

Distribuciones y grupos de Sato-Tate de los twists de la cuártica de Fermat.

Elisa Lorenzo García

Universitat Politècnica de Catalunya

Trabajo conjunto con Francesc Fité Naya

24 de Enero de 2012

Contando puntos.

Consideremos la curva elíptica con CM por $\mathbb{Q}(i)$:

$$y^2 = x^3 + x.$$

Contando puntos.

Consideremos la curva elíptica con CM por $\mathbb{Q}(i)$:

$$y^2 = x^3 + x.$$

¿Cuántos puntos tiene sobre \mathbb{F}_p ?

Contando puntos.

Consideremos la curva elíptica con CM por $\mathbb{Q}(i)$:

$$y^2 = x^3 + x.$$

¿Cuántos puntos tiene sobre \mathbb{F}_p ?

p	3	5	7	11	13	17	19	23	29	...
	4	4	8	12	20	16	20	24	20	...

Contando puntos.

El número de puntos sobre \mathbb{F}_p de una curva C de género g es

$$N_p(C) = 1 + p - t_p,$$

donde t_p es la **traza del endomorfismo de Frobenius**. Que es un entero $t_p \in [-2g\sqrt{p}, 2g\sqrt{p}]$.

Contando puntos.

El número de puntos sobre \mathbb{F}_p de una curva C de género g es

$$N_p(C) = 1 + p - t_p,$$

donde t_p es la **traza del endomorfismo de Frobenius**. Que es un entero $t_p \in [-2g\sqrt{p}, 2g\sqrt{p}]$.

Definimos

$$x_p = \frac{t_p}{\sqrt{p}} \in [-2g, 2g].$$

Contando puntos.

p	3	5	7	11	13	17	19	23	29	...
t_p	0	2	0	0	-6	2	0	0	10	...
x_p	0	0,894...	0	0	-1,664...	0,484...	0	0	1,856...	...

Contando puntos.

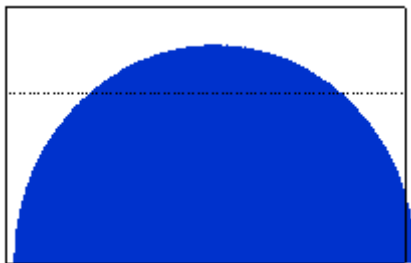
p	3	5	7	11	13	17	19	23	29	...
t_p	0	2	0	0	-6	2	0	0	10	...
x_p	0	0,894...	0	0	-1,664...	0,484...	0	0	1,856...	...

Cómo se distribuye x_p cuando p varía?

Género 1 (sobre \mathbb{Q}).

LA CONJETURA ORIGINAL DE SATO-TATE.

Dada una curva elíptica ($g = 1$) sin CM, x_p tiene la distribución semicircular.

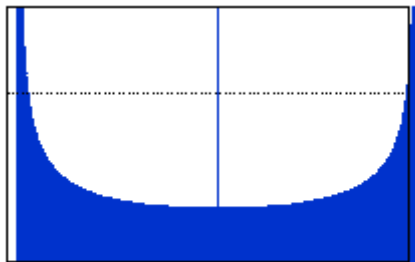


$$f(t) = \frac{1}{2\pi} \sqrt{4 - t^2}.$$

Género 1 (sobre \mathbb{Q}).

CASO EXCEPCIONAL (CM).

Dada una curva elíptica con CM, x_p tiene la siguiente distribución:



$$f(t) = \frac{1}{2}\delta_0 + \frac{1}{2} \frac{1}{\pi\sqrt{4-t^2}}.$$

El factor local en un primo p .

Dada una curva C/\mathbb{Q} de género g se define su función zeta en un primo p como:

$$Z(C/\mathbb{F}_p; T) = \exp\left(\sum_{k=1}^{\infty} N_{p^k}(C) T^k\right).$$

El factor local en un primo p .

Dada una curva C/\mathbb{Q} de género g se define su función zeta en un primo p como:

$$Z(C/\mathbb{F}_p; T) = \exp\left(\sum_{k=1}^{\infty} N_{p^k}(C) T^k\right).$$

Que es una función racional:

$$Z(C/\mathbb{F}_p; T) = \frac{L_p(T)}{(1-T)(1-pT)}.$$

$L_p(T)$ es el **factor local** en el primo p de C .

El factor local en un primo p .

El factor local $L_p(T)$ es un polinomio con coeficientes enteros:

$$L_p(C) = \sum_{i=0}^{2g} c_i(T) T^i.$$

El factor local en un primo p .

