Generalizaciones de la conjetura de Sato–Tate

Francesc Fité (MIT)

Seminario Latinoamericano de Teoría de Números

24/6/2021

Trazas de Frobenius para curvas elípticas

k un cuerpo de números.

E/k una curva elíptica, es decir, una curva dada por

$$y^2 = x^3 + ax + b\,, \qquad \text{donde } a, b \in k,\ 4a^3 + 27b^2 \neq 0.$$

Para $\mathfrak{p}$ un primo de buena reducción de E, denotemos

$$a_{\mathfrak{p}} := q + 1 - \#E(\mathbb{F}_q)\,, \qquad \text{donde } q = \mathrm{Nm}(\mathfrak{p}).$$

La traza de Frobenius $a_{\mathfrak{p}}$ determina la función Zeta de E

$$Z(E_{\mathfrak{p}}, T) := \exp\left(\sum_{n\geq 1} \#E(\mathbb{F}_{q^n})\frac{T^n}{n}\right) = \frac{1 - a_{\mathfrak{p}}T + qT^2}{(1-T)(1-qT)}\,.$$

Una pregunta abierta

Por la cota de Hasse-Weil tenemos:

$$\overline{a}_{\mathfrak{p}} := \frac{a_{\mathfrak{p}}}{q^{1/2}} \in [-2, 2]\,.$$

Consideremos la secuencia $\{\overline{a}_{\mathfrak{p}}\}_{\mathfrak{p}}$.

Cuál es la distribución de $\{\overline{a}_{\mathfrak{p}}\}_{\mathfrak{p}}$ sobre el intervalo $[-2, 2]$?

La respuesta (conjetural) depende de $\mathcal{A} = \mathrm{End}(E_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$:

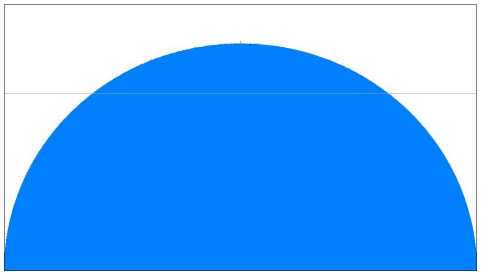
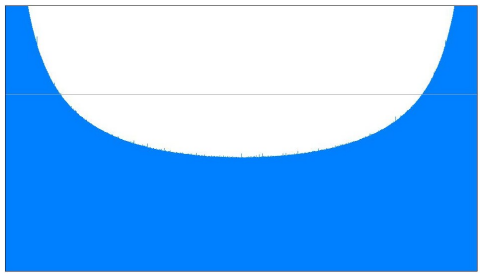
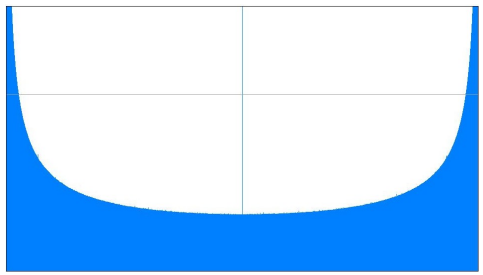
1) $\mathcal{A} \simeq \mathbb{Q}$.
2) $\mathcal{A}$ es un cuerpo cuadrático imaginario contenido en k.
3) $\mathcal{A}$ es un cuerpo cuadrático imaginario *no* contenido en k.

La conjetura de Sato–Tate para curvas elípticas

Conjetura de Sato–Tate

$\{\overline{a}_{\mathfrak{p}}\}_{\mathfrak{p}}$ se distribuye sobre $[-2,2]$ con respecto a las medidas

1) $\frac{1}{2\pi}\sqrt{4-z^2}\,dz$ 2) $\frac{1}{\pi}\frac{dz}{\sqrt{4-z^2}}$ 3) $\frac{1}{2}\delta_0+\frac{1}{2\pi}\frac{dz}{\sqrt{4-z^2}}$

(según los casos de la transparencia anterior).

