Telescopes for Mathematicians

Andrew V. Sutherland

Massachusetts Institute of Technology

September 2, 2011

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

Algebraic curves

Solutions to a polynomial equation $f(x, y) = 0$:

$$y = 2x + 1 \qquad\qquad x^2 + y^2 = 1$$

$$y^2 = x^5 + 3x^3 - 5x + 4 \qquad\qquad 3x^4 + 4y^3 - xy^3 + 2xy + 1 = 0$$

Algebraic curves

Solutions to a polynomial equation $f(x,y)=0$:

$$y = 2x + 1 \qquad\qquad x^2 + y^2 = 1$$

$$y^2 = x^5 + 3x^3 - 5x + 4 \qquad\qquad 3x^4 + 4y^3 - xy^3 + 2xy + 1 = 0$$

How many points are on these curves?

Counting points modulo p

Let's counts points on the curve $x^2 + y^2 = 1 \bmod p$.

Counting points modulo p

Let's counts points on the curve $x^2 + y^2 = 1 \bmod p$.

p	3	5	7	11	13	17	19	23	29	$\ldots$
	4	4	8	12	12	16	20	24	28	$p \pm 1$

Counting points modulo p

Let's counts points on the curve $x^2 + y^2 = 1 \bmod p$.

p	3	5	7	11	13	17	19	23	29	...
	4	4	8	12	12	16	20	24	28	$p \pm 1$

Actually, we really should count the distinct (nonzero) projective points $(x, y, z) \sim (cx, cy, cz)$ on the curve $x^2 + y^2 = z^2 \bmod p$.

Counting points modulo p

Let's counts points on the curve $x^2 + y^2 = 1 \bmod p$.

p	3	5	7	11	13	17	19	23	29	$\dots$
	4	4	8	12	12	16	20	24	28	$p \pm 1$

Actually, we really should count the distinct (nonzero) projective points $(x, y, z) \sim (cx, cy, cz)$ on the curve $x^2 + y^2 = z^2 \bmod p$.

p	3	5	7	11	13	17	19	23	29	$\dots$
	4	6	8	12	14	18	20	24	30	$p + 1$

The Hasse-Weil bound

The number of points on a genus g curve over $\mathbb{F}_p$ is

$$p + 1 - t_p$$

where the *trace of Frobenius* t_p is an integer satisfying

$$|t_p| \leqslant 2g\sqrt{p}.$$

The Hasse-Weil bound

The number of points on a genus g curve over $\mathbb{F}_p$ is

$$p + 1 - t_p$$

where the *trace of Frobenius* t_p is an integer satisfying

$$|t_p| \leqslant 2g\sqrt{p}.$$

So $x_p = t_p/\sqrt{p}$ is a real number in the interval $[-2g, 2g]$.

What is the distribution of x_p as p varies?

The Hasse-Weil bound

The number of points on a genus g curve over $\mathbb{F}_p$ is

$$p + 1 - t_p$$

where the *trace of Frobenius* t_p is an integer satisfying

$$|t_p| \leqslant 2g\sqrt{p}.$$

So $x_p = t_p/\sqrt{p}$ is a real number in the interval $[-2g, 2g]$.

What is the distribution of x_p as p varies?

Let's compute the distribution of x_p over $p \leqslant N$, then look at what happens as $N \to \infty$.

Sato-Tate distributions in genus 1 (over $\mathbb{Q}$)

1. Typical case (no CM)

All elliptic curves without CM have the semi-circular distribution.

[Clozel, Harris, Shepherd-Barron, Taylor, Barnet-Lamb, and Geraghty]

2. Exceptional case (CM)

All elliptic curves with CM have the same exceptional distribution.

[classical]

Zeta functions and L-polynomials

For a smooth projective curve $C/\mathbb{Q}$ and a good prime p define

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

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

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

where $L_p(T)$ is an integer polynomial of degree $2g$. For $g=2$:

$$L_p(T) = p^2T^4 + c_1pT^3 + c_2pT^2 + c_1T + 1.$$

Unitarized L-polynomials

The polynomial

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

has coefficients that satisfy $a_i = a_{2g-i}$ and $|a_i| \leqslant \binom{2g}{i}$.

