Sato-Tate and notions of generality

David Kohel
Institut de Mathématiques de Luminy

Oberwolfach, 19 July 2011

Explicit point counting and cryptography

The original motivation for this talk is to understand the properties of RM curves with a view towards cryptography. For example, in the family considered by Tautz, Top, and Verberkmoes:

$$\mathcal{C} : y^2 = x^5 - 5x^3 + 5x + t,$$

over $\mathbb{A}^1 = \mathrm{Spec}(\mathbb{Q}[t])$, the fibers have Jacobians with real multiplication by $\mathbb{Z}[\phi] = \mathbb{Z}[(1+\sqrt{5})/2]$. Moreover, the real endomorphism ϕ is explicitly computable (K. & Smith), and with Gaudry and Smith we developed:

Theorem (Gaudry,K. & Smith)

There exists an algorithm for the point counting problem in a family of genus 2 curves with efficiently computable RM of class number 1, whose complexity is in $\widetilde{O}((\log q)^5)$.

Explicit point counting example

Let $q = 2^{512} + 1273$ (prime), and consider the curve over $\mathbb{F}_q$ from the family $\mathcal{C}$, specialized at (random)

$$\begin{aligned} t = \; & 29085666333787272437998261129919801749 \\ & 74533003680957762232569868073752702720 \\ & 14471477919882845604269700820270816721 \\ & 53243497592108531656059083265912235127 8. \end{aligned}$$

Let π be the Frobenius endomorphism, and set $\pi + \bar{\pi} = m + n\phi$, so $a_1 = 2m + n$ and $a_2 = (a_1^2 - n^2 5)/4 = m^2 + mn - n^2$, where

$$\chi(t) = x^4 - a_1 x^3 - (a_2 + 2q)x^2 - a_1 q x + q^2.$$

The values of m and n for this curve are

$$\begin{aligned} m = & -33785412452026953770179131338679489596 \\ & 56475470770107628408426925155470967294, \\ n = & -37786020778198256317368570028183842800 \\ & 47374979214207223099354900103509328849 2. \end{aligned}$$

Cryptographic notions of generality

We can compute zeta functions as efficiently as for elliptic curves (and even better — unconditionally), but can we in good faith recommend the use of such curves for cryptographic applications?

Q1: In what way is an RM family special?

Q2: How special is the (one dimensional) family of Tautz, Top, and Verberkmoes inside of the (two dimensional) moduli space of genus 2 curves with RM by $\mathbb{Z}[(1+\sqrt{5})/2]$?

Motivation: Serre's talk at AGCT in Luminy, 2011, explaining and motivating work of Kedlaya and Sutherland for higher dimensional Sato–Tate conjectures (particularly $g = 2$).

First we recall some standard families of interest.

Examples of families of curves

We consider $\mathcal{C} \to S$ a family of curves, such that each fiber over a closed point x of S is a curve $C/k = \mathbb{F}_q$.

Examples. Elliptic curves.

1. $\mathcal{E} : y^2 = x^3 + ax + b$ over S, where

$$S = \mathrm{Spec}(\mathbb{Z}[a, b, \frac{1}{6ab}]) \subset \mathbb{A}^2/\mathbb{Z}[\frac{1}{6}],$$

a family of dimension 3.

2. $\mathcal{E} : y^2 + xy = x^3 + ax^2 + b$ over S, where

$$S = \mathrm{Spec}(\mathbb{F}_2[a, b, \frac{1}{b}]) \subset \mathbb{A}^2/\mathbb{F}_2,$$

a family of dimension 2.

3. $\mathcal{E} : y^2 = x^3 + x^2 - 3x + 1$ over $S = \mathrm{Spec}(\mathbb{Z}[\frac{1}{2}])$, a CM family with endomorphism ring $\mathbb{Z}[\sqrt{-2}]$, of dimension 1.

Examples of families of genus 2

Examples. Genus 2 curves.

4. $\mathcal{C} : y^2 = x^5 + a_3x^3 + a_2x^2 + a_1x + a_0$, over

$$S = \mathrm{Spec}(\mathbb{Z}[a_0, \ldots, a_3][\frac{1}{\Delta}]) \subset \mathbb{A}^4/\mathbb{Z}[\frac{1}{10}],$$

a 5-dimensional family.

