Some extensions of Duke's theorems

Ph. Michel, EPF Lausanne

Online Conference in Automorphic Forms

based on joint works with

M. Aka, M. Luethi, D. Ramakrishnan, A. Wieser

Rényi Institute, via Zoom 01 June - 05 June 2020

Duke's Theorems

Duke's Theorems (1988) are three equidistribution theorems for the set of representations of large integers by a fixed ternary (integer valued) quadratic form $q(a, b, c)$.
Given $d \in \mathbb{Z} - \{0\}$, the set of representation of d by q is

$$\mathcal{R}_q(d) := \{(a, b, c) \in \mathbb{Z}^3, q(a, b, c) = d\}.$$

Given $l \in \mathbb{R}$, the l-level set of q is

$$V_{q,l}(\mathbb{R}) := \{(x, y, z) \in \mathbb{R}^3, \ q(x, y, z) = l\}.$$

For $l = \text{sign}(d)$, one has

$$\frac{1}{|d|^{1/2}} \mathcal{R}_q(d) \subset V_{q,l}(\mathbb{R}).$$

Duke's Theorems

Theorem (Duke)

For q either of the quadratic forms

$$E_3(a,b,c) = -(a^2+b^2+c^2),\ \Delta(a,b,c) = b^2 - 4ac$$

As $d \to \infty$ such that

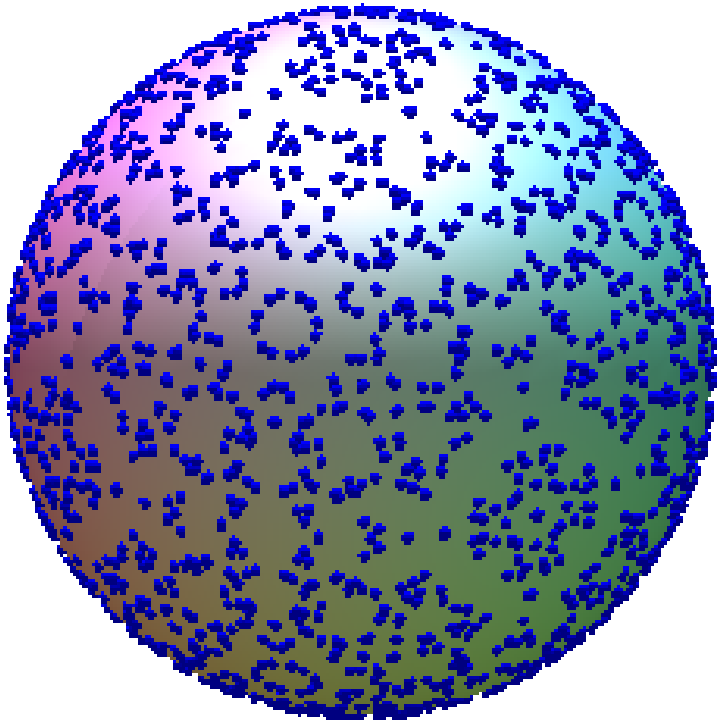
- *if $q = E_3$: $d < 0,\ d \neq 0,1,4 \mod 8$,*
- *if $q = \Delta,\ d \equiv 1 \mod 4$,*

the set $|d|^{-1/2}.\mathcal{R}_q(d)$ become equidistributed on $V_{q,\pm 1}(\mathbb{R})$ ($\pm 1 = \mathrm{sign}(d)$) wrt to the unique (up to scalars) $\mathrm{SO}_q(\mathbb{R})$-invariant measure $\mu_{q,\pm 1}$.

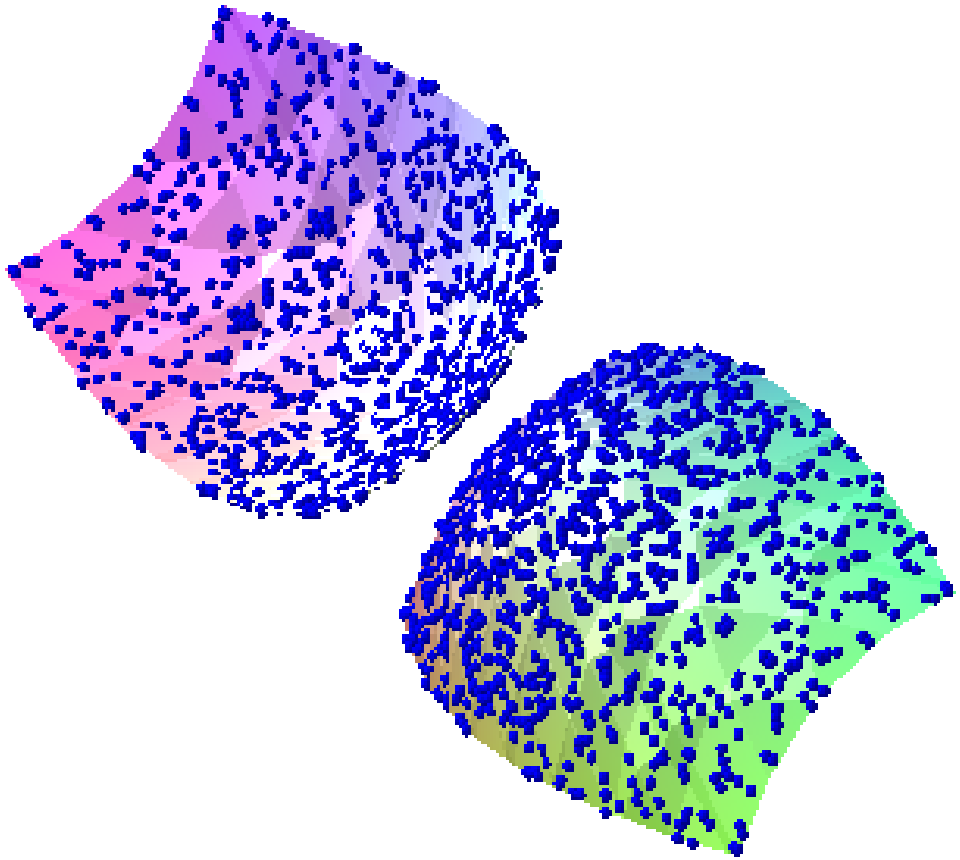
Remark

For E_3 this was also proven by Fomenko-Golubeva at about the same time.

