The generalized Sato-Tate conjecture.

Elisa Lorenzo.

Universidad Politécnica de Cataluña.

November 23, 2011

Introduction: elliptic curves.

We will start with the definition of elliptic curve:

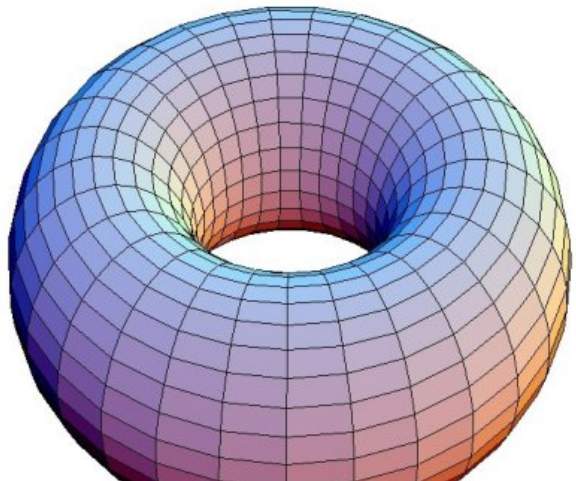
Definition

An elliptic curve is a smooth projective curve that holds an equation of the form:

$$E: \ y^2 = x^3 + ax + b,$$

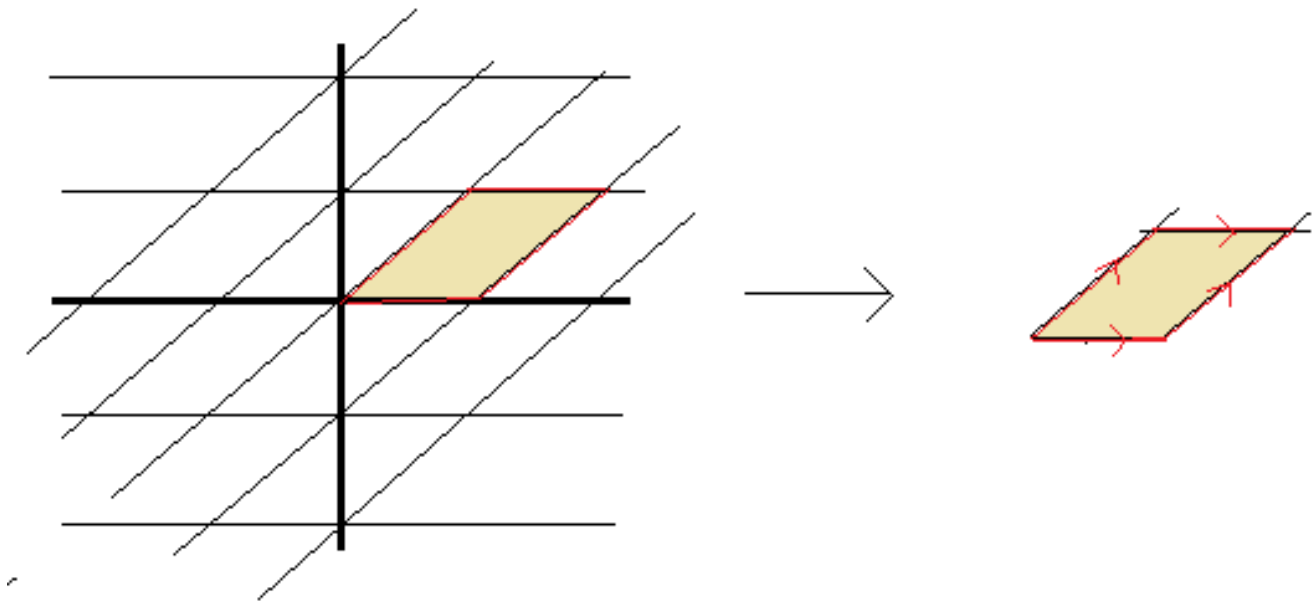
that has a distinguished point $O = (0 : 1 : 0)$ called the point at infinity. And we say that it is defined over a field k, if $a, b \in k$.

