Fields of definition of elliptic k-curves with CM and Sato–Tate groups of abelian surfaces

Francesc Fité[1] Xevi Guitart[2]

[1]Universität Duisburg–Essen

[2]Universitat de Barcelona

February 2016

Elliptic Curves over number fields

- An elliptic curve over a number field k is a projective curve

$$E\colon yz^2 = x^3 + axz^2 + bz^3, \quad a, b \in \mathcal{O}_k$$

- The set of points $E(k)$ admits a natural structure of abelian group.
- An endomorphism of E is an algebraic map $\varphi\colon E \to E$ (given by polynomials) which induces a group endomorphism on $E(k)$.
- The set of endomorphisms of E is a ring, and
  - $\mathrm{End}(E) \simeq \mathbb{Z}$ (generic case)
  - $\mathrm{End}(E)$ an order in an imaginary quadratic field M (E has CM by M)
- Given a prime $\mathfrak{p} \subset \mathcal{O}_k$ we can reduce the equation of E modulo $\mathfrak{p}$

$$\bar{E}\colon yz^2 = x^3 + \bar{a}xz^2 + \bar{b}z^3, \quad \bar{a}, \bar{b} \in \mathcal{O}_k/\mathfrak{p}$$

  - $\mathcal{O}_k/\mathfrak{p}$ is a finite field with $|\mathfrak{p}|$ elements
  - $\bar{E}(\mathcal{O}_k/\mathfrak{p})$ is now a finite set
  - $a_{\mathfrak{p}} = |\mathfrak{p}| + 1 - \#\bar{E}(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p})$
  - Hasse bound: $|a_{\mathfrak{p}}| \leq 2\sqrt{|\mathfrak{p}|}$

Sato-Tate for elliptic curves

- k a number field and E/k an elliptic curve
- $\mathfrak{p}$ a prime of $k \rightsquigarrow a_{\mathfrak{p}} := |\mathfrak{p}| + 1 - \#E(\mathbb{F}_{\mathfrak{p}})$
- Hasse bound: $\bar{a}_{\mathfrak{p}} = \frac{a_{\mathfrak{p}}}{\sqrt{|\mathfrak{p}|}} \in [-2, 2]$
- Sato–Tate is about regarding $\mathfrak{p} \mapsto \bar{a}_{\mathfrak{p}}$ as a random variable, when $\mathfrak{p}$ is uniformly distributed over the primes of k.
- infinitely many $\mathfrak{p}$'s, what does it mean to be uniformly distributed?
  - fix N and consider $\mathfrak{p}$'s with $|\mathfrak{p}| \leq N$; there are finitely many
  - give each $\mathfrak{p}$ equal probability, so $\bar{a}_{\mathfrak{p}}$ is a random variable
  - let $N \to \infty$ and see if there is a limiting distribution
- Equidistribution with respect to a measure
  - X compact topological space, $C(X) = \{f\colon X \to \mathbb{C} \text{ continuous}\}$
  - Measure μ on X is $\mu\colon C(X) \to \mathbb{C}$ continuous (positive and of mass 1)
  - Notation: $f \mapsto \int f d\mu$
  - A sequence $\{x_n\}_{n \geq 1} \subseteq X$ is equidistributed w.r.t. a measure μ if

$$\text{for every } f \in C(X): \quad \int f d\mu = \lim_{N \to \infty} \frac{1}{N} \sum_{i=1}^{N} f(x_i)$$

Equidistribution for Elliptic Curves

- Suppose that E/k does not have Complex Multiplication (CM)

Sato–Tate Conjecture

The sequence $\{\bar{a}_{\mathfrak{p}}\}_{\mathfrak{p}}$ of normalized Frobenius traces (ordered by $|\mathfrak{p}|$) is equidistributed in $[-2,2]$ w.r.t the measure $\frac{4}{\pi}\sqrt{4-x^2}$.

- Proved for k totally real (Clozel–Harris–Taylor–Stepherd-Barron).
- (Hecke) If E has CM by an imaginary quadratic M
  - $M \subseteq k$: equidistributed by $\frac{1}{\pi}\frac{1}{\sqrt{4-x^2}}$
  - $M \not\subseteq k$: by $\frac{1}{2\pi}\frac{1}{\sqrt{4-x^2}} + \frac{1}{2}\delta_0(x)$

Easy remark

The three distributions can be realized by curves over the same field.

- For example, any imaginary quadratic M of class number 1
  - E_1/M without CM.
  - $E_2/\mathbb{Q}$ with CM by M, and base change to M.
  - $E_3/\mathbb{Q}$ with CM by $M' \neq M$, and base to M.