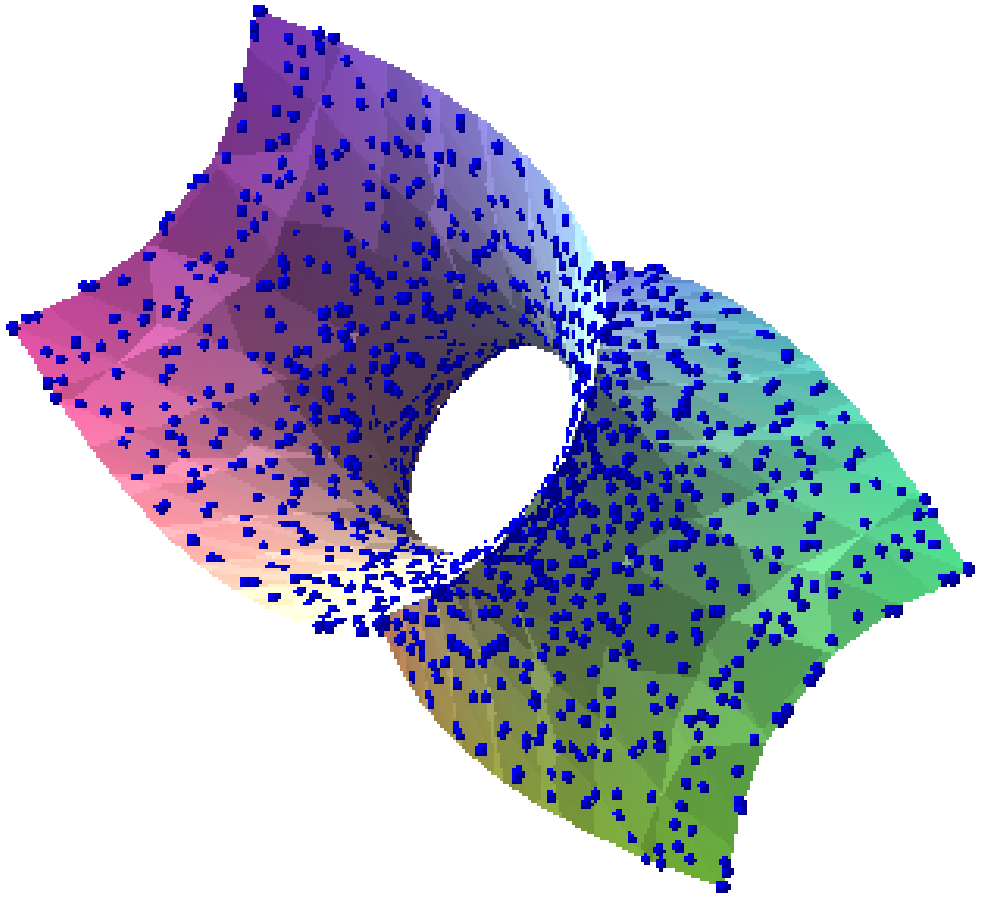
d=-40001



$d = -110003$



$d = 10001$



Duke's Theorems : dual formulation

Set $\mathrm{G} = \mathrm{SO}_q$. Choosing a base point $\mathbf{x} \in V_{q,\pm 1}(\mathbb{R})$ one has

$$V_{q,\pm 1}(\mathbb{R}) \simeq \mathrm{G}(\mathbb{R})/\mathrm{G}_{\mathbf{x}}(\mathbb{R}),\ \mathrm{G}_{\mathbf{x}} = \mathrm{Stab}_{\mathrm{G}}(\mathbf{x})$$