El factor local $L_p(T)$ es un polinomio con coeficientes enteros:

$$L_p(C) = \sum_{i=0}^{2g} c_i(T) T^i.$$

Para $g = 1$: $L_p(C) = pT^2 + c_1T + 1$ donde $t_p = -c_1$.

Para $g = 2$: $L_p(C) = p^2T^4 + c_1pT^3 + c_2T^2 + c_1T + 1$.

Y para $g = 3$:

$L_p(C) = p^3T^6 + c_1p^2T^5 + c_2pT^4 + c_3T^3 + c_2T^2 + c_1T + 1$.

El factor local normalizado.

Definimos el factor local normalizado como:

$$\bar{L}_p(T) = L_p(T/\sqrt{p}) = \sum_{i=0}^{2g} a_i(p) T^i.$$

Es un polinomio simétrico real con raíces de norma 1. Luego,

$$a_{2g-i}(p) = a_i(p) \in \left[-\binom{2g}{i}, \binom{2g}{i} \right].$$

El factor local normalizado.

Definimos el factor local normalizado como:

$$\bar{L}_p(T) = L_p(T/\sqrt{p}) = \sum_{i=0}^{2g} a_i(p) T^i.$$

Es un polinomio simétrico real con raíces de norma 1. Luego,

$$a_{2g-i}(p) = a_i(p) \in \left[-\binom{2g}{i}, \binom{2g}{i} \right].$$

Y podemos estudiar la distribución de a_1, a_2, \dots, a_g cuando p varía.

The Generalized Sato-Tate Conjecture.

Como $\bar{L}_p(T)$ es un polinomio real simétrico cuyas raíces tienen norma 1, podemos ver $\bar{L}_p(T)$ como el polinomio característico $P(T)$ de una matriz unitaria y simpléctica de tamaño $2g$.

The Generalized Sato-Tate Conjecture.

Como $\bar{L}_p(T)$ es un polinomio real simétrico cuyas raíces tienen norma 1, podemos ver $\bar{L}_p(T)$ como el polinomio característico $P(T)$ de una matriz unitaria y simpléctica de tamaño $2g$.

Conjetura (Generalized Sato-Tate): Dada una variedad abeliana A/k de dimensión g (e.g. la jacobiana de una curva de género g), la distribución de $\bar{L}_p(T)$ converge a la distribución de $P(T)$ en algún subgrupo infinito y compacto $G \subseteq USp(2g)$ con la medida de Haar.

The Generalized Sato-Tate Conjecture.

Como $\bar{L}_p(T)$ es un polinomio real simétrico cuyas raíces tienen norma 1, podemos ver $\bar{L}_p(T)$ como el polinomio característico $P(T)$ de una matriz unitaria y simpléctica de tamaño $2g$.

Conjetura (Generalized Sato-Tate): Dada una variedad abeliana A/k de dimensión g (e.g. la jacobiana de una curva de género g), la distribución de $\bar{L}_p(T)$ converge a la distribución de $P(T)$ en algún subgrupo infinito y compacto $G \subseteq USp(2g)$ con la medida de Haar.

El grupo G es el grupo de Sato-Tate de la var. ab. A .

Grupos de Sato-Tate en género 1 (sobre \mathbb{Q}).

El grupo de Sato-Tate de una curva elíptica sin CM es el grupo $USp(2g) = SU(2)$.

Grupos de Sato-Tate en género 1 (sobre \mathbb{Q}).

El grupo de Sato-Tate de una curva elíptica sin CM es el grupo $USp(2g) = SU(2)$.

Si la curva elíptica tiene CM, entonces su grupo de Sato-Tate es conjugado a

$$H = \left\{ \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}, \begin{pmatrix} i \cos \theta & i \sin \theta \\ i \sin \theta & -i \cos \theta \end{pmatrix} : \theta \in [0, 2\pi] \right\}$$

que es el normalizador del grupo $SO(2) = U(1)$ en $SU(2)$.

La sucesión de momentos.

La sucesión de momentos de una variable aleatoria X es

$$M(X) = (M_0(X), M_1(X), M_2(X), \dots)$$

donde $M_n(X) = \mathbb{E}[X^n]$.

Bajo ciertas condiciones en la variable X , $M_n(X)$ existe y la sucesión de momentos determina completamente la variable aleatoria X .

Si X es un coeficiente del polinomio característico de una matriz en un subgrupo compacto de $USp(2g)$, entonces los momentos $M_n(X)$ son números enteros. Es decir, $M_n(a_i) \in \mathbb{Z}$.

La sucesión de momentos en género 1 (sobre \mathbb{Q}).