Abelian varieties

- An abelian variety is an algebraic variety whose set of points has a group structure (with the addition law given by algebraic functions)
    - Elliptic curves are the abelian varieties of dimension 1
    - Abelian varieties of dimension 2 are called abelian surfaces
- It is difficult to give equations of an abelian variety of dim > 1
- C curve of genus g over $k \rightsquigarrow$ the Jacobian $J(C)$
    - It is an abelian variety over k of dimension g
    - $J(C)(k) \simeq \mathrm{Div}^0(C)/\sim$
    - $C\colon y^2 = x^5 - x$ is of genus 2 $\rightsquigarrow J(C)$ is an abelian surface
- Abelian variety $A \rightsquigarrow \mathrm{End}(A)$ the ring of endomorphisms
    - A special type of endomorphisms are the isogenies: those which are surjective.
    - We work in a category where isogenies become isomorphisms.

A reformulation of ST for Elliptic curves

- $\bar{a}_{\mathfrak{p}} \in [-2,2] \iff \bar{p}_{\mathfrak{p}}(T) = T^2 - \bar{a}_{\mathfrak{p}} T + 1$ is the characteristic polynomial of a matrix in

$$\mathrm{SU}(2) = \{A \in \mathrm{GL}_2(\mathbb{C})\colon A^{-1} = A^*,\ \det(A) = 1\}.$$

- Moreover, the matrices in $\mathrm{SU}(2)$ with characteristic polynomial $\bar{p}_{\mathfrak{p}}(T)$ form a conjugacy class:

$$\mathrm{Conj}(\mathrm{SU}(2)) \xrightarrow{\mathrm{tr}} [-2,2] \quad \text{is a bijection}$$

- Equidistribution result can be stated in terms of $\mathrm{Conj}(\mathrm{SU}(2))$.
- Any compact subgroup $G \subseteq \mathrm{SU}(2)$ gives rise to a measure in $\mathrm{Conj}(\mathrm{SU}(2))$: the push forward of the Haar measure in G via

$$G \longrightarrow \mathrm{Conj}(G) \longrightarrow \mathrm{Conj}(\mathrm{SU}(2)).$$

Restatement of the Sato–Tate conjecture

$\{\bar{p}_{\mathfrak{p}}(T) = T^2 - \bar{a}_{\mathfrak{p}} T + 1\}_{\mathfrak{p}} \in \mathrm{Conj}(SU(2))$ is equidistributed w.r.t

- $\mathrm{SU}(2)$; $\mathrm{SO}(2)$; Normalizer of $\mathrm{SO}(2)$ in $\mathrm{SU}(2)$.

The Sato–Tate group

- A/k abelian variety of dim g and $\mathfrak{p} \subset \mathcal{O}_k$ prime, $\mathbb{F}_q = \mathcal{O}_k/\mathfrak{p}$
- (Weil) There is a polynomial $L_\mathfrak{p}(T) = (1-\alpha_1 T)\dots(1-\alpha_{2g}T)$ s.t.

$$\#A(\mathbb{F}_{q^n}) = (1-q^{n/2}\alpha_1^n)\dots(1-q^{n/2}\alpha_{2g}^n), \quad \forall n \geq 1$$

- $\bar{L}_\mathfrak{p}(T) = L_\mathfrak{p}(T/\sqrt{|\mathfrak{p}|}) \rightsquigarrow$ unique element in $\mathrm{Conj}(\mathrm{USp}(2g))$
  - $\mathrm{USp}(2g) = \{A \in \mathrm{GL}_{2g}(\mathbb{C})\colon A^{-1} = A^*, A^tJA = J\}, \quad J = \mathrm{diag}\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$
- Equidistribution of $\{\bar{L}_\mathfrak{p}(A,T)\}_\mathfrak{p} \subseteq \mathrm{Conj}(\mathrm{USp}(2g))$
  - Compact subgroup of $\mathrm{USp}(2g) \rightsquigarrow$ measure in $\mathrm{Conj}(\mathrm{USp}(2g))$
- Serre gives a construction that associates to any A/k a certain compact subgroup ST_A of $\mathrm{USp}(2g)$, the Sato–Tate group of A
  - e.g. if $\dim A \leq 3$ and $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$ then $\mathrm{ST}_A = \mathrm{USp}(2g))$

Generalized Sato–Tate conjecture

The polynomials $\bar{L}_\mathfrak{p}(A,T) \in \mathrm{Conj}(\mathrm{USp}(2g))$ are equidistributed with respect to the push forward of the Haar measure in ST_A under the map

$$\mathrm{ST}_A \longrightarrow \mathrm{Conj}(\mathrm{ST}_A) \longrightarrow \mathrm{Conj}(\mathrm{USp}(2g))$$

- Elliptic curves: there are 3 possible distributions/Sato–Tate groups

The case of dimension 2

Theorem (Fité–Kedlaya–Rotger–Sutherland)

There are 52 groups (up to conjugacy in $\mathrm{USp}(4)$) that arise as Sato–Tate groups of abelian surfaces over number fields.