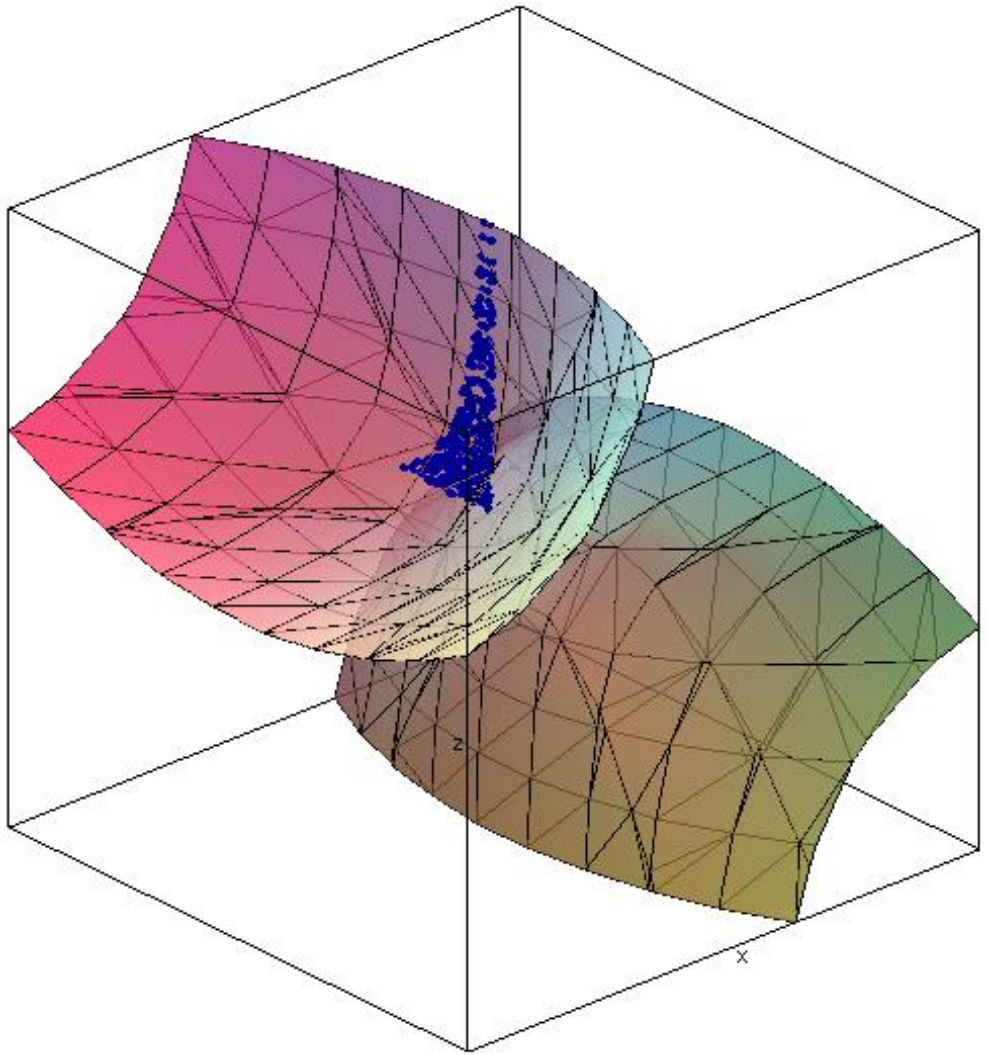
and

$$|d|^{-1/2}(a,b,c) \simeq g_{(a,b,c)}.\mathrm{G}_{\mathbf{x}}(\mathbb{R}).$$

The group $\mathrm{G}(\mathbb{Z})$ acts (on the left) on $\mathcal{R}_q(d)$ and decompose into finitely many orbits (classes)

$$[a,b,c] := \mathrm{G}(\mathbb{Z}).(a,b,c) \simeq \mathrm{G}(\mathbb{Z}).g_{(a,b,c)}.\mathrm{G}_{\mathbf{x}}(\mathbb{R})/\mathrm{G}_{\mathbf{x}}(\mathbb{R})$$

$$d = -194444$$



Duke's Theorems : dual formulation

Theorem (Duality principle)

TFAAE

- *Equidistribution of the finite union of (left)* $\mathrm{G}(\mathbb{Z})$*-orbits*

$$\bigsqcup_{[a,b,c]} \mathrm{G}(\mathbb{Z}).g_{(a,b,c)}\mathrm{G}_{\mathbf{x}}(\mathbb{R})/\mathrm{G}_{\mathbf{x}}(\mathbb{R})$$

  on $\mathrm{G}(\mathbb{R})/\mathrm{G}_{\mathbf{x}}(\mathbb{R}) \simeq V_{q,\pm 1}(\mathbb{R})$.

- *Equidistribution of the finite set of (right)* $\mathrm{G}_{\mathbf{x}}(\mathbb{R})$*-orbits*

$$\{\mathrm{G}(\mathbb{Z})\backslash\mathrm{G}(\mathbb{Z}).g_{(a,b,c)}.\mathrm{G}_{\mathbf{x}}(\mathbb{R}),\ [a,b,c] \in [\mathcal{R}_q(d)]\}$$

  on $\mathrm{G}(\mathbb{Z})\backslash\mathrm{G}(\mathbb{R})$.

Duke's Theorems : dual formulation

- For $q = E_3$ the dual form amounts to equidistribution of collection of circles at the surface of (a quotient of) the 3-sphere (which is a 2-covering of $\mathrm{SO}_q(\mathbb{R})$) and projecting to $\mathbb{R}^3$ we obtain points on the 2-sphere.
- For $q = \Delta$, $\mathrm{SO}_q \simeq \mathrm{PGL}_2$ and $\mathrm{PGL}_2(\mathbb{Z})\backslash \mathrm{PGL}_2(\mathbb{R})$ is identified with the unit tangent bundle of the modular curve

$$X_0(1) = \mathrm{PGL}_2^+(\mathbb{Z})\backslash\mathbb{H} \simeq \mathrm{PGL}_2(\mathbb{Z})\backslash \mathrm{PGL}_2(\mathbb{R})/\mathrm{PSO}_2(\mathbb{R})$$

Duke's Theorems : dual formulation

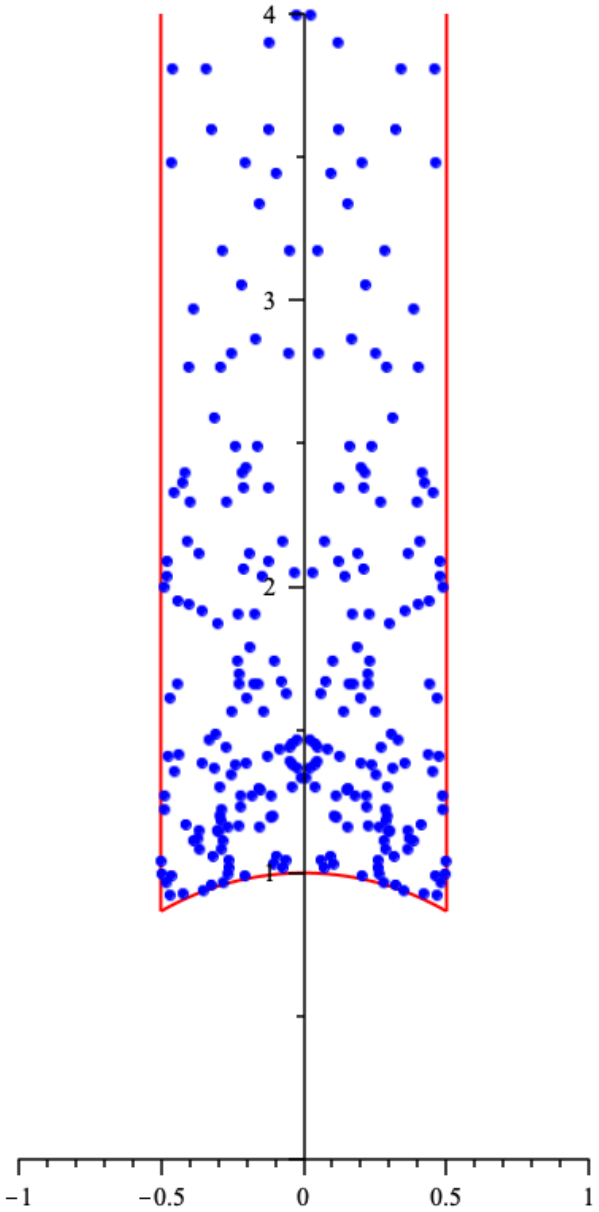
- For $d < 0$, Duke's theorem is equivalent to the equidistribution of Heegner points on the modular surface $X_0(1)$

$$z_{[a,b,c]} = \mathrm{SL}_2(\mathbb{Z}) z_{a,b,c}, \ z = \frac{-b + i|d|^{1/2}}{2a}, \ (a,b,c) \in \mathcal{R}_\Delta(d).$$