Caso genérico (sin CM):

$$M(a_1) = (1, 0, 1, 0, 2, 0, 5, 0, 14, 0, 42, 0, 132, \dots)$$

de hecho $M_{2n}(a_1) = c_n$ y $M_{2n+1}(a_1) = 0$. Donde $c_n = \tilde{c}_n / (n + 1)$ y \tilde{c}_n representa el número de Catalan n -ésimo.

La sucesión de momentos en género 1 (sobre \mathbb{Q}).

Caso genérico (sin CM):

$$M(a_1) = (1, 0, 1, 0, 2, 0, 5, 0, 14, 0, 42, 0, 132, \dots)$$

de hecho $M_{2n}(a_1) = c_n$ y $M_{2n+1}(a_1) = 0$. Donde $c_n = \tilde{c}_n / (n + 1)$ y \tilde{c}_n representa el número de Catalan n -ésimo.

Caso excepcional (CM):

$$M(a_1) = (1, 0, 1, 0, 3, 0, 10, 0, 35, 0, 126, 0, \dots)$$

se tiene $M_{2n+1}(a_1) = 0$ y $M_{2n}(a_1) = \frac{1}{2}\tilde{c}_n$.

Ejemplo de una sucesión de momentos.

Queremos estudiar el 4^º momento de la curva elíptica:

$$E : y^2 = x^3 + x.$$

Ejemplo de una sucesión de momentos.

Queremos estudiar el 4^º momento de la curva elíptica:

$$E : y^2 = x^3 + x.$$

N	10	50	100	200	500	1000
$\frac{1}{N} \sum_{n=1}^N \left(\frac{t_n}{\sqrt{p}} \right)^4$	2,025...	2,341...	2,520...	2.802...	2,816...	2,891...

Ejemplo de una sucesión de momentos.

Queremos estudiar el 4^º momento de la curva elíptica:

$$E : y^2 = x^3 + x.$$

N	10	50	100	200	500	1000
$\frac{1}{N} \sum_{n=1}^N \left(\frac{t_n}{\sqrt{p}} \right)^4$	2,025...	2,341...	2,520...	2.802...	2,816...	2,891...

que tiende a 3!

Dimensión 2.

En [FKRS11] se estudia el caso de dimensión 2. Donde se calcula:

Dimensión 2.

En [FKRS11] se estudia el caso de dimensión 2. Donde se calcula:

1. Todos los grupos de Sato-Tate de $USp(4)$. Obtienen 52 grupos de Sato-Tate diferentes.
2. La distribución de los polinomios característicos de las matrices de los grupos de Sato-Tate encontrados.
3. Una curva de género 2 con grupo de Sato-Tate cada uno de los calculados. Prueban que de los 52 grupos de S-T encontrados, 34 se pueden realizar sobre \mathbb{Q} .

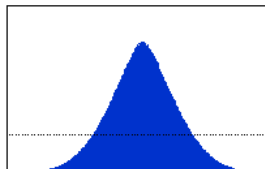
Dimensión 2.

En [FKRS11] se estudia el caso de dimensión 2. Donde se calcula:

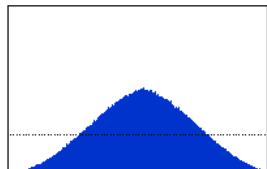
1. Todos los grupos de Sato-Tate de $USp(4)$. Obtienen 52 grupos de Sato-Tate diferentes.
2. La distribución de los polinomios característicos de las matrices de los grupos de Sato-Tate encontrados.
3. Una curva de género 2 con grupo de Sato-Tate cada uno de los calculados. Prueban que de los 52 grupos de S-T encontrados, 34 se pueden realizar sobre \mathbb{Q} .

Además, se comprueba numericamente que la distribución de Sato-Tate de estas curvas coincide con la distribución de los grupos de Sato-Tate.

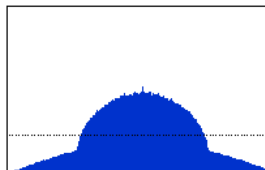
Dimensión 2: a_1 .



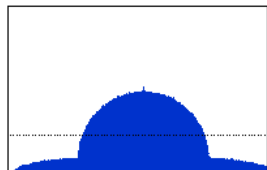
#1



#2

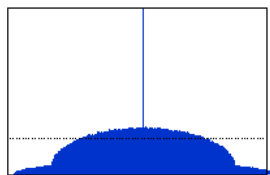


#3

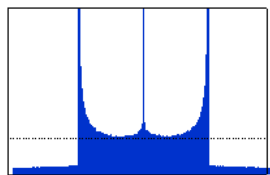


#4

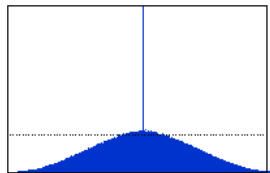
Dimensión 2: a_1 .



