Equidistribution of CM points on products

Ph. Michel, EPF Lausanne

A series of joint works with
M. Aka, M. Luethi, A. Wieser, R. Menares, V. Blomer

Around Frobenius Distributions III

10 octobre 2022

Elliptic curves

An elliptic curve E/F is a smooth algebraic curve of genus 1 such that $E(F) \neq \emptyset$. It admits a projective plane embedding plane $(\mathrm{Char}(F) \neq 2, 3)$

$$ZY^2 = 4X^3 - g_2(E)Z^2X - g_3(E)Z^3,\ \ g_2(E), g_3(E) \in F.$$

$$\Delta(E) = g_2(E)^3 - 27g_3(E)^2 \neq 0.$$

It has the structure of an abelian group which is the plane model is given by the usual chord/tangent construction. The isomorphism class of $E/\overline{F}$ is determined by the j-invariant

$$j(E) = 1728g_2(E)/\Delta(E).$$

CM elliptic curves

Let

$$\mathcal{O}_E := \mathrm{End}_{\overline{F}}(E) = \{\varphi : E/\overline{F} \mapsto E/\overline{F},\ \varphi(0_E) = 0_E\}.$$

be its ring of endomorphisms of $E/\overline{F}$.

1. Ordinary case : $\mathcal{O}_E = \mathbb{Z}.\mathrm{Id}_E$ ($\implies \mathrm{Char}(F) = 0$).
2. CM case :

$$\mathcal{O}_E \simeq \mathscr{O}_D = \mathbb{Z} + (D/D_K)\mathscr{O}_K,\ \ K = \mathbb{Q}(\sqrt{D}), D < 0.$$

3. Supersingular case :

$$\mathcal{O}_E \simeq \mathcal{O}_p$$

with $\mathcal{O}_p \subset \mathrm{B}_p$ a maximal order in the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. ($\implies \mathrm{Char}(F) = p$ and $j(E) \in \mathbb{F}_{p^2}$).

CM ELLIPTIC CURVES

If $F \subset \mathbb{C}$, the complex points $E(\mathbb{C})$ identify with a complex torus

$$E(\mathbb{C}) \simeq \mathbb{C}/\Lambda,\ \Lambda \subset \mathbb{C}$$

via

$$z + \Lambda \neq \Lambda \mapsto (\mathfrak{P}(z,\Lambda), \mathfrak{P}'(z,\Lambda))$$

$$\mathfrak{P}(z,\Lambda) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda - \{0\}} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}.$$

and

$$\mathrm{End}(E) \simeq \mathrm{End}(\Lambda) = \{w \in \mathbb{C},\ w.\Lambda \subset \Lambda\}.$$

CM elliptic curves

$E/\mathbb{C}$ has CM iff for some discriminant $D < 0$

$$\mathrm{End}(\Lambda) = \{w \in \mathbb{C},\ w.\Lambda \subset \Lambda\} = \mathscr{O}_D.$$

In particular for $\mathfrak{a} \subset K \subset \mathbb{C}$ a (fractional) proper $\mathscr{O}_D$-ideal

$$E_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}$$

has CM by $\mathscr{O}_D$.

Conversely, any CM elliptic curve/$\mathbb{C}$ is of that shape.

CM elliptic curves

let

$$\mathcal{E}\ell\ell_D^{CM} := \{\text{elliptic curves}/\mathbb{C} \text{ with CM by } \mathscr{O}_D\}/\sim$$

and

$$\mathrm{Pic}(\mathscr{O}_D) = \{\text{proper } \mathscr{O}_D \text{ ideals } \mathfrak{a} \subset K\}/K^\times$$

the ideal class group.

Theorem (Gauss ?)

The map $\mathfrak{a} \mapsto \mathbb{C}/\mathfrak{a}$ *provides* $\mathcal{E}\ell\ell_D^{CM}$ *with the structure of a* $\mathrm{Pic}(\mathscr{O}_D)$*-torsor via the action* ($E \simeq \mathbb{C}/\Lambda$)

$$[\mathfrak{b}] \star E := [\mathbb{C}/\mathfrak{b}.\Lambda].$$

(One of) Duke's Equidistribution Theorems

Set

$$\mathcal{E}\ell\ell(\mathbb{C}) = \{\text{elliptic curves}/\mathbb{C}\}/\sim.$$

One has

$$\mathcal{E}\ell\ell(\mathbb{C}) \simeq \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} := Y_0(1)$$

via the map

$$\tau \in \mathbb{H} \mapsto \Lambda_\tau = \mathbb{Z} + \mathbb{Z}.\tau \mapsto \mathbb{C}/\Lambda_\tau$$

and the CM elliptic curves correspond to certain "CM" points on $Y_0(1)$:

$$\mathcal{E}\ell\ell_D^{CM} \simeq \mathcal{H}_D$$

$$\mathcal{H}_D = \mathrm{SL}_2(\mathbb{Z})\backslash\{\tau_{(a,b,c)} = \frac{-b + i|D|^{1/2}}{2a},\ b^2 - 4ac = D,\ (a,b,c) = 1\}$$