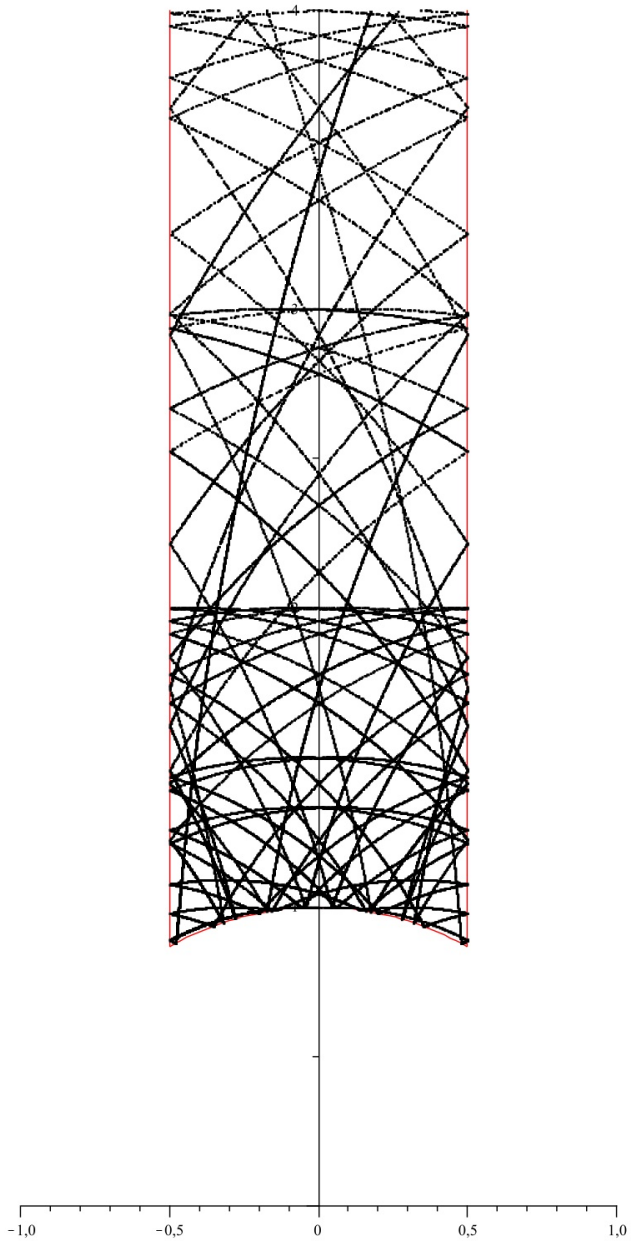
- For $d > 0$, this is equivalent to the equidistribution of closed geodesics $\gamma_{[a,b,c]}$ on the unit tangent bundle of $X_0(1)$ with diametral "end-points"

$$x^{\pm}_{a,b,c} = \frac{-b \pm d^{1/2}}{2a}, \ (a,b,c) \in \mathcal{R}_\Delta(d).$$

$$d = -418916$$



$$d = 2308$$



Duke's Theorems

Analogous equidistribution results hold for *any* integral valued ternary quadratic form q.

Theorem (Duke–Schulze-Pillot)

As $d \to \infty$ such that d is everywhere locally representable by q, $(d, \mathrm{disc}(q)) = 1$, the squarefree part of d avoid a finite set of integers depending on q, the set $|d|^{-1/2}\mathcal{R}_q(d)$ is non-empty and equidistribute on $V_{q,\pm 1}(\mathbb{R})$.

Remark

This solved Hilbert's 11th problem over $\mathbb{Q}$ in the (remaining) case of definite ternary forms : for these the set of genus classes (global isometry classes of forms locally isometric to q) is of size > 1 as soon as $\mathrm{disc}(q) \gg 1$.

Duke's Theorems : proofs

The proofs use the dual formulation. Goal : show that the Weyl sums attached to (non-characters) automorphic forms satisfy :

$$\frac{1}{\mathrm{vol}(d)} \sum_{[a,b,c]} \int_{\mathrm{G}_{\mathbf{x}}(\mathbb{R})} \varphi(g_{(a,b,c)}.t)\, dt \to 0, \;\; d \to \infty,$$

$$\mathrm{vol}(d) = \sum_{[a,b,c]} \int_{\mathrm{G}_{\mathbf{x}}(\mathbb{R})} dt.$$

In Duke's original proof, the Weyl sums are shown to be related to the Fourier coefficients of metaplectic forms (theta series) which have to be bounded non-trivially.
Such bounds were obtained by Iwaniec in the definite case and by Duke in the indefinite case.

Waldspurger's formula & subconvexity

A different and more powerful proof comes from Waldspurger's formula. For this is it useful to first adelize the problem (Clozel-Ullmo) :

