Sato-Tate in genus 2

Andrew V. Sutherland

Massachusetts Institute of Technology

March 30, 2009

joint work with Kiran Kedlaya

http://arxiv.org/abs/0803.4462

The distribution of Frobenius traces

Let $E/\mathbb{Q}$ be an elliptic curve (non-singular).
Let $t_p = \#E(\mathbb{F}_p) - p + 1$ denote the trace of Frobenius.

Consider the distribution of

$$x_p = t_p/\sqrt{p} \in [-2, 2]$$

as $p \leq N$ varies over primes of good reduction.

What happens as $N \to \infty$?

Two trace distributions for $E/\mathbb{Q}$

Curves with complex multiplication

All elliptic curves with CM have the same limiting distribution.
This follows from classical results.

Conjecture (Sato-Tate)

For any elliptic curve without CM, the limiting distribution is the semicircular distribution.

Proven by Clozel, Harris, Shepherd-Baron, and Taylor (2006), provided E does not have purely additive reduction.

L-polynomials

Let $C/\mathbb{Q}$ be a smooth projective curve of genus g.
The zeta function of C is defined by

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

where $N_k = \#C/\mathbb{F}_{p^k}$. It is a rational function of the form

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

where $L_p(T)$ has degree $2g$.

Unitarized L-polynomials

The polynomial

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

is a real symmetric polynomial whose roots lie on the unit circle.

Every such polynomial arises as the characteristic polynomial $\chi(T)$ of some matrix in $USp(2g)$ ($2g \times 2g$ complex matrices that are both unitary and symplectic).

Note that the coefficients satisfy $|a_i| \leq \binom{2g}{i}$.

The Katz-Sarnak model

Conjecture (Katz-Sarnak)

For a typical curve of genus g, the distribution of $\bar{L}_p(T)$ converges to the distribution of $\chi(T)$ in $USp(2g)$.

"Typical" means curves with large Galois image.
For $g = 2$ this is equivalent to $\mathrm{End}(C) \cong \mathbb{Z}$ (i.e. no CM).

This conjecture is known to be true "on average" for universal families of hyperelliptic curves (including all genus 2 curves).

The Haar measure on $USp(2g)$

Let $e^{\pm i\theta_1}, \ldots, e^{\pm i\theta_g}$ denote the eigenvalues of a random matrix (conjugacy class) in $USp(2g)$. The Weyl integration formula yields the Haar measure

$$\mu = \frac{1}{g!}\Bigl(\prod_{j<k}(2\cos\theta_j - 2\cos\theta_k)\Bigr)^2 \prod_j \left(\frac{2}{\pi}\sin^2\theta_j d\theta_j\right).$$

In genus 1 we have $USp(2) = SU(2)$ and $\mu = \frac{2}{\pi}\sin^2\theta d\theta$, which is the Sato-Tate distribution.

Note that $-a_1 = \sum 2\cos\theta_j$ is the trace.

Improving resolution

Methods of computing $\bar{L}_p(T)$ in genus 2:

1. point counting: $\tilde{O}(p^2)$.
2. group computation: $\tilde{O}(p^{3/4})$.
3. p-adic methods: $\tilde{O}(p^{1/2})$.
4. ℓ-adic methods: $\tilde{O}(1)$.

Currently (4) is impractical and (3) is the fastest for large p.
However, for the feasible range of $p \leq N$, (2) is the best choice.

Computing L-series of hyperelliptic curves, ANTS VIII, 2008, KS.

Moment sequences

The *moment sequence* of a random variable X is

$$M[X] = (\,\mathrm{E}[X^0], \mathrm{E}[X^1], \mathrm{E}[X^2], \ldots).$$

Provided is X is suitably bounded, $M[X]$ exists and uniquely determines the distribution of X.

Moment sequences

The *moment sequence* of a random variable X is

$$M[X] = (\mathrm{E}[X^0], \mathrm{E}[X^1], \mathrm{E}[X^2], \ldots).$$

Provided is X is suitably bounded, $M[X]$ exists and uniquely determines the distribution of X.

Given sample values $x_1, \ldots, x_N$ for X, the nth *moment statistic* is the mean of x_i^n. It converges to $\mathrm{E}[X^n]$ as $N \to \infty$.

Moment sequences

The *moment sequence* of a random variable X is

$$M[X] = (\mathrm{E}[X^0], \mathrm{E}[X^1], \mathrm{E}[X^2], \ldots).$$

Provided is X is suitably bounded, $M[X]$ exists and uniquely determines the distribution of X.

Given sample values $x_1, \ldots, x_N$ for X, the nth *moment statistic* is the mean of x_i^n. It converges to $\mathrm{E}[X^n]$ as $N \to \infty$.

If X is a symmetric integer polynomial of the eigenvalues of a random matrix in $USp(2g)$ (e.g. the trace), then $M[X]$ is an *integer* sequence (follows from representation theory).

The typical trace moment sequence in genus 1

Using the measure μ in genus 1, for $t = -a_1$ we have

$$E[t^n] = \frac{2}{\pi}\int_0^{\pi}(2\cos\theta)^n \sin^2\theta d\theta.$$

The typical trace moment sequence in genus 1

Using the measure μ in genus 1, for $t = -a_1$ we have

$$E[t^n] = \frac{2}{\pi}\int_0^{\pi}(2\cos\theta)^n \sin^2\theta d\theta.$$

This is zero when n is odd, and for $n = 2m$ we obtain

$$E[t^{2m}] = \frac{1}{2m+1}\binom{2m}{m}.$$

and therefore

$$M[t] = (1, 0, 1, 0, 2, 0, 5, 0, 14, 0, 42, 0, 132, \ldots).$$

This is sequence A126120 in the OEIS.