Observación

Demostrada en los casos 2), 3), y en 1) cuando k es un cuerpo TR o CM.

Pregunta

En el caso 1), sea δ_- la densidad de $\{\mathfrak{p} : a_{\mathfrak{p}} < 0\}$.
Cuál es la mejor cota inferior conocida para δ_- para k arbitrario?

El grupo de Sato–Tate de una curva elíptica

Las medidas de la transparencia anterior 'provienen' de subgrupos de $\mathrm{SU}(2)$. Estos subgrupos son:

1) $\mathrm{SU}(2) := \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C}) \,:\, a\overline{a} + b\overline{b} = 1 \right\}$.

2) $\mathrm{U}(1) := \left\{ \begin{pmatrix} u & 0 \\ 0 & \overline{u} \end{pmatrix} : u \in \mathbb{C},\, |u| = 1 \right\}$.

3) $N_{\mathrm{SU}(2)}(\mathrm{U}(1)) := \left\langle \mathrm{U}(1), \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$.

Para un G como en 1), 2), 3), tenemos $\mathrm{Tr} : G \to [-2, 2]$.

La medida de la conjetura se puede describir como

$$\mathrm{Tr}_*(\mu_G)\,,$$

donde μ_G es la medida de Haar de G.

Reformulación de la conjectura

Definimos el grupo de Sato–Tate de E como $\mathrm{ST}(E) = \mathrm{SU}(2)$, $\mathrm{U}(1)$, o $N_{\mathrm{SU}(2)}(\mathrm{U}(1))$ según los casos vistos.

Denotemos

$$\overline{L}_{\mathfrak{p}}(E, T) := L_{\mathfrak{p}}(E, q^{-1/2}T) = 1 - \overline{a}_{\mathfrak{p}}T + T^2 .$$

Conjetura de Sato–Tate

Existe una factorización

$$\{\text{primos de } k\} \to \mathrm{Conj}(\mathrm{ST}(E)) \twoheadrightarrow \mathrm{CharPolys}(\mathrm{ST}(\mathrm{E})) , \quad \mathfrak{p} \mapsto x_{\mathfrak{p}} \mapsto \overline{L}_{\mathfrak{p}}(E, T)$$

tal que la secuencia $\{x_{\mathfrak{p}}\}_{\mathfrak{p}}$ se distribuye sobre el espacio $\mathrm{Conj}(\mathrm{ST}(E))$ con respecto a la medida de Haar de $\mathrm{ST}(E)$.

Estrategia para la demostración

La construcción de $x_{\mathfrak{p}}$ no es complicada.

Asociada a una representación irreducible ϱ de $\mathrm{ST}(E)$, se define

$$L(E, \varrho, s) := \prod_{\mathfrak{p}} \det(1 - \varrho(x_{\mathfrak{p}}) \,\mathrm{Nm}(\mathfrak{p})^{-s})^{-1} \qquad \text{para } \Re(s) > 1.$$

Ejemplo

Si $\mathrm{ST}(E) = \mathrm{SU}(2)$, entonces las irreps de $\mathrm{ST}(E)$ son $\mathrm{Sym}^m(\mathbb{C}^2)$.

Teorema (Serre)

Si para toda ϱ no trivial, $L(E, \varrho, s)$ se extiende a (un entorno de) $\Re(s) \geq 1$ y no se anula sobre $\Re(s) = 1$, entonces se tiene la equidistribución de $\{x_{\mathfrak{p}}\}_{\mathfrak{p}}$.

Observación

Típicamente, la no anulación de $L(E, \varrho, s)$ se deduce demostrando su automorfía potencial.

El grupo de Sato–Tate de una variedad abeliana

Sea A/k una variedad abeliana de dimensión $g \geq 1$.