5. $\mathcal{C} : y^2 = x^5 + 5x^3 + 5x + t$, the RM family of Tautz, Top, and Verberkmoes, over

$$S = \mathrm{Spec}(\mathbb{Z}[t, \frac{1}{10(t^2+4)}]) \subset \mathbb{A}^1/\mathbb{Z}[\frac{1}{10}],$$

a 2-dimensional family with real multiplication by $\mathbb{Z}[(1+\sqrt{5})/2]$.

6. $\mathcal{C} : y^2 = x^5 + 1$, a CM family over $S = \mathrm{Spec}(\mathbb{Z}[\frac{1}{10}])$.

Notions of generality in cryptography

We address the question: "What is special about special curves?" Here we distinguish certain geometric and arithmetic properties.

Geometric speciality. If $\mathcal{C} \to S$ is a family (of genus g curves), what is the induced image $S \to \mathcal{X}$ in the moduli space (in $\mathcal{M}_g$)?

Arithmetic speciality. Here we distiguish the (local) level structure and the (global or geometric) Galois distributions.

a. What level structure is fixed by the family? — Is there an exceptional N such that the Galois representation

$$\bar{\rho}_N : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_{2g}(\mathbb{Z}/N\mathbb{Z})$$

is smaller than expected?

b. What is the image of the Galois action on the Tate module?

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_\ell(J)) \cong \mathrm{GL}_{2g}(\mathbb{Z}_\ell).$$

Frobenius angles and normalized traces

Let $E/\mathbb{Q}$ be an elliptic curve, with discriminant Δ, viewed as a scheme over $S = \mathrm{Spec}(\mathbb{Z}[\frac{1}{\Delta}])$. The Sato–Tate conjecture concerns the distribution of the Frobenius *angles* at primes p.

For each p, let $\pi = \pi_p$ be the Frobenius endomorphism on $\bar{E}/\mathbb{F}_p$ and

$$\chi(T) = T^2 - a_p T + p$$

its characteristic polynomial of Frobenius. Set t_p equal to the normalized Frobenius trace

$$t_p = a_p/\sqrt{p},$$

and denote by θ_p in $[0, \pi]$ the Frobenius angle, defined by $t_p = 2\cos(\theta_p)$. We set $\mu_p = e^{i\theta_p}$ (the unit Frobenius), and

$$\widetilde{\chi}(T) = T^2 - t_p T + 1 = (T - \mu_p)(T - \bar{\mu}_p).$$

Sato–Tate Conjecture

Sato–Tate Conjecture. Suppose that $E/\mathbb{Q}$ is a non-CM elliptic curve. For $[\alpha, \beta] \subset [0, \pi]$,

$$\lim_{N\to\infty} \frac{|\{p \leq N \mid \alpha \leq \theta_p \leq \beta\}|}{|\{p \leq N\}|} = \int_\alpha^\beta \frac{2\sin^2(\theta)}{\pi} d\theta,$$

or equivalently for $[a, b] \subset [-2, 2]$,

$$\lim_{N\to\infty} \frac{|\{p \leq N \mid a \leq t_p \leq b\}|}{|\{p \leq N\}|} = \int_a^b \frac{\sqrt{4-t^2}}{2\pi} dt.$$

The analogous distributions for CM elliptic curves is classical:

$$\lim_{N\to\infty} \frac{|\{p \leq N \mid \alpha \leq \theta_p \leq \beta\}|}{|\{p \leq N\}|} = \frac{1}{\pi}\int_\alpha^\beta d\theta = \frac{\beta-\alpha}{\pi}.$$

Sato–Tate distributions

We call the distributions $\mu(\theta)$ on $[0,\pi]$ and $\mu(t)$ and $[-2,2]$, defined by

$$\mu(\theta) = \frac{2\sin^2(\theta)}{\pi} d\theta \quad \text{and} \quad \mu(t) = \frac{\sqrt{4-t^2}}{2\pi} dt,$$

the *Sato–Tate distributions* for non-CM E/S.