- An explicit list of 52 subgroups of $\mathrm{USp}(4)$ s.t. for every abelian surface A over a number field, ST_A is conjugate to one of these.
- For every G in the list, they exhibit an abelian surface A over a number field such that $\mathrm{ST}_A = G$
  - The number field is not always the same, it depends on G...

Question

Does there exist a number field k_0 such that there exist 52 abelian surfaces over k_0 realizing all possible Sato–Tate groups?

- First idea: take k_0 the compositum of the fields of definition of the 52 curves of [FKRS12], and base change the curves to k_0
  - It doesn't work, the Sato–Tate group is sensitive to base change
- How to determine the Sato–Tate group of an abelian surface A?

The Sato–Tate group via the arithmetic of A

Theorem (Fité–Kedlaya–Rotger–Sutherland)

The Sato–Tate group of A/k is completely determined by $\mathrm{End}(A_{\bar{k}}) \otimes_{\mathbb{Z}} \mathbb{R}$, viewed as a G_k-module. Moreover

- $(\mathrm{ST}_A)^0$ is determined by $\mathrm{End}(A_{\bar{k}}) \otimes_{\mathbb{Z}} \mathbb{R}$ (as an $\mathbb{R}$-algebra)
- $\mathrm{ST}_A/(\mathrm{ST}_A)^0 \simeq \mathrm{Gal}(L/k)$ (smallest field of definition of $\mathrm{End}(A_{\bar{k}})$)

- The G_k-module $\mathrm{End}(A_{\bar{k}}) \otimes_{\mathbb{Z}} \mathbb{R}$ is called the Galois type of A.
- [FKRS12]: dictionary between Galois types and Sato–Tate groups
- Observe that the component group is sensitive to base change
  - But if $k' \cap L = k$ then $\mathrm{ST}_{A_{k'}} = \mathrm{ST}_A$
  - Base change is helpful, but it does not completely solve the problem
- To sum up: we need to find k_0 and construct 52 abelian surfaces over k_0 realizing all 52 possible Galois endomorphism types
  - What kind of arithmetic problems this leads to?
  - Why controlling fields of definition of CM curves is important?

A possible obstruction

- There are three Sato–Tate groups, called O, O_1, and $J(O)$, whose component group contains S_4.
- If A/k has one of these Sato–Tate groups $\rightsquigarrow \mathrm{Gal}(L/k) \supseteq \mathrm{S}_4$
- This implies that $A_{\bar{k}} \sim E^2$ with E a CM curve, say by M
- [FKRS12] prove that
  - If the group is O then $M \subseteq k$
  - If the group is O_1 or $J(O)$, then $M \not\subseteq k$
- So far all examples in the literature of abelian surfaces A/k s.t.

$$A_{\bar{k}} \sim E^2 \text{ and } \mathrm{Gal}(L/k) \supseteq \mathrm{S}_4 \tag{1}$$

  had $M = \mathbb{Q}(\sqrt{-2})$.
- Are there examples with $M \neq \mathbb{Q}(\sqrt{-2})$?
  - If not, one could not realize all Sato–Tate groups over a single k_0: one would have $\mathbb{Q}(\sqrt{-2}) \subseteq k_0$ and $\mathbb{Q}(\sqrt{-2}) \not\subseteq k_0$ at the same time!
  - The answer is yes, and constructing such a variety is part of the solution to the problem

A more general question

Suppose that A/k is such that $A_{\bar{k}} \sim E^2$ and E has CM by M.

- What are the possibilities for M?
- Does the prescription of $\mathrm{Gal}(L/k)$ impose extra restrictions on M?

- Our techniques need to assume that $M \subseteq k$
  - In fact, to control the possibilities for M we assume $k = M$
  - This solves the case $k = \mathbb{Q}$ (by base change)

A result on the arithmetic of abelian surfaces

- Let $A/\mathbb{Q}$ with $A_{\overline{\mathbb{Q}}} \sim E^2$, where E has CM by M.
- $L =$ smallest field of definition of $\mathrm{End}(A_{\overline{\mathbb{Q}}})$. Obs: $M \subseteq L$.
  - Known that $\mathrm{Gal}(L/M) \simeq C_1, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6, A_4, S_4$
- $\mathcal{M}^1, \mathcal{M}^2 =$ M's of class number 1 and 2; $\mathcal{M}^{2,2,} =$ M's with class group $C_2 \times C_2$