Para un primo ℓ, definimos

$$T_\ell(A) = \varprojlim_r A[\ell^r](\overline{\mathbb{Q}}), \qquad V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell .$$

Consideremos la representación ℓ-ádica asociada a A

$$\varrho_\ell \colon G_k \to \mathrm{Aut}(V_\ell(A)) .$$

Denotemos por $\mathcal{G}_\ell \subseteq \mathrm{GSp}_{2g}/\mathbb{Q}_\ell$ la clausura de Zariski de la imagen de ϱ_ℓ.

Denotemos por $\mathcal{G}_\ell^0 \subseteq \mathrm{GSp}_{2g}/\mathbb{Q}_\ell$ la componente conexa de $\mathcal{G}_\ell$.

Tenemos una inyección

$$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{\mathcal{G}_\ell^0}(V_\ell(A))$$

(un isomorfismo por un teorema de Faltings).

La inclusión anterior se puede reinterpretar como

$$\mathcal{G}_\ell^0 \hookrightarrow \{\gamma \in \mathrm{GSp}_{2g}/\mathbb{Q}_\ell \,|\, \gamma\alpha\gamma^{-1} = \alpha \text{ para todo } \alpha \in \mathrm{End}(A_{\overline{\mathbb{Q}}})\}\,.$$

De hecho, tenemos

$$\mathcal{G}_\ell \hookrightarrow \bigcup_{\sigma \in G_k} \{\gamma \in \mathrm{GSp}_{2g}/\mathbb{Q}_\ell \,|\, \gamma\alpha\gamma^{-1} = \sigma(\alpha) \text{ para todo } \alpha \in \mathrm{End}(A_{\overline{\mathbb{Q}}})\}\,.$$

Edificando sobre el trabajo de muchos, Banaszak y Kedlaya muestran que si $g \leq 3$, entonces la inyección anterior es una igualdad. Independencia de ℓ!

De ahora en adelante, supondremos $g \leq 3$.

Definimos el grupo twistado de Lefschetz de A como

$$\mathrm{TL}(A) := \bigcup_{\sigma \in G_k} \{\gamma \in \mathrm{Sp}_{2g}/\mathbb{Q} \,|\, \gamma\alpha\gamma^{-1} = \sigma(\alpha) \text{ para todo } \alpha \in \mathrm{End}(A_{\overline{\mathbb{Q}}})\}\,.$$

Definimos $\mathrm{ST}(A)$ como un subgrupo maximal compacto de $\mathrm{TL}(A)(\mathbb{C})$.

Es un subgrupo de $\mathrm{USp}(2g)$, no necesariamente conexo, sensible a cambio de base, y sólo bien definido *salvo conjugación*.

Conjetura de Sato–Tate en dimensión ≤ 3

Sea $\mathfrak{p}$ un primo de buena reducción para A. Definamos

$$L_{\mathfrak{p}}(A,T) = \det(1 - \varrho_\ell(\mathrm{Frob}_{\mathfrak{p}})T \,|\, V_\ell(A))\,, \qquad \overline{L}_{\mathfrak{p}}(A,T) = L_{\mathfrak{p}}(A, T/q^{1/2})\,.$$

Junto con $\mathrm{ST}(A)$, se pueden definir $x_{\mathfrak{p}} \in \mathrm{Conj}(\mathrm{ST}(A))$ tales que

$$\mathrm{Charpoly}(x_{\mathfrak{p}}) = \overline{L}_{\mathfrak{p}}(A,T)\,.$$

En general, la aplicación

$$\mathrm{Conj}(\mathrm{ST}(A)) \twoheadrightarrow \mathrm{Charpolys}(\mathrm{ST}(A))\,, \qquad x \mapsto \mathrm{Charpoly}(x)$$

no es inyectiva.

Conjetura de Sato–Tate para variedades abelianas (Serre)

La secuencia $\{x_{\mathfrak{p}}\}_{\mathfrak{p}}$ se distribuye sobre el espacio $\mathrm{Conj}(\mathrm{ST}(A))$ con respecto a la medida de Haar de $\mathrm{ST}(A)$.