- $\exists$ a quat. algebra B, s.t. $(\mathbb{Q}^3, q) \sim (\mathrm{B}^0, \lambda\,\mathrm{Nr}_{\mathrm{B}})$; wlogwma
$$\mathrm{G} = \mathrm{PB} = Z_{\mathrm{B}}^{\times}\backslash \mathrm{B}^{\times}.$$
- Equidistribution takes place on an adelic quotient
$$[\mathrm{G}]/K_f,\ [\mathrm{G}] := \mathrm{G}(\mathbb{Q})\backslash \mathrm{G}(\mathbb{A}),\ K_f \subset \mathrm{G}(\mathbb{A}_f).$$
- The set of orbits$^{(\star)}$ $\bigsqcup_{[a,b,c]} \mathrm{G}(\mathbb{Z})\backslash \mathrm{G}(\mathbb{Z}).g_{(a,b,c)}\mathrm{G}_{\mathbf{x}}(\mathbb{R})$ correspond to the projection to $[\mathrm{G}]/K_f$ of an adelic orbit
$$[\mathrm{T}.g] = \mathrm{T}(\mathrm{PB})\backslash \mathrm{T}(\mathbb{A}).g \subset [\mathrm{G}],\ \mathrm{g} = \mathrm{g}_{\infty}.\mathrm{g}_{\mathrm{f}} \in \mathrm{G}(\mathbb{A}).$$
$$\mathrm{T} = \mathrm{G}_{(a,b,c)} \simeq \mathrm{res}_{K/\mathbb{Q}}\mathbb{G}_m/\mathbb{G}_m,\ K = \mathbb{Q}(\sqrt{-d/\lambda}).$$

Waldspurger's formula & subconvexity

Let B/F, $\mathrm{G} = \mathrm{PB}$, $\mathrm{T} = \mathrm{G}_{\mathbf{x}}$, $\mathbf{x} \in \mathrm{B}^0$, $-\mathrm{Nr}_{\mathrm{B}}(\mathbf{x}) = d = x^2 \notin F^2$, $K = F(x)$.

Theorem (Waldspurger)

Let $\varphi : [\mathrm{G}] \to \mathbb{C}$ is an (factorable) automorphic form which is not a character, $\pi = \langle \mathrm{G}(\mathbb{A}).\varphi \rangle \in \mathrm{Aut}(\mathrm{G})$ the autorep it generates, $\pi^{JL} \in \mathrm{Aut}(\mathrm{PGL}_2)$ the Jacquet-Langlands correspondant and π_K^{JL} its base change to $\mathrm{PGL}_{2,K}$, one has

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

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

Waldspurger's formula & subconvexity

To the adelic torus orbit $[\mathrm{T}.g] = \mathrm{T}(F)\backslash\mathrm{T}(\mathbb{A}).g$ is associated a *discriminant* (related to the volume of the intersection of $\mathrm{T}(\mathbb{A}).g$ with a fixed compact of $\mathrm{G}(\mathbb{A})$).

$$D_{[\mathrm{T}.g]} = \prod_v D_{\mathrm{T}(F_v).g_v} > 0.$$

Theorem (Einsiedler-Lindenstrauss-M-Venkatesh)

$\exists \eta > 0$ *absolute s.t.*

$$\frac{\int_{[\mathrm{T}]} \varphi(tg)\,dt}{\langle \varphi, \varphi \rangle^{1/2}} \ll_{F,\varphi} D_{[\mathrm{T}.g]}^{-\eta}$$

Waldspurger's formula & subconvexity

The proof consists in bounding the righthand side in Waldspurger's formula

1. The local integrals $\int_{\mathrm{T}(\mathbb{Q}_v)} \langle g_v.\varphi_v, t_v.g_v.\varphi_v \rangle dt_v$ are bounded using the *decay of matrix coefficients* (as t_v varies).
2. The global L-function is bounded using *subconvex bounds* (due to DFI for $\mathbb{Q}$ and Venkatesh for F)

$$L(\pi_K^{JL}, 1/2) = L(\pi^{JL}, 1/2)L(\pi^{JL}.\chi_K, 1/2) \ll_\pi \mathrm{Nr}_{F/\mathbb{Q}}(d_K)^{1/2-\eta}.$$

This bound essentially resolves Duke's theorem in general.

Waldspurger's formula & subconvexity

To conclude it remains to deal with the case of characters :

$$\varphi = \chi_{\mathrm{B}} : g \in \mathrm{B}^{\times}(\mathbb{A}) \mapsto \chi(\mathrm{Nr}_{\mathrm{B}}(g)),\ \chi^2 = 1,\ \chi \neq 1.$$

In that case, the period is easy to compute : let K_χ be the quadratic field whose χ is the "Legendre symbol"

$$\int_{[\mathrm{T}]} \chi(\mathrm{Nr}(tg))dt = \chi(\mathrm{Nr}(g)) \int_{[\mathrm{T}]} \chi(\mathrm{Nr}(t))dt = \begin{cases} \chi(\mathrm{Nr}(g)) & \text{if } K = K_\chi \\ 0 & \text{if } K \neq K_\chi \end{cases}.$$

Therefore Duke's theorem hold for the quotient

$$\mathrm{G}(F)\backslash \mathrm{G}(\mathbb{A})/K_f$$

($K_f \subset \mathrm{G}(\mathbb{A}_f)$ open compact) as long as the quadratic fields K involved are not amongst the finite set of quadratic fields K_χ such that χ_{B} is K_f-invariant.

Waldspurger's formula & subconvexity

The two approaches toward Duke's theorem (via Fourier coefficients of theta series or via L-functions) are connected via another formula of Waldspurger.
However the L-function approach has advantages : the realization of the set of (classes of) representations as a torus orbit $[\mathrm{T}.g]$ provides it with a group-like (torsor) structure : that was already identified by Gauss for the discriminant and sums of three squares in the *Disquisitiones*).

- This allows to refine Duke's theorem by restricting the average along $[\mathrm{T}]$ via harmonic analysis : for any Hecke character $\chi_{\mathrm{T}} : [\mathrm{T}] \to \mathbb{C}^{\times}$, Waldspurger established the more general formula relating the twisted period $|\int_{[\mathrm{T}]} \varphi(tg)\chi_{\mathrm{T}}(t)\,dt|^2$ to $L(\pi_K^{JL}.\chi_{\mathrm{T}}, 1/2)$ and a product of twisted local integrals and non-trivial bounds for these are known (M, M-V).