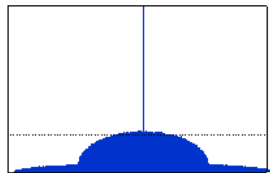
#7



#8



#9



#10

Dimensión 2.

Conclusiones importante en [FKRS11].

- ▶ Para cada grupo de S-T existe una curva de género 2 tal que su jacobiana tiene dicho grupo de S-T.
- ▶ Dada una curva de género 2 con muchos automorfismos, si se varía el cuerpo de definición k y se consideran diferentes twists, se obtienen muchísimas de las posibilidades para los grupos y las distribuciones de S-T en dimensión 2.

Estos dos puntos motivan nuestro trabajo en el caso de dimensión 3 con la cuártica de Fermat y sus twists.

La cuártica de Fermat.

La **cuártica de Fermat** es una curva de género 3 no hiperelíptica:

$$C : x^4 + y^4 + z^4 = 0.$$

La consideraremos definida sobre \mathbb{Q} . Y entonces $Aut(C)$ está definido sobre $\mathbb{Q}(i)$.

La cuártica de Fermat.

La **cuártica de Fermat** es una curva de género 3 no hiperelíptica:

$$C : x^4 + y^4 + z^4 = 0.$$

La consideraremos definida sobre \mathbb{Q} . Y entonces $\text{Aut}(C)$ está definido sobre $\mathbb{Q}(i)$.

Se tiene que

$$J(C) \simeq_{\mathbb{Q}} E^3,$$

con $E : y^2 = x^3 + x$, que tiene CM por $\mathbb{Q}(i)$ y por tanto:

$$\text{End}_{\overline{\mathbb{Q}}}(J(C)) \otimes \mathbb{Q} \simeq \mathcal{M}_3(\mathbb{Q}(i)).$$

La cuártica de Fermat.

Tenemos una **clasificación** de todos los **twists** de la cuártica de Fermat sobre cualquier cuerpo de números k .

La cuártica de Fermat.

Tenemos una **clasificación** de todos los **twists** de la cuártica de Fermat sobre cualquier cuerpo de números k .
Desde los más sencillos:

$$a^2x^4 + y^4 + z^4 = 0,$$

La cuártica de Fermat.

Tenemos una **clasificación** de todos los **twists** de la cuártica de Fermat sobre cualquier cuerpo de números k .

Desde los más sencillos:

$$a^2x^4 + y^4 + z^4 = 0,$$

al más “complicado”:

$$8x^3y - 3(4x^3z + 6x^2y^2) + 2(12x^2yz + 4xy^3) - 5(12xy^2z + y^4 + 6x^2z^2) + \\ + 5(12xyz^2 + 4y^3z) - 7(4xz^3 + 6y^2z^2) + 40yz^3 - 12z^4 = 0$$

con $K = \mathbb{Q}\left(i, a, b, c, \sqrt[4]{\frac{b}{a}}, \sqrt[4]{\frac{c}{a}}\right)$ y a, b, c las raíces de $T^3 - T + 1 = 0$.

La distribución de Sato-Tate de la cuártica de Fermat.

El factor local normalizado de un twist de la cuártica de Fermat tiene la forma:

$$\begin{aligned}\bar{L}_p(J(C')) &= \\ &= T^6 + a_1(p) T^5 + a_2(p) T^4 + a_3(p) T^3 + a_2(p) T^2 + a_1(p) T + 1.\end{aligned}$$

La distribución de Sato-Tate de la cuártica de Fermat.

El factor local normalizado de un twist de la cuártica de Fermat tiene la forma:

$$\begin{aligned}\bar{L}_p(J(C')) &= \\ &= T^6 + a_1(p) T^5 + a_2(p) T^4 + a_3(p) T^3 + a_2(p) T^2 + a_1(p) T + 1.\end{aligned}$$

Y denotamos por $t_p = 1 + p - N_p(E)$ a la traza del endomorfismo de Frobenius de la curva elíptica:

$$E : y^2 = x^3 + x.$$

La distribución de Sato-Tate de un twist.

- ▶ $C : x^4 + y^4 + z^4 = 0$ y $J(C) \simeq_{\mathbb{Q}} E^3$, entonces: $a_1(p) = 3 \frac{t_p}{\sqrt{p}}$
y por tanto:

$$M_{2n}(a_1/J(C)) = \frac{3^{2n}}{2} \tilde{c}_n.$$

La distribución de Sato-Tate de un twist.