Given a curve C, we may consider the distribution of $a_1, a_2, \ldots, a_g$, taken over primes $p \leqslant N$ of good reduction, as $N \to \infty$.

In this talk we will focus on genus $g = 2$.

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

The random matrix model

$\bar{L}_p(\mathrm{T})$ is a real symmetric polynomial whose roots lie on the unit circle.

The random matrix model

$\bar{L}_p$(T) is a real symmetric polynomial whose roots lie on the unit circle.

Every such polynomial arises as the characteristic polynomial $\chi(T)$ of a unitary symplectic matrix in $\mathbb{C}^{2g\times 2g}$.

The random matrix model

$\bar{L}_p$(T) is a real symmetric polynomial whose roots lie on the unit circle.

Every such polynomial arises as the characteristic polynomial $\chi(T)$ of a unitary symplectic matrix in $\mathbb{C}^{2g\times 2g}$.

Conjecture (Katz-Sarnak)

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

This conjecture has been proven “on average” for universal families of hyperelliptic curves, including all genus 2 curves, by Katz and Sarnak.

The Haar measure on $USp(2g)$

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

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

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

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

$\bar{L}_p$-distributions in genus 2

Our goal was to understand the $\bar{L}_p$-distributions that arise in genus 2, including all the exceptional cases.

This presented three challenges:

- Collecting data.
- Identifying and distinguishing distributions.
- Classifying the exceptional cases.

Collecting data

There are four ways to compute $\bar{L}_p$ 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: $\tilde{O}(1)$.

Collecting data

There are four ways to compute $\bar{L}_p$ 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: $\tilde{O}(1)$.

For the feasible range of $p \leqslant N$, we found (2) to be the best.
We can accelerate the computation with partial use of (1) and (4).

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

Time to compute $\bar{L}_p$ for all $p \leqslant N$

N	2 cores	16 cores
2^{16}	1	< 1
2^{17}	4	2
2^{18}	12	3
2^{19}	40	7
2^{20}	2:32	24
2^{21}	10:46	1:38
2^{22}	40:20	5:38
2^{23}	2:23:56	19:04
2^{24}	8:00:09	1:16:47
2^{25}	26:51:27	3:24:40
2^{26}		11:07:28
2^{27}		36:48:52

Characterizing distributions

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 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 $N \to \infty$.

Characterizing distributions

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 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 $USp(2g)$, then $M[X]$ is an *integer* sequence.

This applies to all the coefficients of $\chi(T)$.

Trace moment sequence in genus 1 (typical curve)

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

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

Trace moment sequence in genus 1 (typical curve)

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.

Trace moment sequence in genus $g > 1$ (typical curve)

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.

In genus g, the nth moment of the trace is the number of returning walks of length n on $\mathbb{Z}^g$ with $x_1 \geqslant x_2 \geqslant \cdots \geqslant x_g \geqslant 0$ [Grabiner-Magyar].

Exceptional trace moment sequence 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.

An exceptional trace moment sequence in Genus 2

For a hyperelliptic curve whose Jacobian is isogenous to 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 $A138551$,

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

The second moment already differs from the standard sequence, and the fourth moment differs greatly (11 versus 3).

Searching for exceptional curves (take 1 [KS2009])

We surveyed the trace-distributions of 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 $|c_i| \leqslant 64$ and $|b_i| \leqslant 16$, over 2^{36} curves.

We initially set $N \approx 2^{12}$, discarded about 99% of the curves (those whose moment statistics were "unexceptional"), then repeated this process with $N = 2^{16}$ and $N = 2^{20}$.

We eventually found some 30,000 non-isogenous exceptional curves and a total of 23 distinct trace distributions.

Representative examples were computed to high precision $N = 2^{26}$.

Searching for exceptional curves (take 1 [KS2009])

We surveyed the trace-distributions of 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 $|c_i| \leqslant 64$ and $|b_i| \leqslant 16$, over 2^{36} curves.