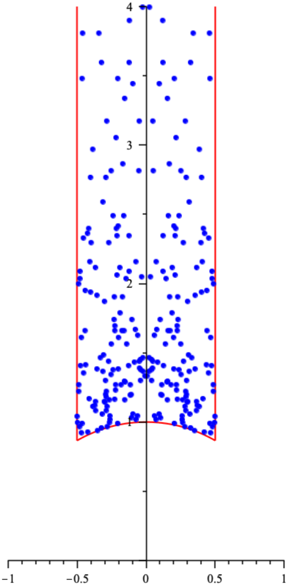
(One of) Duke's Equidistribution Theorems

Theorem (Duke)

As $D \to \infty$, the set $\mathcal{H}_D$ becomes equidistributed on $Y_0(1)$ w.r.t the hyperbolic measure $d\mu_\infty = \frac{3}{\pi}\frac{dxdy}{y^2}$: for $f \in \mathcal{C}_c(Y_0(1))$

$$\frac{1}{h(D)} \sum_{\tau \in \mathcal{H}_d} f(\tau) \to \int_{Y_0(1)} f(z) d\mu_\infty(z).$$

$$d = -418916$$



Reduction of CM elliptic curves

Given $E \in \mathcal{E}\ell\ell_D^{CM}$

- The j-invariant $j(E)$ is algebraic and E is defined over $H_D = K(j(E))$:

$$ZY^2 = 4X^3 - g_2(E)Z^2X - g_3(E)Z^3, \ g_2(E), g_3(E) \in H_D.$$

  The extension H_D/K is Galois and one has Artin reciprocity :

$$\theta : \mathrm{Pic}(\mathscr{O}_D) \simeq \mathrm{Gal}(H_D/K).$$

- In fact $j(E)$ is an algebraic integer (so E has potential good reduction at every prime).
- For $p > 2$ a prime and $\mathfrak{p}$ a $\overline{\mathbb{Q}}$-place above p, if p is inert or ramified in K, $E \pmod{\mathfrak{p}}$ is supersingular :

$$\mathrm{End}(E \pmod{\mathfrak{p}}) = \mathcal{O}_{E \pmod{\mathfrak{p}}} \simeq \mathcal{O}_p \subset \mathrm{B}_p.$$

Reduction of CM elliptic curves

Let

$$\mathcal{E}\ell\ell_p^{sups} = \{\text{Supersingular elliptic curves}/\overline{\mathbb{F}_p}\}/\sim .$$

For p is inert or ramified in K, there is a "reduction mod p" map

$$\mathrm{red}_p : E \in \mathcal{E}\ell\ell_D^{CM} \mapsto E \pmod{\mathfrak{p}} \in \mathcal{E}\ell\ell_p^{sups}$$

so that

$$j(E) \equiv j(e) \pmod{\mathfrak{p}}.$$

This also induce an embedding

$$\iota_p : \mathcal{O}_E \simeq \mathscr{O}_D \hookrightarrow \mathrm{End}(E \pmod{\mathfrak{p}}) \simeq \mathcal{O}_p$$

Reduction of CM elliptic curves

Another of Duke's theorems (joint with Schulze-Pillot) implies the following :

Corollary (M / Elkies-Ono-Yang)

As $D \to \infty$ along D such that $(D, p) = 1$ and p is inert in $K = \mathbb{Q}(\sqrt{D})$, the multiset $\mathrm{red}_p(\mathcal{E}\ell\ell_D^{CM})$ becomes equidistributed on $\mathcal{E}\ell\ell_p^{sups}$ w.r.t the measure μ_p defined for any $e \in \mathcal{E}\ell\ell_p^{sups}$ by

$$\mu_p(e) = \frac{|\mathcal{O}_e^\times|^{-1}}{\sum_{e' \in \mathcal{E}\ell\ell_p^{sups}} |\mathcal{O}_{e'}^\times|^{-1}}.$$

That is, as $D \to \infty$

$$\frac{|\{E \in \mathcal{E}\ell\ell_D^{CM},\ \mathrm{red}_p(E) = e\}|}{h(D)} \to \mu_p(e).$$

- Recently, Herrero, Menares and Rivera-Letellier have obtained a significant refinement of the above corollary :
  - The set of supersingular elliptic curves is the indexing set of a disjoint union of p-adic disks $\mathrm{D}_e,\ e \in \mathcal{E}\ell\ell_p^{ss}$ of radius 1 ; each disk D_e parametrize the deformations of the formal group $\hat{e}$ of the supersingular curve e.
  - The formal group of a CM curve $E/H_{D,\mathfrak{p}}$ reducing to e provides such a deformation and therefore yields a point on D_e. In other terms , the reduction modulo p map is refined to a map

$$\mathrm{form}_p : \mathcal{E}\ell\ell_D^{CM} \mapsto \bigsqcup_{e \in \mathcal{E}\ell\ell_p^{ss}} \mathrm{D}_e$$