For a CM curve E/S, the analogous Sato–Tate distributions are classical:

$$\mu(\theta) = \frac{1}{2}\left(\frac{d\theta}{\pi} + \delta_{\pi/2}\right) \quad \text{and} \quad \mu(t) = \frac{1}{2}\left(\frac{dt}{\pi\sqrt{4-t^2}} + \delta_0\right),$$

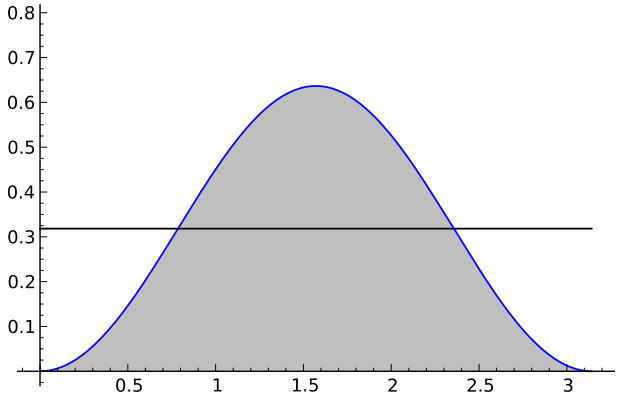
where δ_x is the Dirac distribution. Restricting to the 50% of ordinary primes, we have distributions

$$\mu_0(\theta) = \frac{d\theta}{\pi} \quad \text{and} \quad \mu_0(t) = \frac{dt}{\pi\sqrt{4-t^2}}.$$

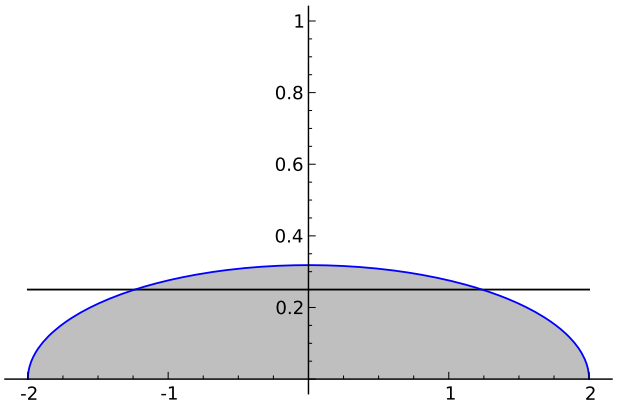
Sato–Tate plots

Generic curve

$$\frac{2\sin^2(\theta)}{\pi}d\theta$$

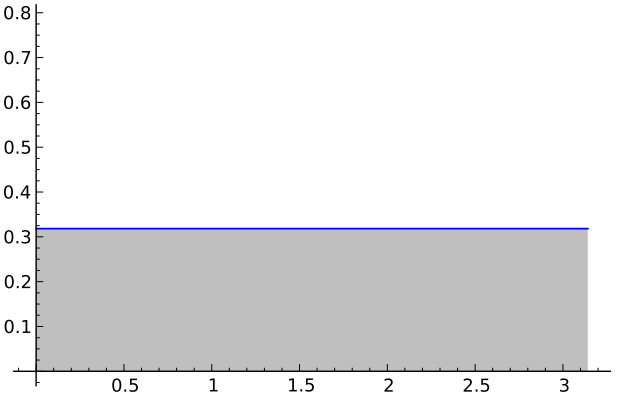


$$\frac{\sqrt{4-t^2}}{2\pi}dt$$

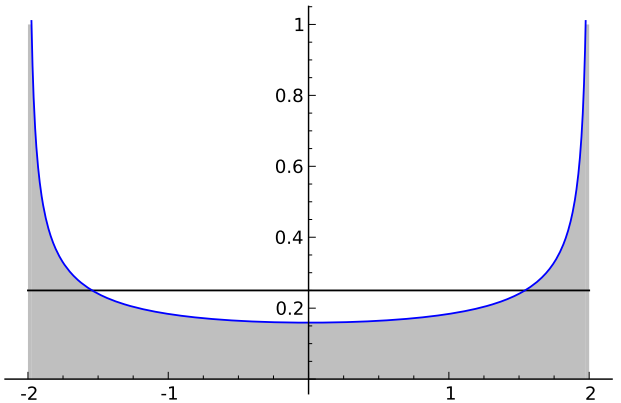


CM curve

$$\frac{1}{\pi}d\theta$$



$$\frac{1}{\pi\sqrt{4-t^2}}dt$$



Galois representation groups

Where do these come from?

The CM case is easy: the ordinary Frobenius endomorphisms π_p lie in a CM field K and their unit normalizations μ_p in $K \otimes \mathbb{R} \cong \mathbb{R}^2$ are uniformly distributed around the unit circle

$$\mathrm{SO}(2) = \left\{ \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \right\} \cong S^1.$$

The supersingular Frobenius endomorphisms lie in a coset of the normalizer in $\mathrm{USp}(2) = \mathrm{SU}(2)$:

$$\mathrm{SO}(2) \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \left\{ \begin{pmatrix} i\cos(\theta) & i\sin(\theta) \\ i\sin(\theta) & -i\cos(\theta) \end{pmatrix} \right\}.$$

The ordinary distribution $d\theta/\pi$ arises from the uniform distribution on the unit circle (hence of $\theta \in [0, \pi]$); the supersingular coset has uniform trace zero.