This kind of curves has genus 1 ($g = 1$), that is, they have "only one hole".



Introduction: elliptic curves.

And there is a group law defined on it, where the point at inifinity plays the role of the neutral element in the group, the zero.
We can also see an elliptic curve as the quotient of $\mathbb{C}$ by a 2-dimensional lattice:



And, in that case, the group law is adding vectors.

Introduction: elliptic curves.

We defined the endomorphisms of an elliptic curve as the morphisms of algebraic curves, $\varphi : E \longrightarrow E$, that are also morphisms of groups. That is, such that, $\varphi(Q_1 + Q_2) = \varphi(Q_1) + \varphi(Q_2)$ for all $Q_1, Q_2 \in E$. In particular, $\varphi(O) = O$.
There always exist the endomorphisms multiplication-by-m: $Q \longrightarrow m \cdot Q$. Thus,

$$\mathbb{Z} \subseteq End(E).$$

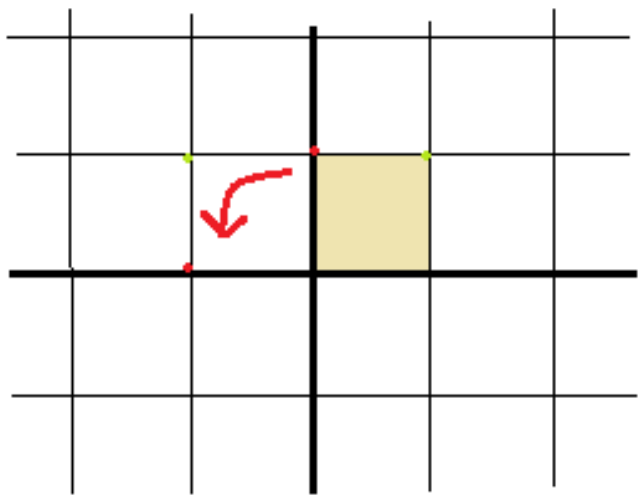
The set of endomorphisms is a ring with the sum and the composition of endomorphisms.

Definition

In the generic case, $End(E) = \mathbb{Z}$, and we say that E does not have complex multiplication (CM). When $\mathbb{Z} \subsetneq End(E)$ we say that E has CM.

Introduction: elliptic curves.

Example: The elliptic curve $E: y^2 = x^3 + x$ that corresponds to the lattice generated by $\{1, i\}$ has an extra endomorphism that we call i because $i^2 = -1$.

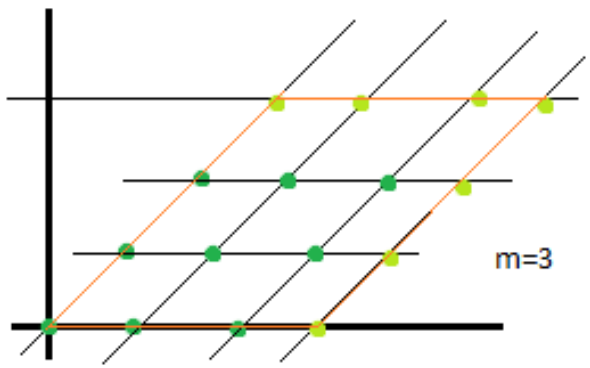


That endomorphism is a 90^o rotation.
Thus, E has CM and in fact, $End(E) \simeq \mathbb{Z}[i]$.

Introduction: The Tate module.

Fix an integer $m \in \mathbb{Z}$ and consider the points of order m, that is, such that $m \cdot Q = O$. We denote this set by $E[m]$, and we have that

$$E[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$



Now, given a prime number l we define the $l-$adic Tate module as:

$$T_l(E) := \varprojlim E[l^n] \simeq \mathbb{Z}_l \times \mathbb{Z}_l.$$

So, $T_l(E)$ is the "union" of all the points of order a power of l.

Introduction: The Frobenius endomorphism.