p-ADIC EQUIDISTRIBUTION OF CM ELLIPTIC CURVES

- Recently, Herrero, Menares and Rivera-Letellier have obtained a significant refinement of the above corollary :
  - For each class of p-adic discriminant
    $$[D_p] \in (\mathbb{Z}_p - \mathbb{Z}_p^2)/(\mathbb{Z}_p^\times)^2,$$
    HMR-L have identified a probability measure $\mu_{e,[D_p]}$ supported along the subspace $\Lambda_{e,[D_p]} \subset \mathrm{D}_e$ (a p-adic annulus) of deformations $\hat{E}$ of $\hat{e}$ whose ring of formal endomorphisms satisfies
    $$\mathrm{End}(\hat{E}) \simeq \mathscr{O}_{D_p}.$$

p-adic equidistribution of CM elliptic curves

Let $\mu_{[D_p]}$ be the probability measure supported on the union

$$\Lambda_{[D_p]} := \bigsqcup_{e} \Lambda_{e,[D_p]}$$

given by

$$\mu_{[D_p]} := \sum_{e} \mu_p(e) \mu_{e,[D_p]}.$$

Theorem (HMR-L)

Given $[D_p]$ a p-adic discriminant class. As $D \to \infty$ along the fundamental discriminants satisfying $\mathscr{O}_D \otimes \mathbb{Z}_p \simeq \mathscr{O}_{D_p}$ the image $\mathrm{red}_p(\mathcal{E}\ell\ell_D^{CM})$ equidistribute according to the measure $\mu_{[D_p]}$.

Duke's orginal proof

Duke's theorems are consequences of equidistribution results for the representations of D by (the genus classes of) an integral ternary quadratic lattice (L, q).

- For $\mathcal{H}_D \subset Y_0(1)$ this is

$$(L, q) = ((\mathbb{Z}.\mathrm{Id}_2 + 2M_2(\mathbb{Z}))^0, -\det)$$

- For $\mathrm{red}_p(\mathcal{E}\ell\ell_D^{CM}) \subset \mathcal{E}\ell\ell_p^{sups}$ this is

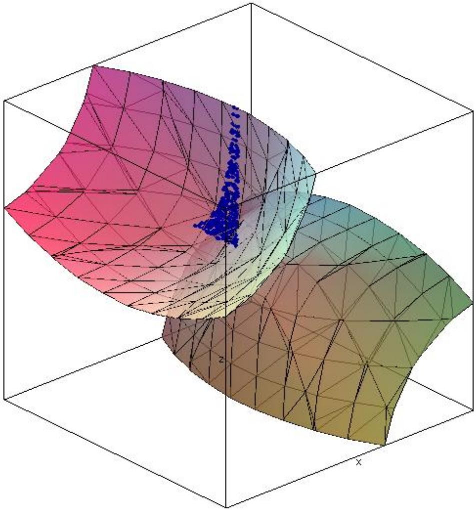
$$(L, q) = ((\mathbb{Z} + 2\mathcal{O}_p)^0, -\mathrm{Nr}_{\mathrm{B}_p})$$

- For $\mathrm{form}_p(\mathcal{E}\ell\ell_D^{CM}) \subset \bigsqcup_{e \in \mathcal{E}\ell\ell_p^{ss}} \mathrm{D}_e$ this is again

$$(L, q) = ((\mathbb{Z} + 2\mathcal{O}_p)^0, -\mathrm{Nr}_{\mathrm{B}_p})$$

  but with additional congruence constraints on the representations (modulo $p^v L$ for any $v \geq 1$).

$d = -194444$



Duke's orginal proof

- The corresponding Weyl sums are related to Fourier coefficients of 1/2-integral modular forms (Maass or holomorphic, cuspidal and Eisenstein). The decay of the Weyl sums follows from Siegel's mass formulae and non-trivial bounds for Fourier coefficients of cuspforms (Iwaniec in the holomorphic (large enough weight) case and Duke in the Maass and low weight cases).
- Duke's original proofs do not use (directly) the $\mathrm{Pic}(\mathscr{O}_D)$-torsor structure of $\mathcal{E}\ell\ell_D^{CM}$. This structure was however used in the 60's by Linnik who in the context of his ergodic method proved several equidistribution theorems for D restricted to certain congruence classes.

Reductions of CM elliptic curves

Fix primes $p_1, \cdots, p_s > 2$; for D such that all the p_i are inert in $K = \mathbb{Q}(\sqrt{D})$, we have a multireduction map on $\mathcal{E}\ell\ell_D^{CM}$

$$\mathrm{red} : E \mapsto (\mathrm{red}_\infty(E), \mathrm{red}_{p_1}(E), \cdots, \mathrm{red}_{p_s}(E)) \in Y_0(1) \times \prod_i \mathcal{E}\ell\ell_{p_i}^{ss}$$

where $\mathrm{red}_\infty(E) := \tau_E \in Y_0(1)$.