We initially set $N \approx 2^{12}$, discarded about 99% of the curves (those whose moment statistics were "unexceptional"), then repeated this process with $N = 2^{16}$ and $N = 2^{20}$.

We eventually found some 30,000 non-isogenous exceptional curves and a total of 23 distinct trace distributions.

Representative examples were computed to high precision $N = 2^{26}$.

These results suggested a candidate 24th trace distribution,
but we were unable to find any examples...

Searching for exceptional curves (take 1 [KS2009])

We surveyed the trace-distributions of 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 $|c_i| \leqslant 64$ and $|b_i| \leqslant 16$, over 2^{36} curves.

We initially set $N \approx 2^{12}$, discarded about 99% of the curves (those whose moment statistics were "unexceptional"), then repeated this process with $N = 2^{16}$ and $N = 2^{20}$.

We eventually found some 30,000 non-isogenous exceptional curves and a total of 23 distinct trace distributions.

Representative examples were computed to high precision $N = 2^{26}$.

These results suggested a candidate 24th trace distribution,
but we were unable to find any examples...
...but in Dec 2010, Fité and Lario constructed just such a curve!

Random matrix subgroup model

Conjecture (Generalized Sato-Tate — naïve form)

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 $G \subseteq \mathrm{USp}(2g)$.

The group G must satisfy several “Sato-Tate axioms”.
These imply that the number of possible Sato-Tate groups of a given genus is bounded: at most 3 in genus 1 and 55 in genus 2.

Sato-Tate groups in genus 1

The Sato-Tate group of an elliptic curve without CM is $\mathrm{USp}(2) = \mathrm{SU}(2)$.

For CM curves (over $\mathbb{Q}$), consider the following subgroup of $\mathrm{SU}(2)$:

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

the normalizer of $\mathrm{SO}(2) = U(1)$ in $\mathrm{SU}(2)$.

H is a (disconnected) compact group whose Haar measure yields the correct trace moment sequence for a CM curve.

The third Sato-Tate group in genus 1 is simply $\mathrm{U}(1)$, which occurs for CM curves E/k where the number field k contains the CM-field of E.

Sato-Tate groups in genus 2 (predicted)

There are a total of 55 groups $G \subseteq \mathrm{USp}(4)$ (up to conjugacy) that satisfy the Sato-Tate axioms, of which 3 can be ruled out [Serre]. Of the remaining 52, only 34 can occur over $\mathbb{Q}$.

There are 6 possibile identity components G^0.
The component group G/G^0 is a finite group whose order divides 48.

G^0	Number of groups	over $\mathbb{Q}$
$\mathrm{U}(1)$	32	18
$\mathrm{U}(1) \times \mathrm{U}(1)$	5	2
$\mathrm{SU}(2)$	10	10
$\mathrm{U}(1) \times \mathrm{SU}(2)$	2	1
$\mathrm{SU}(2) \times \mathrm{SU}(2)$	2	2
$\mathrm{USp}(4)$	1	1

There are a total of 36 distinct trace distributions, 26 of which can occur over $\mathbb{Q}$.