Theorem

The set of possibilities for M is

$\mathrm{Gal}(L/M)$	$\mathcal{M}(\mathrm{Gal}(L/M))$
C_1	$\mathcal{M}^1$
C_2	$\mathcal{M}^1 \cup \mathcal{M}^2$
C_3	$\mathcal{M}^1$
C_4	$\{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})\} \cup \mathcal{M}^2$
C_6	$\{\mathbb{Q}(\sqrt{-3})\} \cup \mathcal{M}^2$
D_2	$\mathcal{M}^1 \cup \mathcal{M}^2 \cup \mathcal{M}^{2,2}$
D_3	$\mathcal{M}^1 \cup \mathcal{M}^2$
D_4	$\{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})\} \cup \mathcal{M}^2 \cup \mathcal{M}^{2,2}$
D_6	$\{\mathbb{Q}(\sqrt{-3})\} \cup \mathcal{M}^2 \cup \mathcal{M}^{2,2}$
A_4	$\mathcal{M}^1 \setminus \{\mathbb{Q}(\sqrt{-7})\}$
S_4	$\{\mathbb{Q}(\sqrt{-2})\} \cup \mathcal{M}^2 \setminus \{\mathbb{Q}(\sqrt{-15}), \mathbb{Q}(\sqrt{-35}), \mathbb{Q}(\sqrt{-51}), \mathbb{Q}(\sqrt{-115})\}$

- Control field of def. of E up to isogeny (control the class group)
- Restrictions coming from representation theory (excludes cases)

A field realizing all Sato–Tate groups

Theorem

Set $k_0 := \mathbb{Q}(\sqrt{-40}, \sqrt{-51}, \sqrt{-163}, \sqrt{-67}, \sqrt{19\cdot 43}, \sqrt{-57})$. Then, there exist 52 abelian surfaces defined over k_0 realizing all possible Sato–Tate groups of abelian surfaces defined over number fields.

- Used several methods to find the 52 abelian surfaces:
  - Restriction of Scalars construction
    - A surface A/k with $A_{\overline{\mathbb{Q}}} \sim E^2$ and $\mathrm{Gal}(L/k) \simeq S_4$ and $M \neq \mathbb{Q}(\sqrt{-2})$
    - We will see that $k = M = \mathbb{Q}(\sqrt{-40})$
  - Base change the curves of [FKRS12] over $\mathbb{Q}$
    - For each $C/\mathbb{Q}$, we checked that $L \cap k_0 = \mathbb{Q}$ so that C_{k_0} works
  - Finding an explicit equation of a genus two curve, and determining the endomorphisms of the Jacobian and the field of definition
    - Search methods (help of Sutherland)
    - looking into families with prescribed automorphisms (Cardona–Quer)

Restriction of scalars construction

- $M = \mathbb{Q}(\sqrt{-40})$ and $k = M$, Hilbert class field $F = M(\sqrt{5})$
- Take L/k an extension with $\mathrm{Gal}(L/k) \simeq S_4$, with $F \subseteq L$
  - Galois closure of the extension given by $x^4 - x^3 + 5x^2 - 5x + 2$
  - field with label 4.0.5780.1 in LMFDB

$$E^* \colon y^2 = x^3 + (-31592955764755818086400\sqrt{5} - 70643996800526942208000)x$$
$$+ 144540688991650801621141888696320\sqrt{5} + 323202806099974987264542375936000$$

- E^* is a k-curve with CM by M.
  - For $\sigma \in \mathrm{Gal}(L/k)$ the isogeny $\mu_\sigma \colon {}^\sigma E \longrightarrow E$ is defined over L
  - Then $c_{E^*} \in H^2(\mathrm{Gal}(L/k), M^*)$ can be explicitly computed
- Need to take a twist: $E = (E^*)_\beta$ for some appropriate $\beta \in L$.
- Consider $R = \mathrm{Res}_{L/k} E$. It is defined over k and $R_L \sim E^{24}$.
  - Gross–Ribet: $\mathrm{End}^0(R) \simeq M^{c_E}[\mathrm{Gal}(L/k)]$ (twisted group algebra)
  - $M^{c_E}[\mathrm{Gal}(L/k)] = \bigoplus_{\sigma \in \mathrm{Gal}(L/k)} M \cdot u_\sigma$, with $u_\sigma \cdot u_\tau = c_E(\sigma, \tau) u_{\sigma\tau}$
- We can compute explicitly c_E, and therefore $\mathrm{End}^0(R)$.
  - Choosing β carefully, R decomposes in the right way
  - There is a simple factor A of dim 2 that has the sought properties

Fields of definition of elliptic k-curves with CM and Sato–Tate groups of abelian surfaces

Francesc Fité[1] Xevi Guitart[2]

[1]Universität Duisburg–Essen

[2]Universitat de Barcelona

February 2016