Conjecture

As $D \to \infty$ as above, the set $\mathrm{red}(\mathcal{E}\ell\ell_D^{CM})$ becomes ed. wrt probability measure $\mu_\infty \otimes \bigotimes_i \mu_{p_i}$.

Corollary (CRT for CM)

Fix $(j(e_1), \cdots j(e_s)) \in \prod_i \mathbb{F}_{p_i^2}$ a tuple of supersingular j-invariants ; for D large enough as above, there exists $\gg_{p_i} h(D)$ elliptic curves $E \in \mathcal{E}\ell\ell_D^{CM}$ such that

$$j(E) \equiv j(e_i) \pmod{\mathfrak{p}_i}, \ \ i = 1, \cdots, s.$$

Reductions of CM elliptic curves

Theorem (Cornut)

The conjecture holds when restricted to the subsequences of discriminants of the shape Dp^{2n} where $D < 0$ is a fixed fundamental discriminant, p is a fixed prime and $n \to \infty$.

- Cornut's proof (inspired by Vatsal) uses the torsor structure via ergodic theoretic methods, in particular Ratner's classification of joinings for unipotent flows on locally homogeneous spaces.
- Handling more general discriminants, is now possible thanks to a powerful classification theorem for joinings for diagonalizable rank 2 actions of Einsiedler and Lindenstrauss.

Reductions of CM elliptic curves

Theorem (ALMW)

Let q_1, q_2 be two primes $\neq p_i$. The conjecture holds for the subsequence of D's as above and satisfying in addition that q_1, q_2 are split in K.

The assumption that q_1, q_2 split K is a condition of Linnik's type.

Reductions of CM elliptic curves

In the case of two factors, Blomer and Brumley have given another proof, trading the splitting hypothesis at q_1, q_2 for another one :

Theorem (Blomer-Brumley)

Under the GRH for suitable L-functions, the conjecture holds for the two maps

$$\mathrm{red}_{\infty,p_1} : E \mapsto (\mathrm{red}_\infty(E), \mathrm{red}_{p_1}(E)) \in Y_0(1) \times \mathcal{E}\ell\ell_{p_1}^{ss}$$

$$\mathrm{red}_{p_1,p_2} : E \mapsto (\mathrm{red}_{p_1}(E), \mathrm{red}_{p_2}(E)) \in \mathcal{E}\ell\ell_{p_1}^{ss} \times \mathcal{E}\ell\ell_{p_2}^{ss}$$

p-ADIC EQUIDISTRIBUTIONS OF CM ELLIPTIC CURVES

In ongoing joint work (ALMW together with with R. Menares), we are implementing the torus orbit/ergodic approach to obtain p-adic equidistribution for multiple factors : so far we have

THEOREM (ALMMW)

Let $p_1, \cdots, p_s, q_1, q_2$ be distinct primes and for $i = 1, \cdots, s$, let D_{p_i} be discriminants of quadratic $\mathbb{Z}_{p_i}$-orders such that $v_{p_i}(D_{p_i}) \leq 1$. As $D \to \infty$ amongst fundamental discriminants such that

- $\mathscr{O}_D \otimes \mathbb{Z}_{p_i} \simeq \mathscr{O}_{D_{p_i}}$,
- $q_1,\ q_2$ *split in* $\mathbb{Q}(\sqrt{D})$,

the image of the multi-formal groups map

$$\mathrm{form} : E \in \mathcal{E}\ell\ell_D^{CM} \mapsto (\mathrm{form}_{p_1}(E), \cdots, \mathrm{form}_{p_s}(E)) \in \prod_{i=1}^{s} \Lambda_{[D_{p_i}]}$$

equidistributes towards $\bigotimes_i \mu_{[D_{p_i}]}$

Corollary

For $i = 1, \cdots, s$ let E_i be a fixed CM elliptic curve with discriminant D_i satisfying $v_{p_i}(D_i) \leq 1$ and $v \geq 1$,
For any large enough fundamental discriminant D satisfying

- *p_i is inert or ramified in $\mathbb{Q}(\sqrt{D})$ for $i = 1, \cdots, s$,*
- *q_1, q_2 are split in $\mathbb{Q}(\sqrt{D})$,*
- *$v_{p_i}(D) = v_{p_i}(D_i)$, $i \leq s$,*

the number of $E \in \mathcal{E}\ell\ell_D^{CM}$ satisfying

$$j(E) \equiv j(E_i) \pmod{\mathfrak{p}_i^v}$$

is $\gg_{p_i,v} h(D)$.

Equidistribution for one factor

The images $\mathrm{red}_\infty(\mathcal{E}\ell\ell_D^{CM})$, $\mathrm{red}_p(\mathcal{E}\ell\ell_D^{CM})$ or $\mathrm{form}_p(\mathcal{E}\ell\ell_D^{CM})$ can be given a purely group theoretic interpretation ; for this, it is convenient (indispensable ?) to pass to the adelic setting.