Axiomas de Sato–Tate

En dimensión $g \leq 3$, $\mathrm{ST}(A)$ satisface las siguientes propiedades:

Condición de Hodge (ST1).
$\mathrm{ST}(A)^0$ contiene algún círculo de Hodge y está topológicamente generado por ellos (un círculo de Hodge es la imagen de un homomorfismo $\theta\colon \mathrm{U}(1) \to \mathrm{ST}(A)^0$ tal que $\theta(u)$ tiene autovalores u, u^{-1} con multiplicidad g).

Condición de racionalidad (ST2).
El valor esperado $\int_H \chi\mu$ de un carácter χ sobre una componente conexa cualquiera $H \subseteq \mathrm{ST}(A)$ es un entero (con $\mu(H) = 1$).

Condición de Lefschetz (ST3).
El subgrupo de $\mathrm{USp}(2g)$ que fija $(\mathbb{C}^{2g})^{\mathrm{ST}(A)^0}$ es $\mathrm{ST}(A)^0$.

Condición de Serre (ST4).
Sea F_A/k la mínima extensión F/k sobre la que $\mathrm{End}(A_F) \simeq \mathrm{End}(A_{\overline{\mathbb{Q}}})$.
Entonces

$$\mathrm{ST}(A)/\mathrm{ST}(A)^0 \simeq \mathrm{Gal}(F_A/k)\,.$$

Grupos de Sato–Tate en dimensión ≤ 2

Observaciones

Ni (ST3) ni (ST4) permanecen ciertos para $g \geq 4$.

Salvo conjugación en $\mathrm{USp}(2) = \mathrm{SU}(2)$, 3 grupos satisfacen los axiomas de ST.

Teorema 1 (F.-Kedlaya-Rotger-Sutherland; 2012)

- Salvo conjugación en $\mathrm{USp}(4)$, existen 52 grupos de Sato–Tate para superficies abelianas definidas sobre cuerpos de números.
- Los 11 grupos maximales (con respecto a inclusiones finitas) ocurren como grupos de Sato–Tate de superficies abelianas sobre $\mathbb{Q}$.
- Para una superficie abeliana A/k, el grado $[F_A : k]$ divide 48.

Observación

El tercer punto refina un resultado anterior de Silverberg.

Puntos adicionales

- Los 52 grupos ocurren como grupos de Sato–Tate de Jacobianas de curvas de género 2 definidas sobre un cuerpo de números (FKRS).
- Sólo 34 ocurren como grupos de Sato-Tate de surperficies sobre $\mathbb{Q}$ (FKRS).
- Existe un cuerpo de números k_0 sobre el que los 52 grupos aparecen como grupo de ST de alguna superficie abeliana definida sobre k_0 (F.-Guitart).
- Para $k = \mathbb{Q}$, la equidistribución es conocida salvo cuando $\mathrm{ST}(A) = \mathrm{USp}(4)$ (Johansson–N.Taylor).
- Para visualizar las 52 distribuciones, visitar:

  https://math.mit.edu/ drew/st2/g2SatoTateDistributions.html

Tipo de endomorfismos

Definimos el tipo de endomorfismos de una variedad abeliana A/k como la clase de isomorfismo de la $\mathbb{R}$-álgebra

$$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{R} \quad \text{equipada con una acción de } \mathrm{Gal}(F_A/k).$$

Ejemplo

Hay tres tipos de endomorfismos para curvas elípticas.

Son $\mathbb{R}$, $\mathbb{C}$ (ambos equipados con la acción del grupo trivial), y $\mathbb{C}$ equipado con la acción de la conjugación compleja.

Teorema (FKRS)

- Hay 52 tipos de endomorfismos para superficies abelianas sobre cuerpos de números.
- El grupo de Sato–Tate y el tipo de endomorfismos de una superficie abeliana se determinan mutuamente de forma unívoca.

Comentarios sobre la clasificación para $g = 2$

(ST1) permite 6 opciones para $G^0 \subseteq \mathrm{USp}(4)$ ((ST3) es redundante para $g = 2$).