d	c	G	$[G/G^0]$	z_1	z_2	$M[a_1^2]$	$M[a_2]$
1	1	C_1	C_1	0	0, 0, 0, 0, 0	8, 96, 1280, 17920	4, 18, 88, 454
1	2	C_2	C_2	1	0, 0, 0, 0, 0	4, 48, 640, 8960	2, 10, 44, 230
1	3	C_3	C_3	0	0, 0, 0, 0, 0	4, 36, 440, 6020	2, 8, 34, 164
1	4	C_4	C_4	1	0, 0, 0, 0, 0	4, 36, 400, 5040	2, 8, 32, 150
1	6	C_6	C_6	1	0, 0, 0, 0, 0	4, 36, 400, 4900	2, 8, 32, 148
1	4	D_2	D_2	3	0, 0, 0, 0, 0	2, 24, 320, 4480	1, 6, 22, 118
1	6	D_3	D_3	3	0, 0, 0, 0, 0	2, 18, 220, 3010	1, 5, 17, 85
1	8	D_4	D_4	5	0, 0, 0, 0, 0	2, 18, 200, 2520	1, 5, 16, 78
1	12	D_6	D_6	7	0, 0, 0, 0, 0	2, 18, 200, 2450	1, 5, 16, 77
1	2	$J(C_1)$	C_2	1	1, 0, 0, 0, 0	4, 48, 640, 8960	1, 11, 40, 235
1	4	$J(C_2)$	D_2	3	1, 0, 0, 0, 1	2, 24, 320, 4480	1, 7, 22, 123
1	6	$J(C_3)$	C_6	3	1, 0, 0, 2, 0	2, 18, 220, 3010	1, 5, 16, 85
1	8	$J(C_4)$	$\mathrm{C}_4 \times \mathrm{C}_2$	5	1, 0, 2, 0, 1	2, 18, 200, 2520	1, 5, 16, 79
1	12	$J(C_6)$	$\mathrm{C}_6 \times \mathrm{C}_2$	7	1, 2, 0, 2, 1	2, 18, 200, 2450	1, 5, 16, 77
1	8	$J(D_2)$	$\mathrm{D}_2 \times \mathrm{C}_2$	7	1, 0, 0, 0, 3	1, 12, 160, 2240	1, 5, 13, 67
1	12	$J(D_3)$	D_6	9	1, 0, 0, 2, 3	1, 9, 110, 1505	1, 4, 10, 48
1	16	$J(D_4)$	$\mathrm{D}_4 \times \mathrm{C}_2$	13	1, 0, 2, 0, 5	1, 9, 100, 1260	1, 4, 10, 45
1	24	$J(D_6)$	$\mathrm{D}_6 \times \mathrm{C}_2$	19	1, 2, 0, 2, 7	1, 9, 100, 1225	1, 4, 10, 44
1	2	$C_{2,1}$	C_2	1	0, 0, 0, 0, 1	4, 48, 640, 8960	3, 11, 48, 235
1	4	$C_{4,1}$	C_4	3	0, 0, 2, 0, 0	2, 24, 320, 4480	1, 5, 22, 115
1	6	$C_{6,1}$	C_6	3	0, 2, 0, 0, 1	2, 18, 220, 3010	1, 5, 18, 85
1	4	$D_{2,1}$	D_2	3	0, 0, 0, 0, 2	2, 24, 320, 4480	2, 7, 26, 123
1	8	$D_{4,1}$	D_4	7	0, 0, 2, 0, 2	1, 12, 160, 2240	1, 4, 13, 63
1	12	$D_{6,1}$	D_6	9	0, 2, 0, 0, 4	1, 9, 110, 1505	1, 4, 11, 48
1	6	$D_{3,2}$	D_3	3	0, 0, 0, 0, 3	2, 18, 220, 3010	2, 6, 21, 90
1	8	$D_{4,2}$	D_4	5	0, 0, 0, 0, 4	2, 18, 200, 2520	2, 6, 20, 83
1	12	$D_{6,2}$	D_6	7	0, 0, 0, 0, 6	2, 18, 200, 2450	2, 6, 20, 82
1	12	T	A_4	3	0, 0, 0, 0, 0	2, 12, 120, 1540	1, 4, 12, 52
1	24	O	S_4	9	0, 0, 0, 0, 0	2, 12, 100, 1050	1, 4, 11, 45
1	24	O_1	S_4	15	0, 0, 6, 0, 6	1, 6, 60, 770	1, 3, 8, 30
1	24	$J(T)$	$\mathrm{A}_4 \times \mathrm{C}_2$	15	1, 0, 0, 8, 3	1, 6, 60, 770	1, 3, 7, 29
1	48	$J(O)$	$\mathrm{S}_4 \times \mathrm{C}_2$	33	1, 0, 6, 8, 9	1, 6, 50, 525	1, 3, 7, 26
3	1	E_1	C_1	0	0, 0, 0, 0, 0	4, 32, 320, 3584	3, 10, 37, 150
3	2	E_2	C_2	1	0, 0, 0, 0, 0	2, 16, 160, 1792	1, 6, 17, 78