– The spaces $Y_0(1)$ and $\mathcal{E}\ell\ell_p^{sups}$ are identified with adelic quotients of the shape

$$[\mathrm{G}] := \mathrm{G}(\mathbb{Q})\backslash\mathrm{G}(\mathbb{A}),\ [\mathrm{G}]_K := [\mathrm{G}]/K,\ K = K_\infty.K_f$$

where $\mathrm{G} = \mathrm{PGL}_2$ or $\mathrm{PB}_p^\times$, and

$$K = K_\infty.K_f,\ K_\infty \subset \mathrm{G}(\mathbb{R}),\ K_f \subset \mathrm{G}(\mathbb{A}_f)$$

is a suitable compact subgroup.

Equidistribution for one factor

Given $E \in \mathcal{E}\ell\ell_D^{CM}$, let T be the one dimensional $\mathbb{Q}$-torus

$$\mathrm{T} := \mathrm{res}_{K/\mathbb{Q}}\mathbb{G}_m/\mathbb{G}_m$$

The data $\mathrm{red}_\infty(E) = \tau_E \in Y_0(1)$ and $\mathrm{red}_p(E) \in \mathcal{E}\ell\ell_p^{sups}$ induce embeddings of $\mathbb{Q}$-algebraic groups

$$\mathrm{T} \hookrightarrow \mathrm{G}$$

Proposition

Under the above identifications the (multi)sets $\mathrm{red}_\infty(\mathcal{E}\ell\ell_D^{CM})$ *and* $\mathrm{red}_p(\mathcal{E}\ell\ell_D^{CM})$ *are identified with the image in* $[\mathrm{G}]_K$ *of an adelic torus orbit*

$$[\mathrm{T}.g] := \mathrm{T}(\mathbb{Q})\backslash\mathrm{T}(\mathbb{A}).g$$

for some $g \in \mathrm{G}(\mathbb{A})$

Waldspurger's formula & subconvexity

The Weyl sums (for one factor) can be evaluated through a beautiful formula :

Theorem (Waldspurger)

Let $\varphi : [\mathrm{G}] \to \mathbb{C}$ be an (factorable) automorphic form which is not a character, let $\pi \in \mathrm{Aut}(\mathrm{G})$ the autorep it generates, $\pi^{JL} \in \mathrm{Aut}(\mathrm{PGL}_{2,K})$ the base change to K of its Jacquet-Langlands correspondant, one has

$$\frac{|\int_{[\mathrm{T}]} \varphi(tg)\,dt|^2}{\langle \varphi, \varphi \rangle} = c.\frac{L(\pi_K^{JL}, 1/2)}{|D_K|^{1/2}} \prod_v \int_{\mathrm{T}(\mathbb{Q}_v)} \frac{\langle g_v.\varphi_v, t_v.g_v.\varphi_v \rangle}{\langle \varphi_v, \varphi_v \rangle}\,dt_v.$$

Here $c = c_{K,\varphi} > 0$ satisfies $c = |D_K|^{o(1)}$.

Waldspurger's formula & subconvexity

Waldspurger's formula reduces equidistribution to the following bound

$$L(\pi_K^{JL}, 1/2) = L(\pi, 1/2)L(\pi.\chi_K, 1/2) \ll |D_K|^{1/2-\eta},\ \eta > 0$$

which is an instance of the subconvexity problem and was solved by Duke, Friedlander and Iwaniec and to bounding the local integrals

$$\int_{\mathrm{T}(\mathbb{Q}_v)} \frac{\langle g_v.\varphi_v, t_v.g_v.\varphi_v\rangle}{\langle \varphi_v, \varphi_v\rangle} dt_v.$$

The latter was the approach taken by Clozel-Ullmo to establish Duke's equidistribution theorems for non-fundamental discriminants.

Waldspurger's formula & subconvexity

Waldspurger formula is in fact more general :

Theorem (Waldspurger)

Notations as above, for any character $\chi = \prod_v \chi_v : \mathrm{T}(\mathbb{Q})\backslash\mathrm{T}(\mathbb{A}) \mapsto \mathbb{C}^\times$

$$\frac{|\int_{[\mathrm{T}]} \varphi(tg)\chi(t)\,dt|^2}{\langle \varphi, \varphi \rangle} = c.\frac{L(\pi_K^{JL}.\chi, 1/2)}{|D_K|^{1/2}} \prod_v \int_{\mathrm{T}(\mathbb{Q}_v)} \chi_v(t_v)\frac{\langle g_v.\varphi_v, t_v.g_v.\varphi_v\rangle}{\langle \varphi_v, \varphi_v\rangle}\,dt_v.$$

This twisted formula plays a key role in the work of Blomer-Brumley : the required GRHs are for the degree 4 L-functions $L(\pi_K^{JL}.\chi, s)$ (which are special cases of Rankin-Selberg L-functions).