The typical trace moment sequence in genus $g > 1$

A similar computation in genus 2 yields

$$M[t] = (1, 0, 1, 0, 3, 0, 14, 0, 84, 0, 594, \ldots),$$

which is sequence A138349, and in genus 3 we have

$$M[t] = (1, 0, 1, 0, 3, 0, 15, 0, 104, 0, 909, \ldots),$$

which is sequence A138540.

The *n*th moment of the trace in genus g is equal to the number of returning lattice paths in $\mathbb{Z}^g$ satisfying $x_1 \geq x_2 \geq \cdots \geq x_g \geq 0$ at ever step (a Weyl chamber) [Grabiner-Magyar].

The trace moment sequence of a CM curve in genus 1

For an elliptic curve with CM we find that

$$E[t^{2m}] = \frac{1}{2}\binom{2m}{m}, \qquad \text{for } m > 0$$

yielding the moment sequence

$$M[t] = (1, 0, 1, 0, 3, 0, 10, 0, 35, 0, 126, 0, \ldots),$$

whose even entries are A008828.

Where does this fit in a random matrix model?

Exceptional distributions in genus 2.

We surveyed the distributions of the genus 2 curves:

$$y^2 = x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0,$$

$$y^2 = b^6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0,$$

with integer coefficients $|c_i| \leq 64$ and $|b_i| \leq 16$.
More than 10^{10} curves were tested.

We found over 30,000 non-isomorphic curves with exceptional distributions, about 20 distinct shapes.

All apparently converge to integer moment sequences.

Genus 2 exceptional distributions (one example)

For a hyperelliptic curve whose Jacobian is the direct product of two elliptic curves, we compute $M[t] = M[t_1 + t_2]$ via

$$\mathrm{E}[(t_1 + t_2)^n] = \sum \binom{n}{i} \mathrm{E}[t_1^i]\mathrm{E}[t_2^{n-i}].$$

For example, using

$$M[t_1] = (1, 0, 1, 0, 2, 0, 5, 0, 14, 0, 42, 0, 132, \ldots),$$
$$M[t_2] = (1, 0, 1, 0, 3, 0, 10, 0, 35, 0, 126, 0, 462, \ldots),$$

we obtain $A138551$,

$$M[t] = (1, 0, 2, 0, 11, 0, 90, 0, 889, 0, 9723, \ldots).$$

Analyzing the data in genus 2

Some survey highlights:

- At least 19 distinct distributions were found. This is exceeds the possibilities for $\mathrm{End}(C)$, $\mathrm{Aut}(C)$, or $\mathrm{MT}(C)$.
- Some obviously correspond to split Jacobians, but many do not. The same distribution can arise for curves with split and simple Jacobians.
- Some have positive zero-trace densities, some do not.
- The a_1 distribution appears to determine the a_2 distribution.

Random matrix subgroup model

Conjecture

For a genus g curve C, the distribution of $\bar{L}_p(T)$ converges to the distribution of $\chi(T)$ in some infinite compact subgroup $H \subseteq USp(2g)$.

Equality holds if and only if C has large Galois image.

Representations of genus 1 distributions

The Sato-Tate distribution has $H = USp(2g)$, the typical case.

For CM curves, consider the subgroup of $USp(2) = SU(2)$:

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

This is a compact group (the normalizer of $SO(2)$ in $SU(2)$).

Its Haar measure yields the desired moment sequence.

Candidate subgroups in genus 2

In genus 2 we have subgroups analogous to the two in genus 1.

Additionally, we consider embeddings of the two genus 1 groups as block diagonal matrices, where we allow "twisting" by *k*th roots of unity that lie in a quadratic extension of $\mathbb{Q}$ (so k is 1,2,3,4, or 6).

This restriction corresponds to the requirement that $L_p(T)$ have integer coefficients (and yields integer moment sequences).

See `http://arxiv.org/abs/0803.4462` for details.

A conjecturally complete classification in genus 2

This model yields a total of 24 candidates in addition to $USp(4)$ itself. Every distribution found in our survey has a distribution matching one of these candidates.

Initially we found only 19 exceptional distributions, but careful examination of the survey data yielded 3 missing cases.

A conjecturally complete classification in genus 2

This model yields a total of 24 candidates in addition to $USp(4)$ itself. Every distribution found in our survey has a distribution matching one of these candidates.

Initially we found only 19 exceptional distributions, but careful examination of the survey data yielded 3 missing cases.

One of the remaining 2 candidates was recently ruled out by Serre, who suggests that the other is also similarly obstructed.

Supporting evidence

In addition to the trace moment sequences, for each candidate subgroup $H \subseteq USp(4)$ we may also consider the component group of H and the dimension of H.

Partitioning the $\bar{L}_p(T)$ data according to suitable constraints on p yields the predicted component distributions.

The dimension of H predicts the cardinality of the mod ℓ Galois image. For small ℓ we estimate this by counting how often the ℓ-Sylow subgroup of $J(C/\mathbb{F}_p)$ has full rank.

Open questions

- Consider the zero-trace densities that arise in genus 2. Can one prove that the list

$$1/6, 1/4, 1/2, 7/12, 5/8, 3/4, 13/16, 7/8$$

is complete in genus 2?

- Is their a lattice path interpretation for each of the identified subgroups in $USp(4)$?

- What happens in genus 3?

Sato-Tate in genus 2

Andrew V. Sutherland

Massachusetts Institute of Technology

March 30, 2009

joint work with Kiran Kedlaya

http://arxiv.org/abs/0803.4462