Galois representation groups

The generic normalized Frobenius representations lie in

$$\mathrm{USp}(2) = \mathrm{SU}(2) = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \;\middle|\; |\alpha|^2 + |\beta|^2 = 1 \right\}.$$

This group is isomorphic to the unit quaternions:

$$(\mathbb{H}^*)^1 = \{a + bi + (c + di)j \mid a^2 + b^2 + c^2 + d^2 = 1\} \cong S^3$$

on identifying $\alpha = a + bi$ and $\beta = c + di$. The Sato–Tate distribution arises from the Haar measure on $\mathrm{SU}(2)$. Setting

$$\begin{aligned} \alpha = a + bi &= \cos(\rho)(\cos(\sigma) + i\sin(\sigma)), \\ \beta = c + di &= \sin(\rho)(\cos(\tau) + i\sin(\tau)), \end{aligned}$$

the conjugacy class (on which trace is a class function) is

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \sim \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}$$

with trace $2\cos(\theta) = 2\cos(\rho)\cos(\sigma)$.

Alternative Sato–Tate domains

Noting that $D = a_p^2 - 4p$ is the discriminant of the ring $\mathbb{Z}[\pi]$, in the case that $E/\mathbb{Q}$ has CM by an order $\mathcal{O}$, we have $D = n^2 D_{\mathcal{O}}$ for some integer n.

In order to study the distribution of Frobenius discriminants, this motivates setting

$$u^2 = \frac{D}{p} = t^2 - 4 \left(= \frac{n^2 D_{\mathcal{O}}}{p} \right)$$

and considering the Frobenius distribution in terms of u.

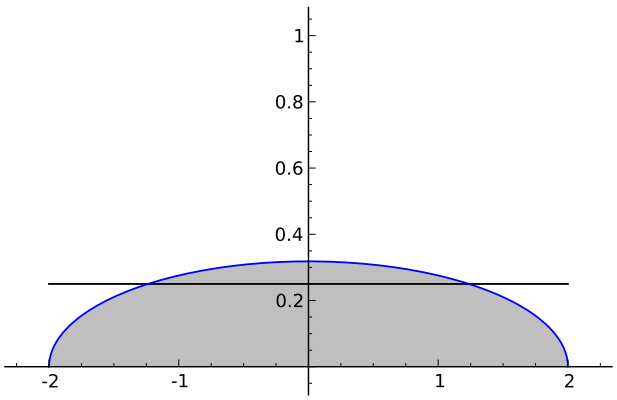
In the non-CM case, the coordinate $u = \sqrt{D/p}$ measures the distribution of normalized square root discriminants (of $\mathbb{Z}[\pi]$).

In the CM case, $\sqrt{D_{\mathcal{O}}}$ remains fixed, and u gives information about the normalized conductors $n/\sqrt{p} = [\mathcal{O} : \mathbb{Z}[\pi]]/\sqrt{p}$ at ordinary primes.