Equidistribution for several factors

Fix s distinct primes $p_i, i = 1, \cdots, s$

- One has an identification

$$\prod_i \mathcal{E}\ell\ell_{p_i}^{sups} \simeq [\mathbf{G}]_{\mathbf{K}} = \mathbf{G}(\mathbb{Q})\backslash\mathbf{G}(\mathbb{A})/\mathbf{K}$$

  with

$$\mathbf{G} = \prod_{i=1}^{s} \mathrm{G}_i,\ \mathrm{G}_i = \mathrm{PB}_{p_i}^{\times}$$

  and

$$\mathbf{K} = \mathbf{K}_\infty.\mathbf{K}_f,\ \mathbf{K}_\infty = \prod_i K_{\infty,i},\ \mathbf{K}_f = \prod_i K_{f,i}$$

Equidistribution for several factors

- Given $E \in \mathcal{E}\ell\ell_D^{CM}$, the images $\mathrm{red}_{p_i}(E) = e_i$ determine a diagonal embedding
$$\mathrm{T} \hookrightarrow \mathbf{G} = \prod_i \mathrm{G}_i$$
and a torus orbit
$$[\mathrm{T}.\mathbf{g}] \subset [\mathbf{G}],\ \mathbf{g} = (g_i)_{i \leq s}.$$
- However the fact that the projection $[\mathrm{T}.\mathbf{g}]/\mathbf{K} \subset [\mathbf{G}]/\mathbf{K}$ corresponds to the image of the multi-reduction map $\mathrm{red}(\mathcal{E}\ell\ell_D^{CM})$ is not immediate. This follows from a scheme theoretic version of the $\mathrm{Pic}(\mathscr{O}_D)$ action $[\mathfrak{a}]\star$ (Serre's $\mathfrak{a}$-transform). The properties of the $\mathfrak{a}$-transform imply that (with suitable definitions)
$$\mathrm{red}_p([\mathfrak{a}] \star E) = [\mathfrak{a}] \star \mathrm{red}_p(E).$$

Joinings

Consider the sequence of discriminants D inert at the p_i such that the two additional fixed primes q_1, q_2 split in $\mathbb{Q}(\sqrt{D})$.

- We have a sequence of probability measures $(\mu_D)_D$ on $\mathbf{G}(\mathbb{Q})\backslash\mathbf{G}(\mathbb{A})$ supported along translates of the diagonally embedded torus orbit $\mathrm{T}(\mathbb{Q})\backslash\mathrm{T}(\mathbb{A})$.
- By the splitting condition (up to taking subsequences) we may assume that these measures are invariant under the actions of the diagonal tuples

$$(\begin{pmatrix} q_1 & 0 \\ 0 & 1 \end{pmatrix})_{i=1,\cdots,s}, \ (\begin{pmatrix} q_2 & 0 \\ 0 & 1 \end{pmatrix})_{i=1,\cdots,s}.$$

Joinings

- Moreover their projections to each factor $[\mathrm{G}_i]$ equidistribute towards the expect measure (Duke's theorem).

Proposition

For each $i = 1, \cdots s$, any weak-$\star$-limit of the projection $\pi_{i,*}(\mu_D)$ converge to a $\mathrm{G}_i^1(\mathbb{A})$-invariant measure. Here G_i^1 is the image in $\mathrm{PB}_i^\times$ of B_i^1.

- Such limiting measures are called *joinings* and we may invoque now a special case of a BIG theorem :

Theorem (Einsiedler-Lindenstrauss)

Any weak-$\star$ limit of the $(\mu_D)_D$ is invariant under the subgroup

$$\mathbf{G}^1(\mathbb{A}) = \prod_{i=1}^{s} \mathrm{G}_i^1(\mathbb{A}).$$

Joinings

- It remains to evaluate the limits of $\mu_D(\chi)$ where

$$\chi(\bullet) = \prod_i \chi_i(\mathrm{Nr}_{\mathrm{B}_i}(\bullet))$$

is a product of characters (necessarily quadratic).

– This is much simpler and these can be done exactly.
– In the end, this leads to an explicit finite set of *exceptional* quadratic fields (their discriminants divide $p_1.\cdots.p_s$) for which the limiting measure is not the full mesure but supported along a coset) ; if $\mathbb{Q}(\sqrt{D})$ is not exceptional the limit is the full measure.

Shifted equidistribution

Another way to exploit the torsor structure is to consider shifted products : suppose $D = D_K$ and for each $[\mathfrak{b}] \in \mathrm{Pic}(\mathscr{O}_K)$, consider

$$\mathcal{E}\ell\ell_K^{CM,2,[\mathfrak{b}]} = \{(E, [\mathfrak{b}] \star E),\ E \in \mathcal{E}\ell\ell_K^{CM}\} \subset Y_0(1) \times Y_0(1).$$

Let $D_K \to \infty$ (and $[\mathfrak{b}]$) vary :

- If $[\mathfrak{b}]$ is principal or has a representative ideal of bounded norm then $\mathcal{E}\ell\ell_D^{CM,2,[\mathfrak{b}]}$ is contained in a finite set of modular curves embedded into $Y_0(1) \times Y_0(1)$ and subsequences of $\mathcal{E}\ell\ell_D^{CM,2,[\mathfrak{a}]}$ equidistribute along these (by Duke's theorem).