We also define the $2-$dimensional $\mathbb{Q}_l-$vector space:

$$V_l(E) := T_l(E) \otimes \mathbb{Q}_l \simeq \mathbb{Q}_l \times \mathbb{Q}_l.$$

Fix another prime p, we will define an endomorphism (a linear application of vector spaces):

$$Frob_p : V_l(E) \longrightarrow V_l(E).$$

Consider the abs. Galois group $G_{\mathbb{Q}} = \left\{\sigma : \bar{\mathbb{Q}} \longrightarrow \bar{\mathbb{Q}} \,\mathrm{s.t.}\, \sigma_{|\mathbb{Q}} = id.\right\}$.
For example the complex conjugation is an element in that group.
And each prime p has an associated element in $G_{\mathbb{Q}}$ called the Frobenius automorphism $Fr_p \in G_{\mathbb{Q}}$ (that I will not define).
Given a point $Q \in V_l(E)$, its coordinates are numbers in $\bar{\mathbb{Q}}$, then we define $Frob_p : V_l(E) \longrightarrow V_l(E)$ as $Q \longrightarrow^{Fr} Q$.

Introduction: The Frobenius endomorphism.

The application $Frob_p : V_l(E) \longrightarrow V_l(E)$ is linear, thus we can consider its characteristic polynomial:

$$L_p(E, T) := det(Id - T \cdot Frob_p) = 1 - a_p T + pT^2.$$

This polynomial is called the local factor of E at p, its coefficients are integer number and its two zeros are conjugated numbers of norm $p^{-1/2}$. Thus, $a_p \in \left[-2\sqrt{p}, 2\sqrt{p}\right]$.
As a remark, it is a well-known fact, that

$$|E(\mathbb{F}_p)| = 1 + p - a_p.$$

Thus, $a_p/2\sqrt{p} \in [-1, 1]$ and we can define the angle

$$\theta_p := arc\ cos\left(\frac{a_p}{2\sqrt{p}}\right).$$

The Sato-Tate conjecture.

We can think of θ_p as a random variable on the set of primes of good reduction of E taking values on $[0, \pi]$.
And now, we can state the Sato-Tate conjecture:

Conjecture *(Sato-Tate)*: If E/k does not have CM, then the angle θ_p appears to be equidistributed on $[0, \pi]$ with respect to the measure

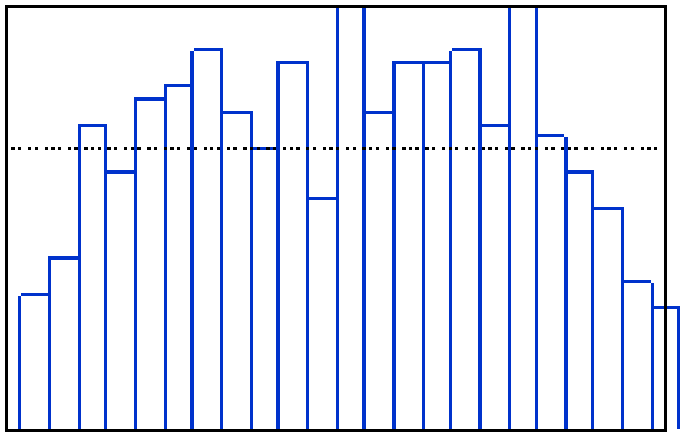
$$\frac{2}{\pi} sin^2\theta \, d\theta$$

on $[0, \pi]$.

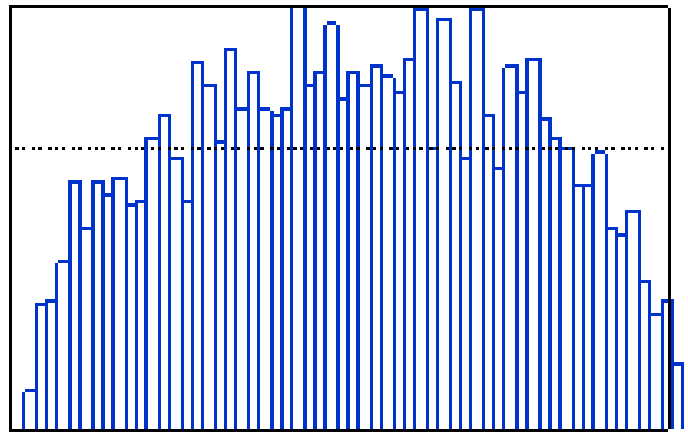
We can illustrate the conjecture with the next example, where appears the distribution of $a_1(p) = a_p/2\sqrt{p}$ for