- ▶ $C : x^4 + y^4 + z^4 = 0$ y $J(C) \simeq_{\mathbb{Q}} E^3$, entonces: $a_1(p) = 3 \frac{t_p}{\sqrt{p}}$
y por tanto:

$$M_{2n}(a_1/J(C)) = \frac{3^{2n}}{2} \tilde{c}_n.$$

- ▶ $C' : a^2 x^4 + y^4 + z^4 = 0$ y $J(C') \sim_{\mathbb{Q}} E \times (E')^2$, entonces

$$a_1(p) = t_p/\sqrt{p} + 2 \left(\frac{a}{p}\right) t_p/\sqrt{p} = \left(1 + 2 \left(\frac{a}{p}\right)\right) t_p/\sqrt{p}$$

La distribución de Sato-Tate de un twist.

- $C : x^4 + y^4 + z^4 = 0$ y $J(C) \simeq_{\mathbb{Q}} E^3$, entonces: $a_1(p) = 3 \frac{t_p}{\sqrt{p}}$
y por tanto:

$$M_{2n}(a_1/J(C)) = \frac{3^{2n}}{2} \tilde{c}_n.$$

- $C' : a^2 x^4 + y^4 + z^4 = 0$ y $J(C') \sim_{\mathbb{Q}} E \times (E')^2$, entonces

$$a_1(p) = t_p/\sqrt{p} + 2 \left(\frac{a}{p}\right) t_p/\sqrt{p} = \left(1 + 2 \left(\frac{a}{p}\right)\right) t_p/\sqrt{p}$$

Y por tanto,

$$M_{2n}(a_1/J(C')) = \frac{3^{2n} + (-1)^{2n}}{2} \frac{1}{2} \tilde{c}_n = \frac{3^{2n} + 1}{4} \tilde{c}_n.$$

La distribución de Sato-Tate de los twists.

Se tiene que:

$$M_{2n+1}(a_1(J(C')/\mathbb{Q})) = 0$$

La distribución de Sato-Tate de los twists.

Se tiene que:

$$M_{2n+1}(a_1(J(C')/\mathbb{Q})) = 0$$

Y:

$$M_{2n}(a_1(J(C')/\mathbb{Q})) =$$

$$\frac{M_{2n}(a_1(J(C')/\mathbb{Q} \mid p \equiv 1 \pmod{4})) + M_{2n}(a_1(J(C')/\mathbb{Q} \mid p \equiv 3 \pmod{4}))}{2}$$
$$= \frac{1}{2} M_{2n}(a_1(J(C')/\mathbb{Q}(i)))$$

La distribución de Sato-Tate de los twists.

Teorema: *Se tiene que:*

$$M_{2n}(a_1(J(C')/\mathbb{Q}(i))) = \frac{1}{|G|} \sum_{\sigma \in \text{Gal}(K/\mathbb{Q}(i))} |a_1(\sigma)|^n \tilde{c}_n.$$

Donde

$$\det(1 - \theta(\sigma) T) = 1 + a_1(\sigma) T + a_2(\sigma) T^2 + a_3(\sigma) T^3$$

y θ es la representación dada por el $\mathbb{Q}(i)$ -esp. vect.

$\text{End}_{\overline{\mathbb{Q}}}(E, J(C')) \otimes \mathbb{Q}$ y la acción natural de $G = \text{Gal}(K/\mathbb{Q}(i))$.

La distribución de Sato-Tate de los twists.

$$M_n(a_2(J(C')/\mathbb{Q})) = \frac{1}{2|G|} \left(\sum_{\sigma \in G} \sum_{i=0}^n \binom{n}{i} c_i |a_2(\sigma)|^i (|a_1(\sigma)| - 2|a_2(\sigma)|)^{n-i} + \right. \\ \left. + (o(2) + 1)3^n + o(4)(-1)^n + o(8) \right).$$

$$M_{2n}(a_3(J(C')/\mathbb{Q})) = \frac{1}{2|G|} \left(\sum_{\sigma \in G} \sum_{i=0}^n \binom{2n}{2i} \sum_{j=0}^{2i} \sum_{k=0}^{n-i} \binom{2i}{j} a_3(\sigma)^j \cdot \right. \\ \left. (r_1(\sigma) - 3a_3(\sigma))^{2i-j} r_2(\sigma)^{2n-2i} \binom{n-i}{k} 4^k (-1)^{n-i-k} c_{j+n-k} \right).$$

La distribución de Sato-Tate de los twists.