Shifted equidistribution

- If this is not the case, one expects

Mixing conjecture (M-Venkatesh)

If $\min_{\mathfrak{b}'\in[\mathfrak{b}]}\mathrm{Nr}(\mathfrak{b}')\to\infty$,

– *the set* $\mathcal{E}\ell\ell_D^{CM,2,[\mathfrak{b}]}$ *becomes equidistributed in* $Y_0(1)\times Y_0(1)$ *wrt* $\mu_\infty\otimes\mu_\infty$.

– *For any* $p>2$ *the set* $\mathrm{red}_p(\mathcal{E}\ell\ell_D^{CM,2,[\mathfrak{b}]})$ *is equidistributed in* $\mathcal{E}\ell\ell_p^{ss}\times\mathcal{E}\ell\ell_p^{ss}$ *wrt* $\mu_p\otimes\mu_p$ *(whenever* p *is inert or ramified in* K*).*

Shifted equidistribution

Theorem (Khayutin)

Given $q_1 < q_2$ two primes, the mixing conjecture is true when restricted to sequences of fundamental discriminant D such that

- q_1, q_2 *split in* K,
- $\zeta_K(s)$ *has no Siegel zero : the zeros of* $\zeta_K(s)$ *are at distance* $\gg 1/\log|D|$ *from* 1.

Theorem (Blomer-Brumley-Khayutin)

Same conclusion for all fundamental D's under GRH (no splitting condition).

Shifted equidistribution

The proof starts as above by using the joinings classification theorem of Einsiedler-Lindenstrauss, however (because the two factors are the same) this only yields

Theorem (Einsiedler-Lindenstrauss)

Any weak-$\star$ limit of the $(\mu_D)_D$ is a convex combination of measures invariant under one of the subgroups

$$\mathrm{G}^1(\mathbb{A}) \times \mathrm{G}^1(\mathbb{A}) \text{ or } \mathrm{G}^{1,\Delta}(\mathbb{A}) \subset \mathrm{G}^1(\mathbb{A}) \times \mathrm{G}^1(\mathbb{A})$$

Ruling out the second option is a very serious roadblock and is the bulk of Khayutin's work.

Shifted equidistribution

- Khayutin bounds the correlations between the $\mu_{\mathrm{T}_{D,\mathfrak{b}}}$ and the (unwanted) diagonal measure(s) μ_{G^Δ} : for $\Omega \subset [\mathrm{G} \times \mathrm{G}]$ compacts and $B \subset \mathrm{G}(\mathbb{A})$ a shrinking ball around the origin

$$\overline{\lim_D} \mu_{\mathrm{T}_{D,\mathfrak{b}}} \times \mu_{\mathrm{G}^\Delta}(\{(z,z') \in \Omega^2,\ z' \in (B \times B).z\}) \ll \mu_{\mathrm{G}}(B)^{1+\delta},\ \delta > 0?$$

- These correlations are bounded by the relative trace of the automorphic kernel of a smooth majorant of the function $1_{B\times B}$ for $\mathrm{T}_D \backslash \mathrm{G} \times \mathrm{G}/\mathrm{G}^\Delta$.

Shifted equidistribution

- The later is bounded by shifted convolution sums of the shape

$$\sum_{0<q_{\mathfrak{b}}(m,n)-|D|\leq\mu_{\mathrm{G}}(B)|D|} r_K(q_{\mathfrak{b}}(m,n)-|D|)$$

  When $\mathrm{Nr}(\mathfrak{b})$ is really large, these constrainst are too tight for harmonic analysis to be efficient. Instead Khayutin bounds this sums by relying on sieve methods *à la* Nair-Tenenbaum using the multiplicativity of $r_k(\bullet)$.
- The Siegel zero hypothesis is necessary to see that the resulting bound is good.

Shifted equidistribution : yet another variant

Theorem (Sarnak)

As $p \to \infty$, the integral points of the closed horocycle of height $1/p$

$$\{\frac{a+i}{p},\ a = 1, \cdots, p\} \subset \{x + \frac{i}{p},\ x \in]0,1]\} \subset Y_0(1)$$

become equidistributed on $Y_0(1)$.

In the same vein we look for $b \in [1, p-1]$ at the shifted product

$$\{(\frac{a+i}{p}, \frac{ab+i}{p}),\ a = 1, \cdots, p\} \subset Y_0(1) \times Y_0(1)$$

Shifted equidistribution : yet another variant

Let

$$\Lambda(b;p) = \{(n_1,n_2) \in \mathbb{Z}^2, n_1 - bn_2 \equiv 0 \,(\mathrm{mod}\, p)\}.$$

This is a lattice of volume p and set

$$m(b;p) = \min(\|(n_1,n_2)\|,\ (n_1,n_2) \in \Lambda(b;p) - \{0\}) \ll p^{1/2}$$

for its minimum

Theorem (Blomer-M)

Assume the Ramanujan-Petersson conjecture. As $m(b;p) \to \infty$, the shifted product

$$\{(\frac{a+i}{p}, \frac{ab+i}{p}),\ a = 1, \cdots, p\} \subset Y_0(1) \times Y_0(1)$$

becomes equidistributed.