Fast backwards : Linnik's ergodic method

This torsor structure was exploited by Linnik and later Skubenko in the 50/60's to prove Duke's theorems under an additional congruence on d

Theorem (Linnik, Skubenko)

For $q = E_3$ or Δ, the set $|d|^{-1/2}\mathcal{R}_q(d)$ equidsitributes on $V_{q,\pm 1}(\mathbb{R})$ for $d \to \infty$ satisfying the previous conditions as in addition

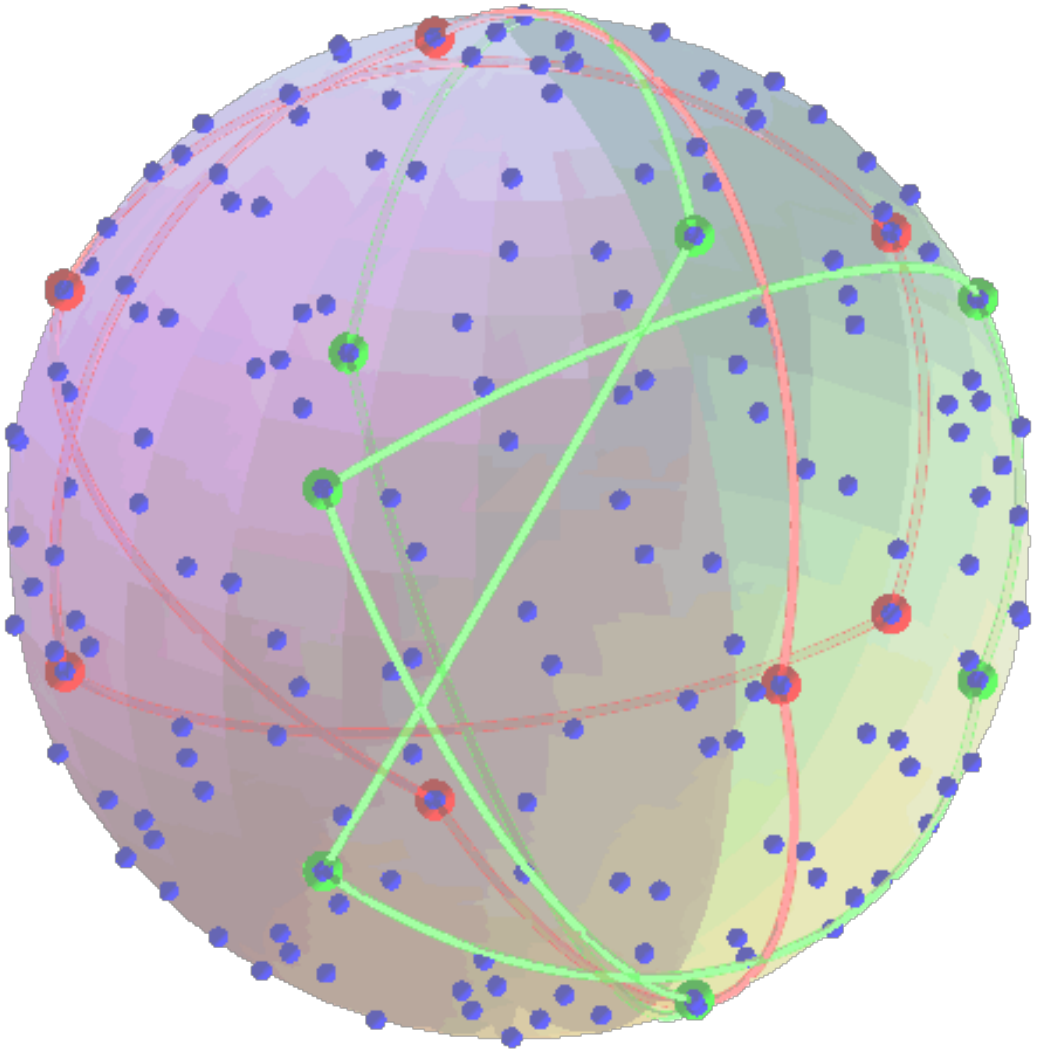
$$5 \text{ split in } \mathbb{Q}(\sqrt{d})$$

Fast backwards : Linnik's ergodic method

The proof of this theorem is via what Linnik's *ergodic method*. Here is a modern reformulation (ELMV)

1. The splitting condition at 5 implies that for any d, $\mathrm{T}_d(\mathbb{Q}_5) \subset \mathrm{G}(\mathbb{Q}_5)$ contains an element conjugate to the matrix (necessarily $\mathrm{B}(\mathbb{Q}_5) \simeq M_2(\mathbb{Q}_5)$) $t_5 := \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}$
2. The sequence of torus orbits $[\mathrm{T}_d.g_d]$ furnishes a sequence of probability measures on $[\mathrm{G}]$ invariant under the action of the group $t_5^{\mathbb{Z}}$. In particular any weak-$\star$ limit of such sequence has this invariance.
3. The *basic lemma* (of Linnik) (a soft form of a case of the Siegel mass formula) implies that the entropy of the t_5-action for any weak limits is maximal.
4. Maximality of entropy $\Longrightarrow$ any weak-$\star$ limit is the Haar measure.

Orbit for the 5-flow



Fast forward : Duke's theorem for products

The group structure allow for further refinements of Duke's theorem.

- We consider a uple of (distinct) quaternion algebras B_i, $i = 1, \cdots, s$ with associated projective groups G_i ; a uple of open-cpt subgroups $K_{f,i} \subset \mathrm{G}_i(\mathbb{A}_f)$. Set

$$\mathbf{G} = \prod_{i=1}^{s} \mathrm{G}_i, \ \mathbf{K}_f = \prod_{i=1}^{s} K_{f,i} \subset \mathbf{G}(\mathbb{A}_f)$$

Fast forward : Duke's theorem for products

- Given a torus $\mathrm{T} \simeq \mathrm{res}_{K/\mathbb{Q}}\mathbb{G}_m/\mathbb{G}_m$, $K = \mathbb{Q}(\sqrt{d})$ with a uple of embeddings

$$\iota_i : \mathrm{T} \hookrightarrow \mathrm{G}_i$$

(take $z_i \in \mathrm{B}_i^0$ s.t. $z_i^2 = d$), which yields a diagonal embedding

$$\iota : t \in \mathrm{T} \hookrightarrow \iota(t) = (\iota_i(t))_{i \leq s} \in \mathbf{T} \subset \mathbf{G}.$$

- The data of a uple $\mathbf{g} = (g_i)_{i \leq s} \in \mathbf{G}(\mathbb{A})$ define an adelic torus orbit $[\mathbf{T}.\mathbf{g}] \subset [\mathbf{G}]$ whose discriminant is defined as $D_{\mathbf{T}.\mathbf{g}} := \min_{i \leq s} D_{\mathrm{T}_i.g_i}$.