Luego, o bien se calcula la acción de $Gal(L/\mathbb{Q}(i))$ en $End_{\overline{\mathbb{Q}}}(E, J(C')) \otimes \mathbb{Q}$:

- ▶ $C : x^4 + y^4 + z^4 = 0$ y $J(C) \simeq_{\mathbb{Q}} E^3$, entonces $G = \{1\}$ y $\theta = 3\mathcal{E}$, y por tanto:

$$M_{2n}(a_1(J(C)/\mathbb{Q})) = \frac{1}{2 \cdot 1} (9^n \tilde{c}_n) = \frac{3^{2n}}{2} \tilde{c}_n.$$

La distribución de Sato-Tate de los twists.

Luego, o bien se calcula la acción de $Gal(L/\mathbb{Q}(i))$ en $End_{\overline{\mathbb{Q}}}(E, J(C')) \otimes \mathbb{Q}$:

- ▶ $C : x^4 + y^4 + z^4 = 0$ y $J(C) \simeq_{\mathbb{Q}} E^3$, entonces $G = \{1\}$ y $\theta = 3\mathcal{E}$, y por tanto:

$$M_{2n}(a_1(J(C)/\mathbb{Q})) = \frac{1}{2 \cdot 1} (9^n \tilde{c}_n) = \frac{3^{2n}}{2} \tilde{c}_n.$$

- ▶ $C' : a^2 x^4 + y^4 + z^4 = 0$ y $J(C') \sim_{\mathbb{Q}} E \times (E')^2$, entonces $G \simeq \mathbb{Z}_2$ y $\theta = \mathcal{E} + 2\chi$, y por tanto:

$$M_{2n}(a_1(J(C')/\mathbb{Q})) = \frac{1}{2 \cdot 2} (9^n + 1^n) \tilde{c}_n = \frac{3^{2n} + 1}{4} \tilde{c}_n.$$

La distribución de Sato-Tate de los twists.

O bien,

Teorema: *Se tiene que $\theta = \xi^{-1} |_{G}$, donde ξ es el cociclo asociado al twist $J(C')$ de $J(C)$.*

La distribución de Sato-Tate de los twists.

O bien,

Teorema: *Se tiene que $\theta = \xi^{-1} |_{G}$, donde ξ es el cociclo asociado al twist $J(C')$ de $J(C)$.*

- ▶ $C : x^4 + y^4 + z^4 = 0$ y $J(C) \simeq_{\mathbb{Q}} E^3$, entonces $G = \{1\}$ y $\xi(1) = id_3$, y por tanto:

$$M_{2n}(a_1(J(C)/\mathbb{Q})) = \frac{1}{2 \cdot 1} (9^n \tilde{c}_n) = \frac{3^{2n}}{2} \tilde{c}_n.$$

La distribución de Sato-Tate de los twists.

O bien,

Teorema: Se tiene que $\theta = \xi^{-1} |_G$, donde ξ es el cociclo asociado al twist $J(C')$ de $J(C)$.

- ▶ $C : x^4 + y^4 + z^4 = 0$ y $J(C) \simeq_{\mathbb{Q}} E^3$, entonces $G = \{1\}$ y $\xi(1) = id_3$, y por tanto:

$$M_{2n}(a_1(J(C)/\mathbb{Q})) = \frac{1}{2 \cdot 1} (9^n \tilde{c}_n) = \frac{3^{2n}}{2} \tilde{c}_n.$$

- ▶ $C' : a^2 x^4 + y^4 + z^4 = 0$ y $J(C') \sim_{\mathbb{Q}} E \times (E')^2$, entonces $G \simeq \mathbb{Z}_2$ y $\xi(1) = id_3$ y $\xi(\sigma) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$, y por tanto:

$$M_{2n}(a_1(J(C')/\mathbb{Q})) = \frac{1}{2 \cdot 2} (9^n + 1^n) \tilde{c}_n = \frac{3^{2n} + 1}{4} \tilde{c}_n.$$

La distribución de Sato-Tate de los twists.

Conclusión:

- ▶ Se obtienen 29 distribuciones distintas para a_1 , de las que 15 se realizan sobre \mathbb{Q} .
- ▶ Se obtienen 43 distribuciones distintas para a_2 , de las que 23 se realizan sobre \mathbb{Q} .
- ▶ Se obtienen 34 distribuciones distintas para a_3 , de las que 17 se realizan sobre \mathbb{Q} .

Finalmente, se obtienen 48 **distribuciones de Sato-Tate** diferentes, de las que 23 se realizan sobre \mathbb{Q} .