$$E: \; y^2 = x^3 + 315149x + 271828.$$

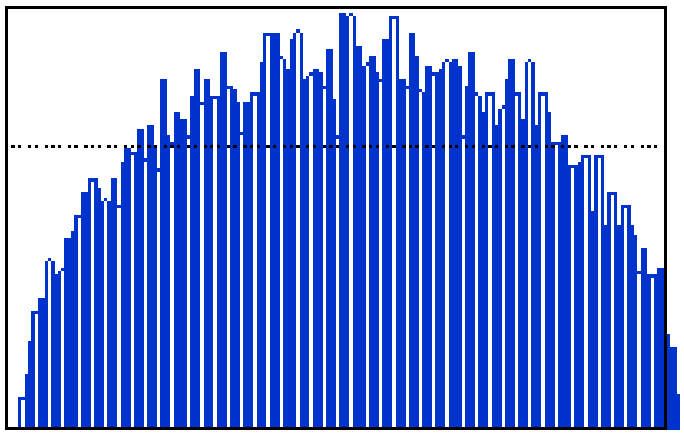
The Sato-Tate conjecture.



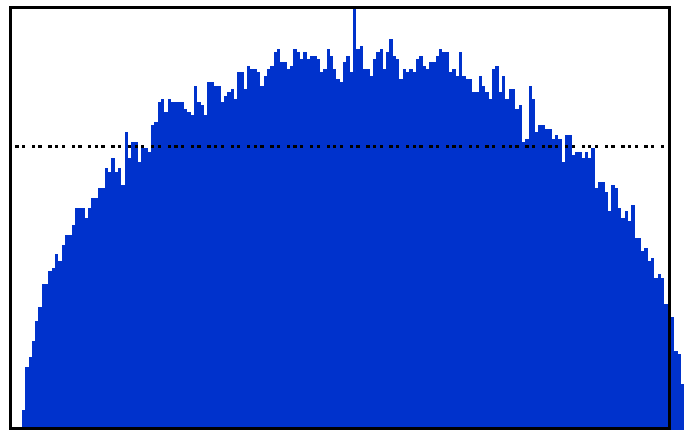
$N = 2^{12}$



$N = 2^{15}$

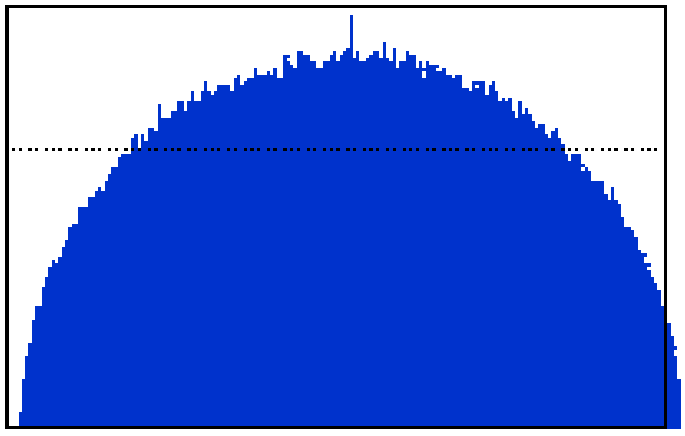


$N = 2^{18}$

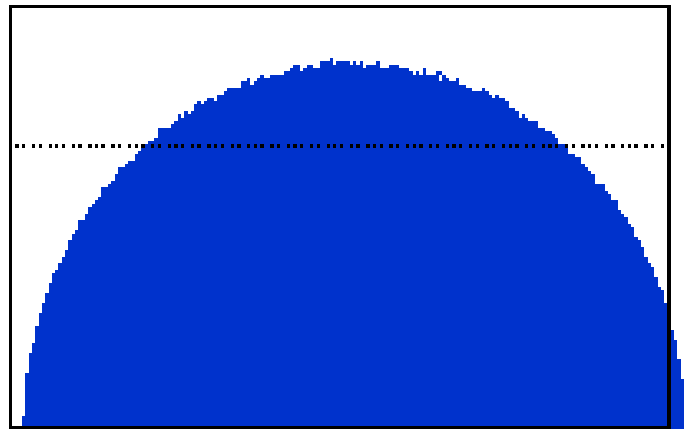


$N = 2^{21}$

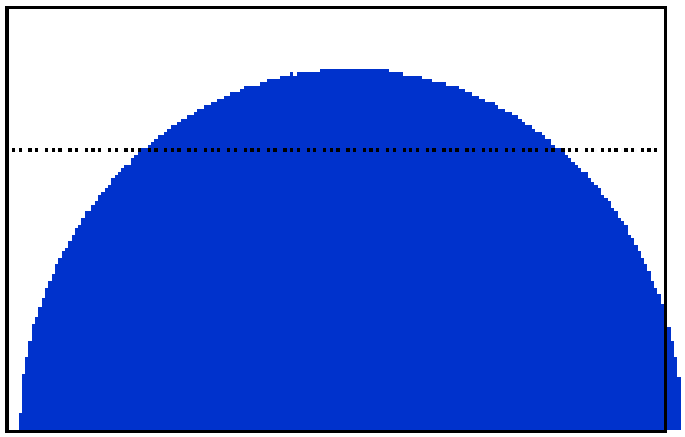
The Sato-Tate conjecture.



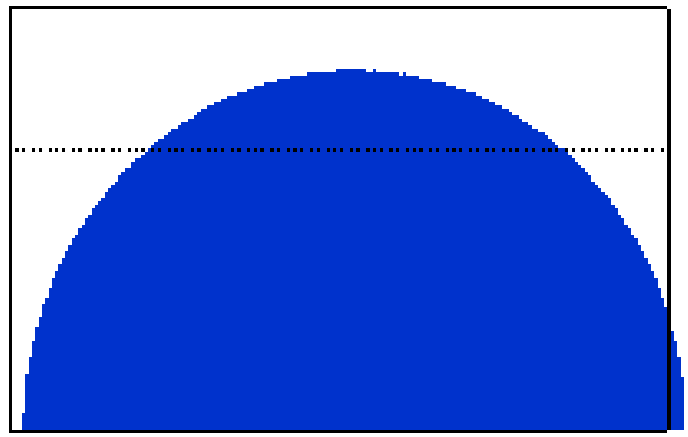
$N = 2^{24}$



$N = 2^{27}$



$N = 2^{30}$



$N = 2^{33}$

The Sato-Tate conjecture.

An equivalent formulation for the Sato-Tate conjecture is that the distribution of the polynomials $L_p(E\ T)$ corresponds to the distribution of the characteristic polynomials of a random matrix in the Lie group $US_p(2)$ (unitary simplectic matrix of size 2). More specifically, it corresponds to the Haar measure on $US_p(2)$ (a special measure defined on compact Lie groups).

If one chooses a matrix on $US_p(2)$, its eigenvalues have the form $e^{i\theta}$ and $e^{-i\theta}$, and this θ is distributed according to the measure $\frac{2}{\pi} sin^2\theta\, d\theta$ on $[0, \pi]$.

That is the one that appears in the Sato-Tate cojecture.
The Sato-Tate conjecture was recently proven when the field k is totally real.