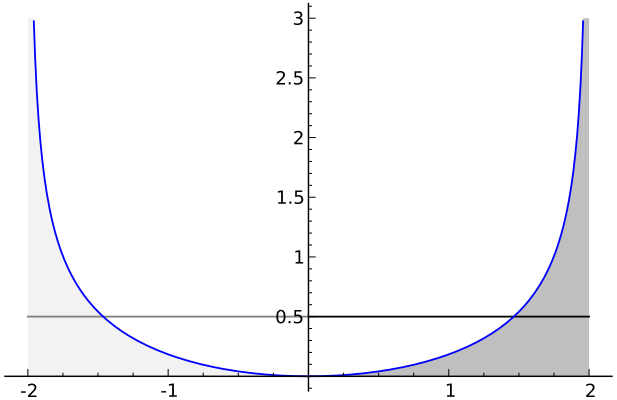
Sato–Tate plots

Generic curve

$$\frac{\sqrt{4-t^2}}{2\pi}dt$$

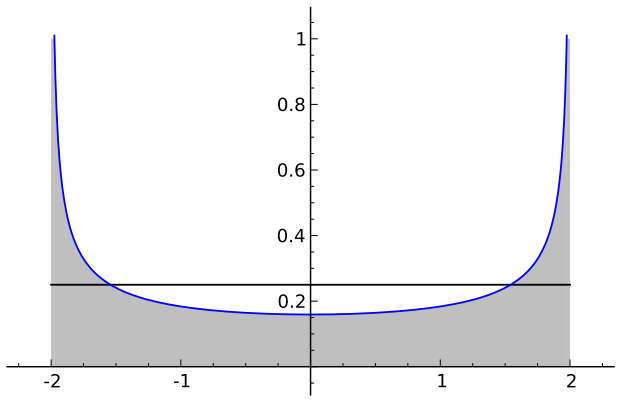


$$\frac{u^2}{\pi\sqrt{4-u^2}}du$$

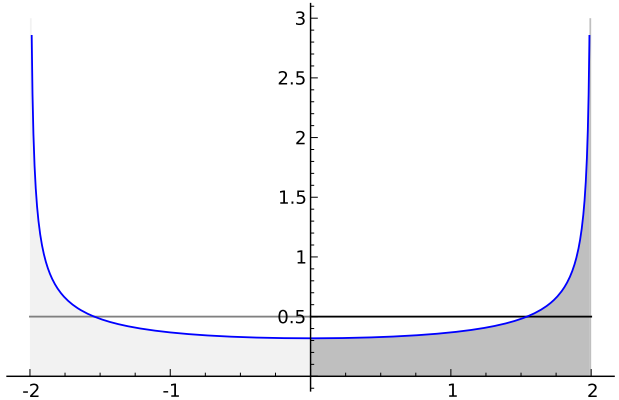


CM curve

$$\frac{1}{\pi\sqrt{4-t^2}}dt$$



$$\frac{2}{\pi\sqrt{4-u^2}}du$$



Generalized Sato–Tate framework

Conjecturally, there exists a compact subgroup H of $\mathrm{USp}(2g)$, with connected component H_0,

$$H_0 \triangleleft H \subseteq \mathrm{USp}(2g),$$

such that the unit Frobenius elements are equidistributed in H.

Remark. The partition into the cosets in $G = H/H_0$ is explained by the Chebotarev density theorem. In general one has a decomposition

$$\mu = \frac{|C_0|}{|G|}\mu_0 + \frac{|C_1|}{|G|}\mu_1 + \cdots \frac{|C_r|}{|G|}\mu_r,$$

where $C_0, C_1, \ldots C_r$ are the conjugacy classes of G.

Here we focus on the distribution $\mu = \mu_0$ in the principle coset H_0 (a vast simplification), and the case $g = 2$ (see work of Kedlaya & Sutherland). We also simplify (experimentally and theoretically) by averaging over fibres over a base scheme.

Sato–Tate domains

Let $C/\mathbb{F}_q$ be a curve and $\chi(T)$ its Frobenius characteristic polynomial

$$\chi(T) = T^{2g} - a_1 T^{2g-1} + \cdots - a_1 q^{g-1} T + q^g.$$

and define the unit Frobenius characteristic polynomial by

$$\begin{aligned}\widetilde{\chi}(T) = \frac{\chi(\sqrt{q}T)}{q^g} &= T^{2g} - s_1 T^{2g-1} + \cdots - s_1 T + 1 \\ &= \prod_{j=1}^{g} (T^2 - t_j T + 1).\end{aligned}$$

By the Weil conjectures, the roots α_j of $\chi(T)$ satisfy $|\alpha_j| = \sqrt{q}$, so we write

$$\mu_j = \frac{\alpha_j}{\sqrt{q}} = e^{i\theta_j},$$

and $t_j = \mu_j + \bar{\mu}_j = 2\cos(\theta_j)$, where $\mu_j \bar{\mu}_j = 1$.