Shifted equidistribution : yet another variant

The proof uses again the joinings classification theorem of Einsiedler-Lindenstrauss and the main ingredient to rule out the unwanted measure is the following bound for cuspidal Weyl sums :

Theorem (Blomer-M)

Assume the Ramanujan-Petersson conjecture. Let f_1, f_2 be two Hecke Maass cuspforms

$$\frac{1}{p}\sum_{a \pmod p} f_1\Big(\frac{a+i}{p}\Big)f_2\Big(\frac{ab+i}{p}\Big) \ll m(b;p)^{-1+o(1)} + (\log p)^{-1/9}.$$

Shifted equidistribution : yet another variant

Using the Fourier expansion and summing over a yields

$$\frac{1}{p} \sum_{n_1 \pm b n_2 \equiv 0 \pmod{p}} \lambda_1(n_1)\lambda_2(n_2)\, V_1(\frac{n_1}{p})\, V_2(\frac{n_2}{p})$$

Sticking to the $-$ case, by basis reduction, this sums equals

$$= \frac{1}{p} \sum_{l_1 n_1 - l_2 n_2 \equiv 0 \pmod{p}} \lambda_1(n_1)\lambda_2(n_2)\, V_1(\frac{n_1}{p})\, V_2(\frac{n_2}{p})$$

for

$$\|(l_1, l_2)\| = m(b; p) \ll p^{1/2}.$$

Shifted equidistribution : yet another variant

- If $m(b;p)$ is not too large $(\leq p^{\delta},\ \delta > 0)$ we write the congruence condition
$$l_1 n_1 - l_2 n_2 = ph,\ h \ll p^{1/2}.$$
For $h = 0$ we have a Rankin-Selberg type sum of size bounded by $\ll m(b;p)^{-1+o(1)}$.
- If $h \neq 0$ this is a shifted convolution problem for which one can apply spectral theory of automorphic forms for $\Gamma_0(l_1 l_2)$.

Shifted equidistribution : yet another variant

- If $m(b;p)$ is large ($\geq p^\delta,\ \delta > 0$), we bound the sum

$$\frac{1}{p}\sum_{(n_1,n_2)\in\Lambda(b;p)} |\lambda_1|(n_1).|\lambda_2|(n_2).|V_1|(\frac{n_1}{p}).|V_2|(\frac{n_2}{p})$$

  This sum of product of non-negative multiplicative functions along the lattice $\Lambda(b;p)$ is amenable to the sieve techniques of Erdos, Wolke, Nair-Tenebaum,... which were generalized recently by Holowinski, Holowinski-Soundararajan and Khayutin in similar equidistribution contexts.

Shifted equidistribution : yet another variant

These methods (along with the RP bound $|\lambda_i|(n) \leq d(n)$) yield

$$\frac{1}{p} \sum_{(n_1,n_2)\in\Lambda(b;p)} |\lambda_1|(n_1).|\lambda_2|(n_2).|V_1|(\frac{n_1}{p}).|V_2|(\frac{n_2}{p})$$

$$\ll p^{o(1)}(\frac{1}{p} + \frac{1}{z^{1/4}} + \frac{z^3}{m(b;p)}) + \frac{1}{\log^2 p} \exp(\sum_{q\leq z} \frac{|\lambda_1|(q) + |\lambda_2|(q)}{q})$$

Using Sato-Tate type bounds

$$\sum_{q\leq z} \frac{|\lambda_i|(q)}{q} \leq \frac{17}{18} \log\log z + O_i(1)$$

the second term is bounded by $(\log p)^{-1/9}$ on choosing $z = p^\gamma$ for $\gamma > 0$ small enough.

Shifted equidistribution : yet another variant

- the RP conjecture can be avoided everywhere excepted for the sieving part ($m(b;p)$ large).
- If f_1 or f_2 is an Eisenstein series, the SCP can possibly be carried out with some efforts (for $m(b;p)$ not too large). However it is unclear whether the sieving part can go through due to the "Sato-Tate" bound

$$\sum_{q \leq z} \frac{d(q)}{q} = 2 \log \log z + O(1)$$

which destroy the $\log^{-2} p$ decay in the Sieve type bound.

Shifted equidistribution : yet another variant

- Applying a functional equations for mod p twists or Voronoi summation one can deduce the following bound

$$\frac{1}{p^2}\sum_{n_1,n_2}\lambda_1(n_1)\lambda_2(n_2)\mathrm{Kl}_2(bn_1n_2;p)\,V_1(\frac{n_1}{p})\,V_2(\frac{n_2}{p})$$
$$\ll p^{-1/2}(m(b;p)^{-1+o(1)}+(\log p)^{-1/9}).$$

This is a very special case of a weak form of a more general algebraic mixing conjecture.

THANK YOU !