G^0	$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$	$N_{\mathrm{USp}(4)}(G^0)/G^0$	$\#\mathcal{A}$
$\mathrm{USp}(4)$	$\mathbb{R}$	C_1	1
$\mathrm{SU}(2) \times \mathrm{SU}(2)$	$\mathbb{R} \times \mathbb{R}$	C_2	2
$\mathrm{SU}(2) \times \mathrm{U}(1)$	$\mathbb{R} \times \mathbb{C}$	C_2	2
$\mathrm{U}(1) \times \mathrm{U}(1)$	$\mathbb{C} \times \mathbb{C}$	D_4	8
$\mathrm{SU}(2)_2$	$\mathrm{M}_2(\mathbb{R})$	$\mathrm{O}(2)$	10
$\mathrm{U}(1)_2$	$\mathrm{M}_2(\mathbb{C})$	$\mathrm{SO}(3) \times C_2$	32
			55

- $\mathcal{A} = \{$subgrupos finitos de $N_{\mathrm{USp}(4)}(G^0)/G^0$ para los que (ST2) se cumple$\}$.
- 3 de los grupos en el caso $G^0 = \mathrm{U}(1) \times \mathrm{U}(1)$ no satisfacen (ST4):
  - A es $\overline{\mathbb{Q}}$-isógena a un producto de variedades abelianas A_i con CM por M_i.
  - $G/G^0 \simeq \mathrm{Gal}(F_A/k) \simeq \prod \mathrm{Gal}(kM_i^*/k) \subseteq C_2 \times C_2, C_4$.

Grupos de Sato–Tate en dimensión $g = 3$

Teorema 2 (F.-Kedlaya-Sutherland; véase arXiv próximamente)

- Salvo conjuación en $\mathrm{USp}(6)$, existen 410 grupos de Sato–Tate de variedades abelianas de dimensión 3 definidas sobre cuerpos de números.
- Los 33 grupos maximales (con respecto a inclusiones finitas) ocurren como grupos de Sato–Tate de variedades abelianas sobre $\mathbb{Q}$ o $\mathbb{Q}(\sqrt{3})$.
- Para una variedad abeliana A/k de dimensión 3, el grado $[F_A : k]$ divide 192, 336, or 432.

Observación

Guralnick y Kedlaya habían probado: $[F_A : k] \mid \mathrm{mcm}(192, 336, 432)$.
Que 192 y 336 se pueden alcanzar se conocía por F.-Lorenzo-Sutherland.

Puntos adicionales (abiertos)

- Cuántos ocurren entre Jacobianas de curvas de género 3? Cuántos ocurren entre variedades principalmente polarizadas?
- Cuántos ocurren sobre $\mathbb{Q}$?
- Existe algún k_0 sobre el cual los 410 grupos se pueden realizar?
- Para visualizar las 410 distribuciones, visitar:

  https://math.mit.edu/ drew/st3/g3SatoTateDistributions.html

Comentarios sobre la clasificación para $g = 3$

G^0	$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes \mathbb{R}$	$N_{\mathrm{USp}(6)}(G^0)/G^0$	$\#\mathcal{A}$
$\mathrm{USp}(6)$	$\mathbb{R}$	C_1	1
$\mathrm{U}(3)$	$\mathbb{C}$	C_2	2
$\mathrm{SU}(2) \times \mathrm{USp}(4)$	$\mathbb{R} \times \mathbb{R}$	C_1	1
$\mathrm{U}(1) \times \mathrm{USp}(4)$	$\mathbb{C} \times \mathbb{R}$	C_2	2
$\mathrm{U}(1) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$	$\mathbb{C} \times \mathbb{R} \times \mathbb{R}$	$C_2 \times C_2$	5
$\mathrm{SU}(2) \times \mathrm{U}(1) \times \mathrm{U}(1)$	$\mathbb{R} \times \mathbb{C} \times \mathbb{C}$	D_4	8
$\mathrm{SU}(2) \times \mathrm{SU}(2)_2$	$\mathbb{R} \times \mathrm{M}_2(\mathbb{R})$	$\mathrm{O}(2)$	10
$\mathrm{SU}(2) \times \mathrm{U}(1)_2$	$\mathbb{R} \times \mathrm{M}_2(\mathbb{C})$	$\mathrm{SO}(3) \times C_2$	32
$\mathrm{U}(1) \times \mathrm{SU}(2)_2$	$\mathbb{C} \times \mathrm{M}_2(\mathbb{R})$	$C_2 \times \mathrm{O}(2)$	31
$\mathrm{U}(1) \times \mathrm{U}(1)_2$	$\mathbb{C} \times \mathrm{M}_2(\mathbb{C})$	$C_2 \times \mathrm{SO}(3) \times C_2$	122
$\mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$	$\mathbb{R} \times \mathbb{R} \times \mathbb{R}$	S_3	4
$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$	$\mathbb{C} \times \mathbb{C} \times \mathbb{C}$	$(C_2 \times C_2 \times C_2) \rtimes S_3$	33
$\mathrm{SU}(2)_3$	$\mathrm{M}_3(\mathbb{R})$	$\mathrm{SO}(3)$	11
$\mathrm{U}(1)_3$	$\mathrm{M}_3(\mathbb{C})$	$\mathrm{PSU}(3) \rtimes C_2$	171

$\mathcal{A} = \{\text{subgrupos finitos de } N_{\mathrm{USp}(6)}(G^0)/G^0 \text{ para los que (ST2) se satisface}\}$.

Una versión efectiva

Sea A/k una variedad abeliana de dimensión $g \geq 1$.

Sea μ_{ST} la medida de Haar de $\mathrm{ST}(A)$ y, sobre el intervalo $[-2g, 2g]$, consideremos la medida $\mu = \mathrm{Tr}_*(\mu_{\mathrm{ST}})$.

Dado $I \subseteq [-2g, 2g]$, sea δ_I la función indicadora de I.

Sea $\mathrm{Li}(x) = \int_2^x \log(t)^{-1} dt$. El teorema del número primo dar lugar a

Reformulación de la conjetura de Sato–Tate

$$\sum_{\mathrm{Nm}(\mathfrak{p}) \leq x} \delta_I(\overline{a}_{\mathfrak{p}}) = \mu(I)\mathrm{Li}(x) + o\left(\frac{x}{\log(x)}\right) \qquad \text{cuando } x \to \infty\,.$$

Versión efectiva de la conjetura de Sato–Tate

Existe $\varepsilon > 0$ tal que

$$\sum_{\mathrm{Nm}(\mathfrak{p}) \leq x} \delta_I(\overline{a}_{\mathfrak{p}}) = \mu(I)\mathrm{Li}(x) + O\left(x^{1-\varepsilon}\right) \qquad \text{cuando } x \to \infty\,.$$

Una versión efectiva vía funciones L

Sea ϱ una irrep de $\mathsf{ST}(A)$.

Sea $\Lambda(A, \varrho, s)$ la función L completada asociada a $L(A, \varrho, s)$.

Hipótesis de Riemann generalizada para ϱ:

- $\Lambda(A, \varrho, s)$ extiende a una función meromorfa a $\mathbb{C}$. Tiene polos simples en $s = 0$ y 1 si ϱ es trivial, y es analítica en otro caso.
- $\Lambda(A, \varrho, s)$ satisface una equación funcional ($s \leftrightarrow 1 - s$).
- Todos los ceros de $\Lambda(A, \varrho, s)$ se hallan sobre la recta $\Re(s) = 1/2$.

Teorema 3 (Bucur-F.-Kedlaya; 2019)

Si HRG se cumple para toda ϱ, entonces la versión efectiva de Sato-Tate se cumple tomando

$$\varepsilon = \frac{1}{2(q + \varphi)},$$

siendo $q = \mathrm{rk}(\mathrm{ST}(\mathrm{A}))$ y φ el núm. de raíces positivas de su parte semisimple.