Domains for Sato–Tate distributions

Rather than defining s_j to be the j-th coefficient of $\widetilde{\chi}(T)$, we let the s_j be the normalized symmetric products not including any terms (as factors of summands) of the form $\mu_j\bar{\mu}_j(=1)$. These are the coefficients of the real Weil polynomial. Thus for $g = 2$

$$\widetilde{\chi}(T) = T^4 - s_1T^3 + (s_2 + 2)T^2 - s_1T + 1,$$

and for $g = 3$:

$$\widetilde{\chi}(T) = T^6 - s_1T^5 + (s_2 + 3)T^4 - (s_3 + 2s_1)T^3 + \cdots$$

A naïve application of the Weil bounds gives bounds on the symmetric sums and s_j, equal to their respective number of monomials:

$$|s_j| \le 2^j \binom{g}{j} \text{ vs. } |\mathrm{sym}_j(\{\mu_1, \bar{\mu}_1, \ldots, \mu_g, \bar{\mu}_g\})| \le \binom{2g}{j}.$$

Domains for Sato–Tate distributions

In higher dimension, the real subring $\mathbb{Z}[\pi + \bar{\pi}]$ is a nontrivial subring of $\mathbb{Z}[\pi, \bar{\pi}]$, and hence

$$\operatorname{disc}(\mathbb{Z}[\pi, \bar{\pi}]) = D_+^2 D_-,$$

where $D_+ = \operatorname{disc}(\mathbb{Z}[\pi + \bar{\pi}])$, and for $g = 2$ we have

$$D_+ = a_1^2 - 4a_2 \text{ and } D_- = -((a_2 - 4q)^2 - 4q(a_1^2 - 4a_2)).$$

where D_- is the norm of the relative discriminant $\mathbb{Z}[\pi, \bar{\pi}]/\mathbb{Z}[\pi, \bar{\pi}]$.

For a family with fixed RM order R, we have $\mathbb{Z}[\pi + \bar{\pi}] \subset R$ of finite index (on any fiber of simple ordinary reduction), hence

$$D_+ = n_+^2 D_R,$$

and additionally for a subfamily with CM by $\mathcal{O}/R$ we have

$$D_- = n_-^2 D_1,$$

where D_1 is the norm of the relative discriminant of $\mathcal{O}/R$.

Domains for Sato–Tate distributions

Generic: $H_0 = H = \mathrm{USp}(4)$

$$\mu_0 = \frac{8(\cos(\theta_1) - \cos(\theta_2))^2 \sin^2(\theta_1) \sin^2(\theta_2)}{\pi^2} d\theta_1 d\theta_2$$

RM: $H_0 = \mathrm{SU}(2) \times \mathrm{SU}(2)$

$$\mu_0 = \frac{4 \sin^2(\theta_1) \sin^2(\theta_2)}{\pi^2} d\theta_1 d\theta_2$$

CM: $H_0 = \mathrm{SO}(2) \times \mathrm{SO}(2)$

$$\mu_0 = \frac{d\theta_1 d\theta_2}{\pi^2}$$

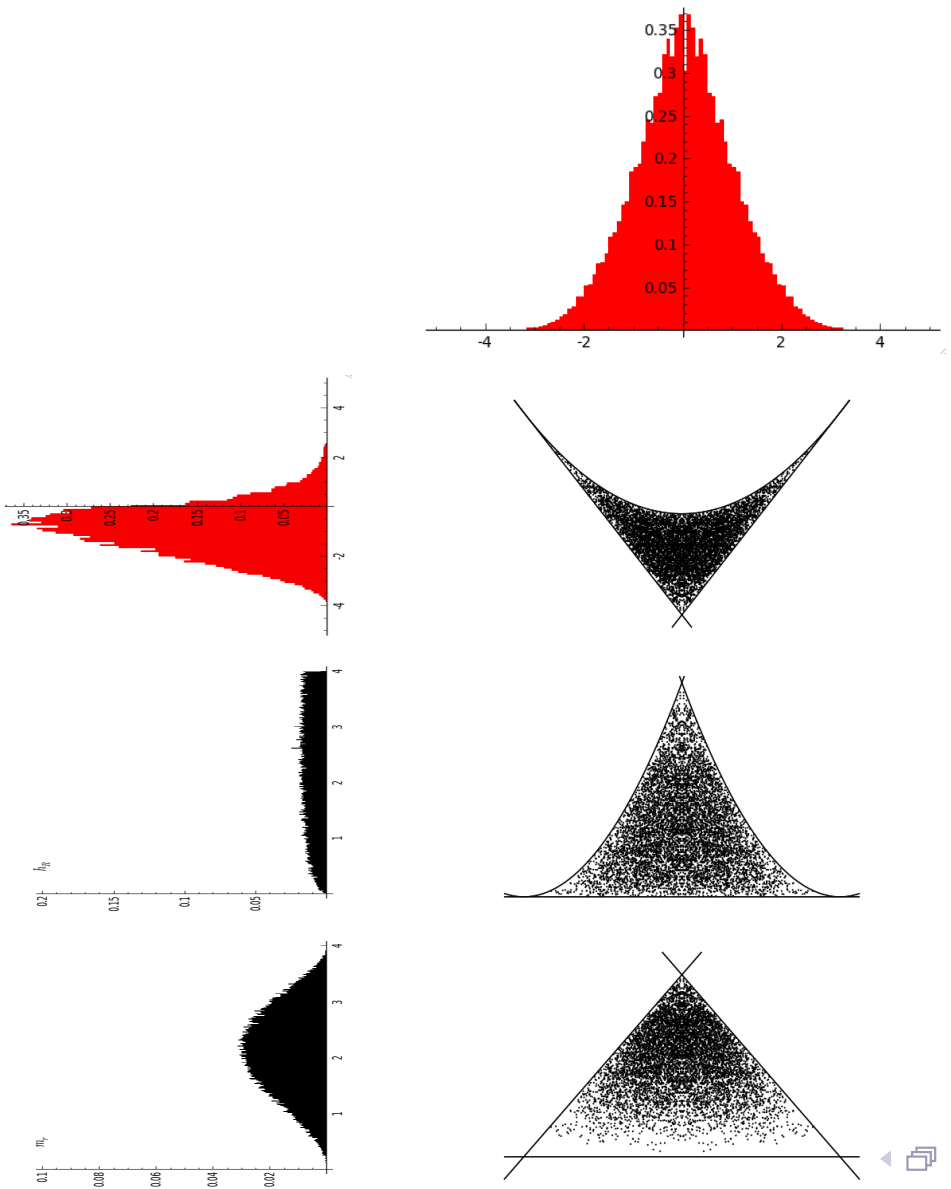
These induced well-defined distributions in terms of the spaces