El grupo de Sato-Tate de los twists.

Teorema ([BK11]): *Sea A/k una var. ab. de dimensión menor o igual que 3, entonces el grupo de Sato-Tate de A/k es un subgrupo maximal compacto de $TL_k(A) \otimes_{\mathbb{Q}_l} \mathbb{C}$.*

Donde $TL_k(A)$ es el grupo de Lefschetz twistado de A/k , definido como

$$TL_k(A) = \sqcup_{\sigma \in \text{Gal}(K/k)} L_{A/k}(\sigma)$$

donde

$$L_{A/k}(\sigma) = \{ \gamma \in Sp_{2g}(\mathbb{Q}_l) : \gamma \beta \gamma^{-1} = \sigma \beta \forall \beta \in \text{End}_{\bar{k}}(V_l(A)) \}.$$

The Sato-Tate group.

Para la cuártica de Fermat $Gal(K/\mathbb{Q}) = \mathbb{Z}_2$ y $End_{\bar{\mathbb{Q}}}(V_l(J(C)))$ está generado por:

$$\begin{pmatrix} id_2 & 0 & 0 \\ 0 & 0 & id_2 \\ 0 & id_2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & id_2 \\ id_2 & 0 & 0 \\ 0 & id_2 & 0 \end{pmatrix}, \begin{pmatrix} J & 0 & 0 \\ 0 & id_2 & 0 \\ 0 & 0 & id_2 \end{pmatrix}$$

con $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Luego:

$$L_{J(C)}(1) \cap U_{2g} \rightarrow \left\{ \begin{pmatrix} A & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & A \end{pmatrix} : A = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \theta \in [0, 2\pi] \right\},$$

$$L_{J(C)}(\tau) \cap U_{2g} \rightarrow \left\{ \begin{pmatrix} B & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & B \end{pmatrix} : B = \begin{pmatrix} i \cos \theta & i \sin \theta \\ i \sin \theta & -i \cos \theta \end{pmatrix} \theta \in [0, 2\pi] \right\}.$$

The Sato-Tate group.

La **traza** de las matrices en $L_{J(C)}(\tau)$ es siempre cero. Luego, en esta componente $\mathbb{E}[a_1^n] = 0$.

La **traza** de las matrices de $L_{J(C')}(\mathbf{1})$ es $6\cos\theta$, luego:

$$\mathbb{E}[a_1^n] = \frac{6^n}{2^n} \int_0^{2\pi} \frac{\cos^n\theta}{2\pi} d\theta = \begin{cases} 0 & \text{si } n \text{ impar} \\ 3^n \tilde{c}_{n/2} & \text{si } n \text{ par} \end{cases}$$

The Sato-Tate group.

La **traza** de las matrices en $L_{J(C)}(\tau)$ es siempre cero. Luego, en esta componente $\mathbb{E}[a_1^n] = 0$.

La **traza** de las matrices de $L_{J(C')}(1)$ es $6\cos\theta$, luego:

$$\mathbb{E}[a_1^n] = \frac{6^n}{2^n} \int_0^{2\pi} \frac{\cos^n\theta}{2\pi} d\theta = \begin{cases} 0 & \text{si } n \text{ impar} \\ 3^n \tilde{c}_{n/2} & \text{si } n \text{ par} \end{cases}$$

Haciendo la media:

$$M_{2n}(a_1/J(C)) = \frac{3^{2n}\tilde{c}_n + 0}{2} = \frac{3^{2n}}{2}\tilde{c}_n.$$

The Sato-Tate group.

Dado un twist $\phi : C' \rightarrow C$ de la cuártica de Fermat y $\sigma \in \text{Gal}(L/\mathbb{Q})$, se tiene que

$$L_{J(C')/\mathbb{Q}}(\sigma) = \begin{cases} \phi^{-1} L_{J(C)/\mathbb{Q}}(\mathbf{1})^\sigma \phi & \text{si } \bar{\sigma} = \mathbf{1}. \\ \phi^{-1} L_{J(C)/\mathbb{Q}}(\tau)^\sigma \phi & \text{si } \bar{\sigma} = \tau. \end{cases}$$

The Sato-Tate group.