Conjecture

As $D_{\mathbf{T}.\mathbf{g}} \to \infty$ the torus orbit $[\mathbf{T}.\mathbf{g}]$ becomes e.d. on $[\mathbf{G}]/\mathbf{K}_f$ for the subspace of functions $\perp$ to the $\mathbf{K}_f$-invariant characters.

Joinings

Theorem (Einsiedler-Lindenstrauss)

Let $v_1 \neq v_2$ be fixed places of $\mathbb{Q}$. The conjecture is true for tori T whose associated quadratic field K splits at v_1, v_2.

- The condition that K splits at v_1, v_2 is similar to Linnik condition in the ergodic method but one needs two places here.
- Duke's theorem for one factor is used as a fuel for the general theorem (in fact as one has already two split places, one could use Linnik's theorem instead).

Joinings

Theorem (Einsiedler-Lindenstrauss)

Let $v_1 \neq v_2$ be fixed places of $\mathbb{Q}$. The conjecture is true for tori T whose associated quadratic field K splits at v_1, v_2.

- Blomer and Brumley have recently obtained a proof for two factors ($s = 2$) without any splitting condition but under several GRHs.
- This is very special case of a much more general theorem classifying *joinings* on products of locally homogeneous spaces invariant under *two* commuting actions (these are *algebraic* measures). In particular the general theorem provides important (but not sufficient) information if some B_i are the same (cf. the work of I. Khayutin).

Characters

To deal with the case of characters, one introduce the following groups

$$\Xi_i(K_{f,i}) = \{\chi_i,\ \chi_i^2 = 1, \chi_i \circ \mathrm{Nr}_{i|K_{f,i}} \equiv 1\}$$

$$\Xi(\mathbf{K}_f) = \prod_i \Xi_i(K_{f,i}).$$

Let Π denote the product map

$$\Pi : (\chi_i)_{i \leq s} \in \Xi(\mathbf{K}_f) \mapsto \prod_i \chi_i$$

Proposition

Under the previous assumptions, if $\ker(\Pi)$ *is trivial, equidistribution holds for tori* T *whose quadratic field* K *is not associated to any quadratic character in the image* $\Pi(\Xi(\mathbf{K}_f))$.

Duke's theorem for products : applications

The first application of the EL Theorem was given by Aka-Einsiedler-Shapira. Here is a simplified version :
Let $(a,b,c) \in \mathcal{R}_{E_3}(d)$ be a primitive representation ; the intersection

$$(a,b,c)^{\perp} \cap \mathbb{Z}^3$$

is a lattice in the $\mathbb{R}$-space $(a,b,c)^{\perp}$ of covolume $|d|^{1/2}$. To this lattice, one can associate a (well defined) $\mathbb{C}^{\times}$-homothety class of lattices $[\Lambda(a,b,c)] = [\mathbb{Z} + \mathbb{Z}.z(a,b,c)]$ in $\mathbb{C}$ and therefore a class on the modular surface

$$[z(a,b,c)] \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} = \mathrm{PGL}_2(\mathbb{Z})\backslash \mathrm{PGL}_2(\mathbb{R})/\mathrm{PSO}_2(\mathbb{R}),$$

$$z(a,b,c) = z_{(a',b',c')},\ (a',b',c') \in \mathcal{R}_{\Delta}(d) \text{ or } \mathcal{R}_{\Delta}(4d).$$

Duke's theorem for products : applications

Theorem (AES)

Let q_1, q_2 be two odd primes. For $d \to \infty$, satisfying the assumption of the first of Duke's Theorems (for S^2) and such that q_1, q_2 split in $\mathbb{Q}(\sqrt{d})$ the set of pairs

$$\{(|d|^{-1/2}(a,b,c), [z(a,b,c)]),\ (a,b,c) \in \mathcal{R}_{E_3}(d)\}$$

is equidistributed on $S^2 \times X_0(1)$.

The proof is an application of the EL theorem with

$$\mathrm{B}_1 = \mathrm{B}_{2,\infty},\ \mathrm{B}_2 = M_2,\ K_{f,1} = \mathrm{P}\widehat{\mathcal{O}}_{2,\infty}^{\times},\ K_{f,2} = \mathrm{PGL}_2(\widehat{\mathbb{Z}}).$$

The only character is the trivial one.

Reduction of CM elliptic curves

An elliptic curve $E/\mathbb{C}$ has CM if $\mathrm{End}(\Lambda) = \mathcal{O} \subset K \subset \mathbb{C}$. If $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ this is equivalent to

$$\mathrm{End}(\Lambda) = \{z \in \mathbb{C},\ z.\Lambda \subset \Lambda\} = \mathcal{O}.$$

$$\mathcal{E}\ell\ell_{\mathcal{O}} = \{\text{Elliptic curves with CM by } \mathcal{O}\}/\sim .$$

- $\mathcal{E}\ell\ell_{\mathcal{O}}$ is a torsor under the action of $\mathrm{Pic}(\mathcal{O})$:

$$\text{for } E \simeq \mathbb{C}/\Lambda,\ \mathfrak{a} \star E \simeq \mathbb{C}/\mathfrak{a}^{-1}\Lambda.$$

- Set $d = \mathrm{disc}(\mathcal{O})$, the map $z \in \mathbb{H} \mapsto \Lambda_z = \mathbb{Z} + \mathbb{Z}.z \mapsto \mathbb{C}/\Lambda_z$ induce

$$\mathcal{E}\ell\ell_{\mathcal{O}} \simeq \{z_{[a,b,c]},\ (a,b,c) \in \mathcal{R}^{\star}_{\Delta}(d)\} \subset X_0(1).$$

So by Duke's second theorem, elliptic curves with CM by $\mathcal{O}$ become ed. on the moduli space of elliptic curves/$\mathbb{C}$ as $\mathrm{disc}(\mathcal{O}) \to \infty$.