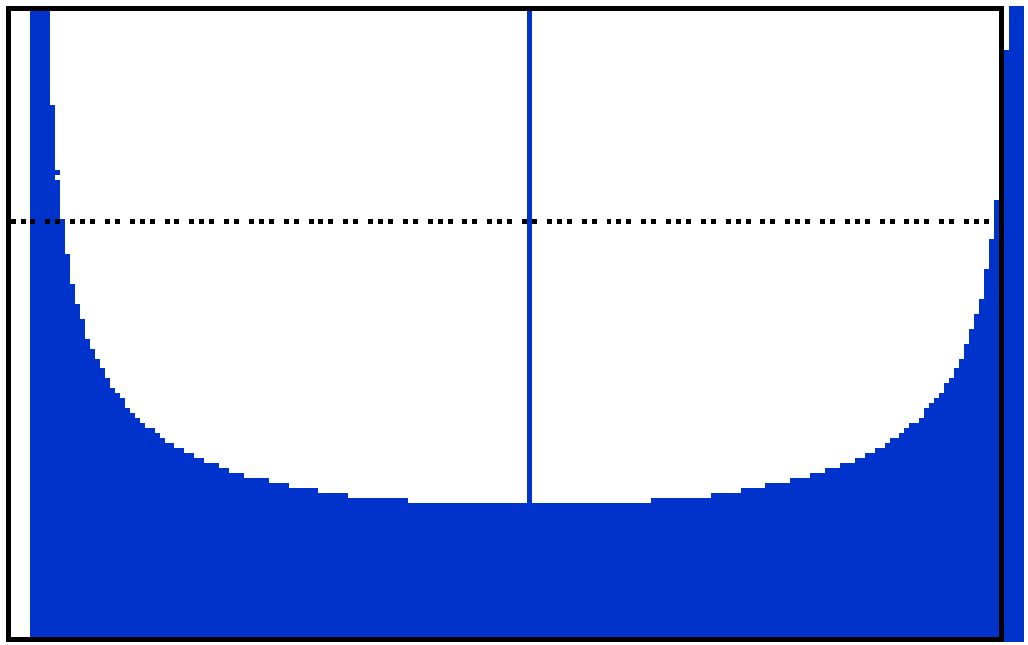
The Sato-Tate conjecture.

The next natural question is asking what happen when E has complex multiplication. In that case appear two subcases and the conjecture is proven for all k.

1. If E has CM defined over k ($E: y^2 = x^3 + x$, $k = \mathbb{Q}(i)$): then one takes the uniform measure. Or equivalently, the Haar measure on $U(1) \subseteq USp(2)$.
2. If E has CM not defined over k ($E: y^2 = x^3 + x$, $k = \mathbb{Q}$): then one takes half of the uniform measure plus half of a discrete measure concentrated at $\pi/2$. Or equivalently, the Haar measure on the normalizer group of $U(1) \subseteq USp(2)$.

The Sato-Tate conjecture.

Distribution of $a_1(p) = a_p/2\sqrt{p}$ for $E: y^2 = x^3 - 15x + 22$:



http://www-math.mit.edu/~drew/

The generalized Sato-Tate conjecture.

Once we know what happens with elliptic curves, it is natural asking what happens with abelian varieties of higher dimension.

Definition

An abelian variety A of dimension g is a projective variety of dimension g such that it has a distinguish point and a continuos group law:

$$\begin{array}{rccc} m_P: & A & \longrightarrow & A \\ & Q & \longrightarrow & P \times Q \end{array}.$$

Example: The variety $E \times E$ where E is an elliptic curve is a abelian variety of dimension 2.

The generalized Sato-Tate conjecture.

- Since we have a group law, we can define the sets $A[m]$ of points of order m. And we have $A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2g}$.
- Then we can also defined the Tate module $V_l(A) = \left(\underset{\leftarrow}{lim} A[l^n] \right) \otimes \mathbb{Q}_l \simeq \mathbb{Q}_l^{2g}$, that is a $2g-$dimensional $\mathbb{Q}_l-$vector space.
- Given a prime p of good reduction we can define an endomorphism: $Frob_p : V_l(A) \longrightarrow V_l(A)$.
- And we can consider the characteristic polynomial of this linear map:

$$L_p(A, T) = \sum_{i=1}^{2g} a_i(p) T^i.$$

The generalized Sato-Tate conjecture.

One can think of the coefficients $a_i(p)$ as random variables on the set of primes of good reduction of A taking values on

$$\left[-\sqrt{p^i}\binom{2g}{i}, \sqrt{p^i}\binom{2g}{i}\right]$$

and defined the angles:

$$\theta_i(p) := arc\,cos\left(\frac{a_i(p)}{\binom{2g}{i}\sqrt{p^i}}\right).$$

Now the question is: how are distributed these random variables on the set $[0, \pi]$?