Dado un twist $\phi : C' \rightarrow C$ de la cuártica de Fermat y $\sigma \in \text{Gal}(L/\mathbb{Q})$, se tiene que

$$L_{J(C')/\mathbb{Q}}(\sigma) = \begin{cases} \phi^{-1} L_{J(C)/\mathbb{Q}}(1)^\sigma \phi & \text{si } \bar{\sigma} = 1. \\ \phi^{-1} L_{J(C)/\mathbb{Q}}(\tau)^\sigma \phi & \text{si } \bar{\sigma} = \tau. \end{cases}$$

Luego los conjuntos $L_{J(C')/\mathbb{Q}}(\sigma)$ son conjugados a los conjuntos:

$$L_{J(C)/\mathbb{Q}}(\bar{\sigma}) \xi_\sigma^{-1}.$$

The Sato-Tate group.

Dado un twist $\phi : C' \rightarrow C$ de la cuártica de Fermat y $\sigma \in \text{Gal}(L/\mathbb{Q})$, se tiene que

$$L_{J(C')/\mathbb{Q}}(\sigma) = \begin{cases} \phi^{-1} L_{J(C)/\mathbb{Q}}(1)^\sigma \phi & \text{si } \bar{\sigma} = 1. \\ \phi^{-1} L_{J(C)/\mathbb{Q}}(\tau)^\sigma \phi & \text{si } \bar{\sigma} = \tau. \end{cases}$$

Luego los conjuntos $L_{J(C')/\mathbb{Q}}(\sigma)$ son conjugados a los conjuntos:

$$L_{J(C)/\mathbb{Q}}(\bar{\sigma}) \xi_\sigma^{-1}.$$

Para $C' : a^2 x^4 + y^4 + z^4 = 0$, tenemos $\text{Gal}(L/\mathbb{Q}) = \{1, \tau, \sigma, \tau\sigma\}$:

The Sato-Tate group.

$$L_{J(C')}(\mathbf{1}) \rightarrow \left\{ \begin{pmatrix} A & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & A \end{pmatrix} : A = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \theta \in [0, 2\pi] \right\}$$

$$L_{J(C')}(\tau) \rightarrow \left\{ \begin{pmatrix} B & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & B \end{pmatrix} : B = \begin{pmatrix} i\cos \theta & i\sin \theta \\ i\sin \theta & -i\cos \theta \end{pmatrix} \theta \in [0, 2\pi] \right\}$$

$$L_{J(C')}(\sigma) \rightarrow \left\{ \begin{pmatrix} -A & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & A \end{pmatrix} : A = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} \theta \in [0, 2\pi] \right\}$$

$$L_{J(C')}(\sigma\tau) \rightarrow \left\{ \begin{pmatrix} -B & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & B \end{pmatrix} : B = \begin{pmatrix} i\cos \theta & i\sin \theta \\ i\sin \theta & -i\cos \theta \end{pmatrix} \theta \in [0, 2\pi] \right\}.$$

The distribution of the Sato-Tate groups.

Haciendo la media:

$$M_{2n}(a_1/J(C')) = \frac{3^{2n}\tilde{c}_n + 0 + 0 + \tilde{c}_n}{4} = \frac{3^{2n} + 1}{4}\tilde{c}_n.$$

The distribution of the Sato-Tate groups.

Haciendo la media:

$$M_{2n}(a_1/J(C')) = \frac{3^{2n}\tilde{c}_n + 0 + 0 + \tilde{c}_n}{4} = \frac{3^{2n} + 1}{4}\tilde{c}_n.$$

¡Qué es la misma sucesión de momentos que la de la distribución de Sato-Tate del twist!

Conclusiones.

- ▶ Se han calculado los **grupos de Sato-Tate** para todos los twists de la cuártica de Fermat sobre cualquier cuerpo de números k . También se ha calculado la distribución de los polinomios característicos de las matrices de estos grupos. En total se han encontrado 48 grupos de Sato-Tate diferentes.
- ▶ Se ha calculado la **distribución de Sato-tate** de todos los twists, es decir, las distribuciones de los coeficientes a_1 , a_2 y a_3 .
- ▶ Por último, se ha comprobado que ambas distribuciones coinciden como la **conjetura de Sato-Tate** predice.

Bibliografía

- ▶ [BK11]: Banaszak G., Kedlaya K.: “An algebraic Sato-Tate group and Sato-Tate conjecture”, preprint.
- ▶ [FKRS11]: Fité F., Kedlaya K., Rotger V., Sutherland A.: “Sato-Tate distribution and Galois endomorphism modules in genus 2”, preprint.
- ▶ [KS09]: Kedlaya K., Sutherland A.: “Hyperelliptic curves, L-polynomials and random matrices”, Contemporary Mathematics (AMS) v.487, 2009.
- ▶ [Lor10]: Lorenzo E.: “Torcimientos de cuárticas planas lisas”, trabajo de máster, 2010.