Reduction of CM elliptic curves

- A CM elliptic curve is defined of a number field $H_{\mathcal{O}} = K(j(E))$.
- A CM elliptic curve has (potential) good reduction at every prime.
- If p is inert in K and $\mathfrak{p}$ is a place in $\overline{\mathbb{Q}}$ above p, $E \pmod{\mathfrak{p}}$ is a *supersingular* elliptic curve :

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

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

We have a reduction modulo p map

$$\mathrm{red}_p : E \in \mathcal{E}\ell\ell_{\mathcal{O}} \mapsto E \pmod{\mathfrak{p}} \in \mathcal{E}\ell\ell_p^{ss}$$

inducing an embedding

$$\iota_p : \mathrm{End}(E) \simeq \mathcal{O} \hookrightarrow \mathrm{End}(E \pmod{\mathfrak{p}}) \simeq \mathcal{O}_{p,\infty}.$$

Reduction of CM elliptic curves

The finite space $\mathcal{E}\ell\ell_p^{ss}$ is identified with an adelic quotient

$$\mathcal{E}\ell\ell_p^{ss} \simeq \mathrm{G}(\mathbb{Q})\backslash\mathrm{G}(\mathbb{A})/\mathrm{G}(\mathbb{R})\mathrm{P}\widehat{\mathcal{O}}_{p,\infty}^{\times},\ \mathrm{G} = \mathrm{PB}_{p,\infty}$$

and the embedding ι_p induces and embedding $\iota_p : \mathrm{T} \hookrightarrow \mathrm{G}$. Under the above identification the image $\mathrm{red}_p(\mathcal{E}\ell\ell_{\mathcal{O}})$ identifies (as a multiset) with the projection of the orbit $[\iota_p(\mathrm{T})]$. Duke's theorem implies

Theorem (M)

As $d \to \infty$ (such that $(d,p) = 1$ and p is inert in K) the map red_p is surjective and $\mathrm{red}_p(\mathcal{E}\ell\ell_{\mathcal{O}})$ (as a multiset) becomes ed. wrt a probability measure μ_p such that $\mu_p(\overline{E}) \approx 1/|\mathrm{End}(\overline{E})^{\times}|$.

Reduction of CM elliptic curves

We can now fix a tuple of primes $p_1, \cdots, p_s$ and for $\mathcal{O}$ such that all the p_i remain inert in K we have a multireduction map

$$\mathrm{red} : E \in \mathcal{E}\ell\ell_{\mathcal{O}} \mapsto (z_E, \mathrm{red}_{p_1}(E), \cdots, \mathrm{red}_{p_s}(E)) \in X_0(1) \times \prod_i \mathcal{E}\ell\ell_{p_i}^{ss}$$

Theorem (ALMW)

Let q_1, q_2 be two primes $\neq p_i$. As $d \to \infty$ – such that $(d, p_i) = 1$, p_i is inert in K for every i, and q_1, q_2 split in K – the set $\mathrm{red}(\mathcal{E}\ell\ell_{\mathcal{O}})$ becomes ed. wrt probability measure $\mu_\infty \otimes \bigotimes_i \mu_{p_i}$.

Reduction of CM elliptic curves

- The proof is an application of the EL theorem for

$$\mathbf{G} = \mathrm{PGL}_2 \times \prod_i \mathrm{G}_{p_i}, \ \mathbf{K}_f = \mathrm{PGL}_2(\widehat{\mathbb{Z}}) \times \prod_i \mathrm{P}\widehat{\mathcal{O}}^{\times}_{p_i,\infty}$$

  with the diagonal embedding for T

$$\iota = (\mathrm{Id}, \iota_{p_1}, \cdots, \iota_{p_s}).$$

- The open compact $\mathbf{K}_f$ is big : this implies that the only character is the trivial one.
- A non obvious point is to verify is that the image $\mathrm{red}(\mathcal{E}\ell\ell_{\mathcal{O}})$ is represented by a diagonal torus orbit $[\iota(\mathrm{T})\mathbf{g}]$. This is a consequence of Serre's "$\mathfrak{a}$-transform", an algebraic version of the $\mathrm{Pic}(\mathcal{O})$-action on complex CM elliptic curves

$$\mathfrak{a} \star \mathbb{C}/\Lambda = \mathbb{C}/\mathfrak{a}^{-1}\Lambda.$$

  This implies that for $\mathfrak{a} \subset \mathcal{O}$

$$(\mathfrak{a} \star E) \,(\mathrm{mod}\, \mathfrak{p}) = \iota_p(\mathfrak{a}) \star (E \,(\mathrm{mod}\, \mathfrak{p})).$$

Reduction of CM elliptic curves : future directions

- Recently, Herrero, Menares and Rivera-Letellier have obtained much more precise version for the equidistribution of the reductions modulo p.
  The set $\mathcal{E}\ell\ell_p^{ss}$ is the indexing set of a disjoint union of p-adic disks of radius 1 ; each disk parametrize the deformations of the (canonical lift of the) formal group of each supersingular curve $\overline{E}$.
  Each CM curve E provide such deformation for $E \pmod{\mathfrak{p}}$ and therefore a point on the corresponding disk. Using the theta series approach, HMR-L have established the equidistribution of the CM points on these disks wrt to a certain probability measure.
  We expect to joint forces to extend this result to several primes simultaneously.

Reduction of CM elliptic curves : future directions

- For his work on Mazur's conjectures, Cornut has proven the equidistribution theorem for simultaneous reductions for elliptic curves with CM by orders

$$\mathcal{O}_{q^k} = \mathbb{Z} + q^k \mathcal{O}_K$$

for K a *fixed* quadratic field, q a *fixed* prime and $k \to \infty$. The proof use Ratner's theory of joinings for unipotent actions. The EL theorem allows to obtain results analogous to those of Vatsal, Cornut and Cornut-Vatsal for orders $\mathcal{O}_{q^k} = \mathbb{Z} + q^k \mathcal{O}_K$ when K is *fixed*, k is *fixed* and $q \to \infty$ and to derivate arithmetic consequences along the lines of C-V (in progress with D. Ramakrishnan).

THANK YOU!