmod q}\varphi_1\left(\frac{z+b}{q}\right)\overline{\varphi}_1\left(\frac{z+ab}{q}\right) \to 0 \text{ as } m(q;a) \to \infty$$

we compute the sum using the Fourier expansions

$$\varphi_i(z) = \sum_n \lambda_i(n) W(|n|y) e(nx)$$

and then use the multiplicativity of the Hecke eignvalue

$$n \mapsto \lambda_i(n)$$

together with sieve type methods along with the fact that the $\lambda_i(p),\ p \in \mathcal{P}$ satisfy some Sato-Tate equidistribution law.

Equidistribution of CM point

Definition

A point $z = \mathrm{SL}_2(\mathbb{Z})z \in X_0(1)$ is CM if the associated elliptic curve

$$E_z = \mathbb{C}/\Lambda_z,\ \Lambda_z = \mathbb{Z} + z\mathbb{Z}$$

has complex multiplications by an order in an imaginary quadratic field K:

$$\mathrm{End}(E_z) = \{\tau \in \mathbb{C},\ \tau\Lambda_z \subset \Lambda_z\} = \mathscr{O}_{K,c} = \mathbb{Z} + c\mathscr{O}_K.$$

If q is prime and z has CM by $\mathscr{O}_{K,c}$ then the Hecke orbit $T_q(z)$ is made of CM point (most of which have CM by $\mathscr{O}_{K,cq}$. So the equidistribution of Hecke orbits carries some cases of the equidistribution of CM points.

Equidistribution of CM point

Given $\mathscr{O} = \mathscr{O}_{K,C}$ an imaginary quadratic order, let

$$\mathrm{CM}(\mathscr{O}) = \{[z] \in X_0(1),\ z \text{ has CM by } \mathscr{O}\} \subset X_0(1).$$

This is a principal homogenous space under the action of the ideal class group $\mathrm{Pic}(\mathscr{O})$ so that

$$|\mathrm{CM}(\mathscr{O})| = |\mathrm{Pic}(\mathscr{O})| = |\,\mathrm{disc}(\mathscr{O})|^{1/2+o(1)} = |D_K c^2|^{1/2+o(1)}.$$

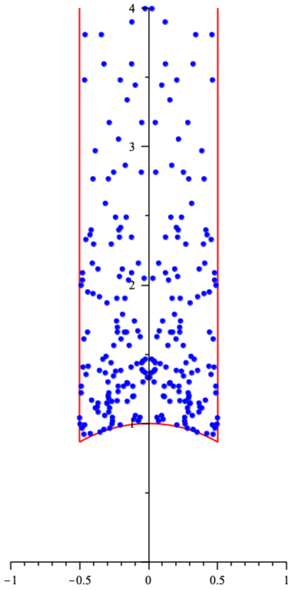
Theorem (Duke)

As $D_K c^2 \to \infty$ the set $\mathrm{CM}(\mathscr{O}_{K,c})$ becomes equidistributed relative to μ_{Hyp}.

The hard part due to Duke (and Iwaniec) is when $c = |D_K|^{o(1)}$; by now the most "natural" proof is via Weyl equidistribution criterion and subconvex bounds for degree 2 L-functions:

$$L(\varphi \times \chi_K, 1/2) \ll |D_K|^{1/2-\delta},\ \delta > 0.$$

$$D_K = -4 \times 104729$$



Equidistribution of CM point

Let ℓ be a prime inert in K, then any $E_z \in \mathrm{CM}(\mathscr{O})$ has supersingular reduction (at a(ny) place $\mathfrak{l}|\ell$):

$$\mathrm{red}_\ell : E_z \mapsto E_z \pmod{\mathfrak{l}} \in \mathrm{Ell}^{ss}(\mathbb{F}_{\ell^2})$$

Theorem (M./Elkies-Ono-Yang)

As $D_K c^2 \to \infty$ amongst the K for which ℓ is inert, $(\ell, c) = 1$, the multiset

$$\mathrm{red}_\ell(\mathrm{CM}(\mathscr{O}_{K,c})) \subset \mathrm{Ell}^{ss}(\mathbb{F}_{\ell^2})$$

becomes equidistributed relative to a natural probability (Haar) measure μ_ℓ on $\mathrm{Ell}^{ss}(\mathbb{F}_{\ell^2})$.
In particular red_ℓ is surjective for $D_K c$ large enough.

The key point is for $c = |D_K|^{o(1)}$. The proof also uses subconvexity for L-functions as $\mathrm{Ell}^{ss}(\mathbb{F}_{\ell^2})$ is realized as an adelic quotient attached to the quaternion algebra $B_{\infty,\ell}$.

Joint Equidistribution of CM point

Let $\mathbf{l} = (\ell_1, \cdots, \ell_s)$ be a tuple of distinct primes all inert in K, then one has a multireduction map

$$\mathrm{red}_{\mathbf{l}} : E_z \mapsto (E_z \pmod{\mathfrak{l}_1}, \cdots, E_z \pmod{\mathfrak{l}_s}) \in \prod_j \mathrm{Ell}^{ss}(\mathbb{F}_{\ell_j^2}).$$

We have a Chinese Reminder Theorem for CM elliptic curves:

Theorem (Aka, Luethi, M., Wieser)

As $D_K c^2 \to \infty$ amongst the K for which all ℓ_j are inert, $(\ell_j, c) = 1$, and p_1, p_2 split in K, the multiset

$$\mathrm{red}_{\mathbf{l}}(\mathrm{CM}(\mathscr{O}_{K,c})) \subset \prod_i \mathrm{Ell}^{ss}(\mathbb{F}_{\ell_j^2})$$

becomes equidistributed relative to the product measure $\otimes_j \mu_{\ell_j}$. In particular $\mathrm{red}_{\mathbf{l}}$ is surjective for $D_K c$ large enough.

Joint Equidistribution of CM point

The proof uses again the classification Theorem of E.L applied to any weak-$\star$ limit of the image by $\mathrm{red}_{\mathbf{l}}$ of the uniform probability measure on $\mathrm{CM}(\mathscr{O}_{K,c})$. For this one uses

- The homogenous space structure $\mathrm{Pic}(\mathscr{O}_{K,c}) \curvearrowright \mathrm{CM}(\mathscr{O}_{K,c})$ and the fact that the action "commutes" with $\mathrm{red}_{\mathbf{l}}$.
- The fact that such measure projects to μ_{ℓ_j} for every $j = 1, \cdots, s$ (by Duke's theorem).
- The splitting condition at p_1, p_2 implies that such measure is invariant under two diagonalisable elements

$$\begin{pmatrix} p_i & 0 \\ 0 & p_i^{-1} \end{pmatrix}^{\Delta} \in \prod_j \mathsf{PB}^{\times}_{\infty,\ell_j}(\mathbb{Q}_{p_i}) \simeq \mathsf{PGL}_2(\mathbb{Q}_{p_i})^s, \ \ i = 1, 2.$$

Joint Equidistribution of CM point

However the proof is easier than for the distribution of joint Hecke orbits since there is NO diagonal measure to rule out (because the $\mathrm{PB}^{\times}_{\infty,\ell_j}$ are non-isogenous for distinct ℓ_j).

Thank you

THANK YOU !