- (s_1, s_2),
- $(s_1, D_+ = s_1^2 - 4s_2)$,
- $(s_1, \sqrt{s_1^2 - 4s_2})$

graphical representations follow . . .

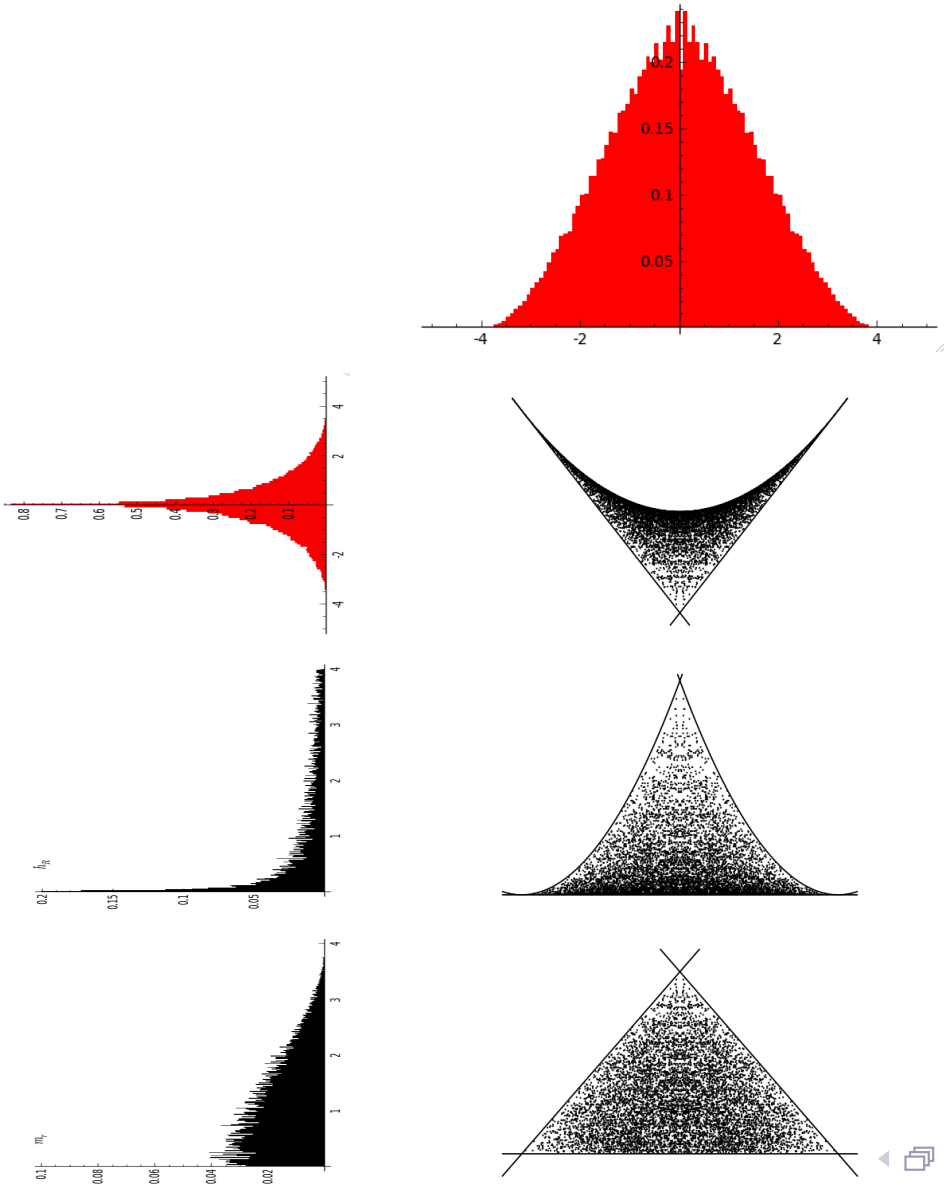
Experimental Sato–Tate: generic family

Generic:



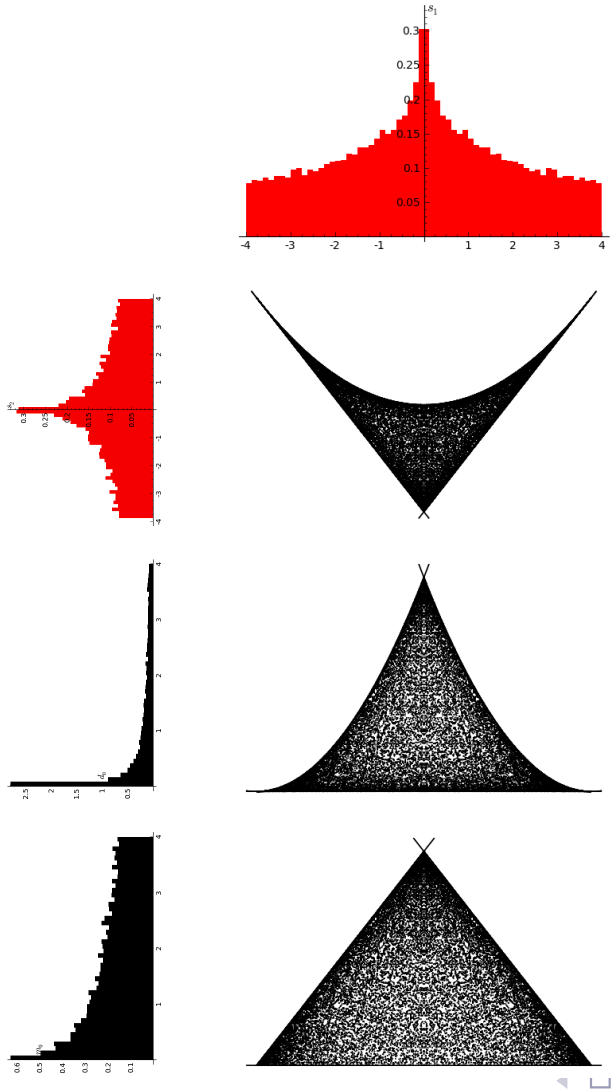
Experimental Sato–Tate: RM family

RM:



Experimental Sato–Tate: CM family

CM:



Conjectural Sato–Tate distributions

What are these distributions?

Note: the real and relative unit discriminants are:

$$D_+ = s_1^2 - 4s_2 \text{ and } D_- = (4 - s_1 + s_2)(4 + s_1 + s_2).$$

Generic: (up to constant scalars)

$$\sqrt{(s_1^2 - 4s_2)(4 - s_1 + s_2)(4 + s_1 + s_2)}\, ds_1 ds_2$$

RM:

$$\frac{\sqrt{(4 - s_1 + s_2)(4 + s_1 + s_2)}\, ds_1 ds_2}{\sqrt{(s_1^2 - 4s_2)}}$$

CM:

$$\frac{ds_1 ds_2}{\sqrt{(s_1^2 - 4s_2)(4 - s_1 + s_2)(4 + s_1 + s_2)}}$$