The generalized Sato-Tate conjecture.

There is a formal (and difficult) definition of a group called the Sato-Tate group of an abelian variety: $ST_k(A)$.

Conjecture *(Generalized Sato-Tate)*: The characteristic polynomial $L_p(A, T)$ are equidistributed with respect to the Haar measure on the group $ST_k(A) \subseteq USp(2g)$.

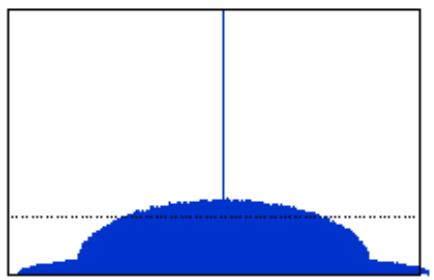
When the abelian variety has dimension 1 (elliptic curves) this conjecture is the original Sato-Tate conjecture. And, in fact we find that the Sato-Tate group is:

1. If E does not have CM: $ST_k(E) = USp(2)$.
2. If E has CM defined over k: $ST_k(E) = U(1)$
3. If E has CM not defined over k: $ST_k(E) =$ to the normalizer group of $U(1)$ in $USp(2)$.

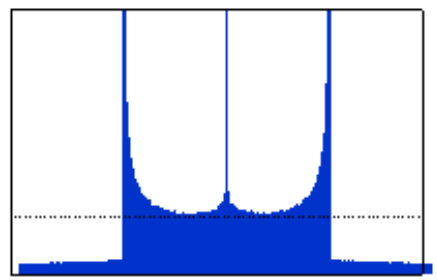
The generalized Sato-Tate conjecture.

In [FKRS11] appears a deep study about the dimension 2 case. They find all the possibilities of Sato-Tate groups for abelian varieties of dimension 2, the distributions attained for this groups and they find numerically abelian varieties that have the same distributions.

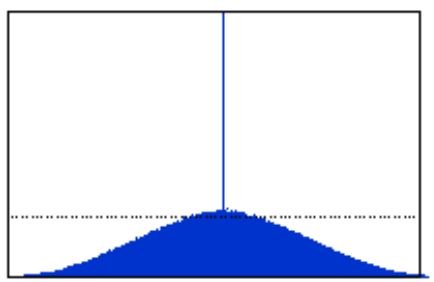
They find 52 different distributions.



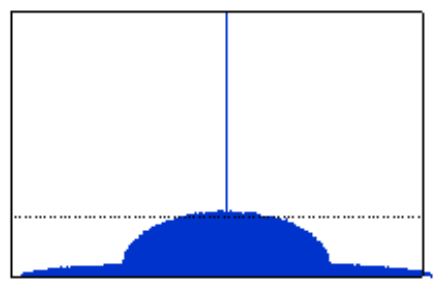
#7



#8



#9



#10

The generalized Sato-Tate conjecture.

Now, I am working in the dimension 3 case. I am considering a small family of abelian varieties and for each variety in that family I am computing:

1. The distribution of the polynomials $L_p(A, T)$.
2. The group $ST_k(A)$.
3. The distribution on the groups $ST_k(A)$.

And I am checking that both distribution coincide. In that way I am proving the Sato-Tate conjecture for this special family. By the moment, I have found more than 15 different distributions.

Bibliography.

- [BK11]: Banaszak G., Kedlaya K.: "An algebraic Sato-Tate group and Sato-Tate conjecture", preprint.
- [Fit11]: Fité F., e-mail correspondence Sep11-Nov11.
- [FKRS11]: Fité F., Kedlaya K., Rotger V., Shuterland A.: "Sato-Tate distribution and Galois endomorphism modules in genus 2", preprint.
- [KS09]: Kedalya K., Shuterland A.: "Hypereliptic curves, L-polynomials and random matrices", Contemporary Mathematics (AMS) v.487, 2009.
- [Lor10]: Lorenzo E.: "Torcimientos de cuárticas planas lisas", master thesis, 2010.