3	3	E_3	C_3	0	0, 0, 0, 0, 0	2, 12, 110, 1204	1, 4, 13, 52
3	4	E_4	C_4	1	0, 0, 0, 0, 0	2, 12, 100, 1008	1, 4, 11, 46
3	6	E_6	C_6	1	0, 0, 0, 0, 0	2, 12, 100, 980	1, 4, 11, 44
3	2	$J(E_1)$	C_2	1	0, 0, 0, 0, 0	2, 16, 160, 1792	2, 6, 20, 78
3	4	$J(E_2)$	D_2	3	0, 0, 0, 0, 0	1, 8, 80, 896	1, 4, 10, 42
3	6	$J(E_3)$	D_3	3	0, 0, 0, 0, 0	1, 6, 55, 602	1, 3, 8, 29
3	8	$J(E_4)$	D_4	5	0, 0, 0, 0, 0	1, 6, 50, 504	1, 3, 7, 26
3	12	$J(E_6)$	D_6	7	0, 0, 0, 0, 0	1, 6, 50, 490	1, 3, 7, 25
2	1	F	C_1	0	0, 0, 0, 0, 0	4, 36, 400, 4900	2, 8, 32, 148
2	2	F_a	C_2	0	0, 0, 0, 0, 1	3, 21, 210, 2485	2, 6, 20, 82
2	2	F_c	C_2	1	0, 0, 0, 0, 0	2, 18, 200, 2450	1, 5, 16, 77
2	2	F_{ab}	C_2	1	0, 0, 0, 0, 1	2, 18, 200, 2450	2, 6, 20, 82
2	4	F_{ac}	C_4	3	0, 0, 2, 0, 1	1, 9, 100, 1225	1, 3, 10, 41
2	4	$F_{a,b}$	D_2	1	0, 0, 0, 0, 3	2, 12, 110, 1260	2, 5, 14, 49
2	4	$F_{ab,c}$	D_2	3	0, 0, 0, 0, 1	1, 9, 100, 1225	1, 4, 10, 44
2	8	$F_{a,b,c}$	D_4	5	0, 0, 2, 0, 3	1, 6, 55, 630	1, 3, 7, 26
4	1	G_4	C_1	0	0, 0, 0, 0, 0	3, 20, 175, 1764	2, 6, 20, 76
4	2	$N(G_4)$	C_2	0	0, 0, 0, 0, 1	2, 11, 90, 889	2, 5, 14, 46
6	1	G_6	C_1	0	0, 0, 0, 0, 0	2, 10, 70, 588	2, 5, 14, 44
6	2	$N(G_6)$	C_2	1	0, 0, 0, 0, 0	1, 5, 35, 294	1, 3, 7, 23
10	1	$\mathrm{USp}(4)$	C_1	0	0, 0, 0, 0, 0	1, 3, 14, 84	1, 2, 4, 10

Searching for exceptional curves (take 2 [FKRS11])

We surveyed the trace-distributions of genus 2 curves

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

$$y^2 = x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0,$$

with integer coefficients $|c_i| \leqslant 128$, over 2^{48} curves.

We specifically searched for curves with zero trace density $> 1/2$.

We found over 10 million non-isogenous exceptional curves, including at least 3 examples matching each of the 34 Sato groups over $\mathbb{Q}$.

Representative examples were computed to high precision $N = 2^{28}$.

Key optimizations

1. Very fast algorithm (100ns per curve) to quickly compute the number of zero traces up to a small bound. This let us quickly discard curves that did not have many zero traces at small primes.

Key optimizations

1. Very fast algorithm (100ns per curve) to quickly compute the number of zero traces up to a small bound. This let us quickly discard curves that did not have many zero traces at small primes.

2. Additional group invariants $z_{i,j}$ defined by

$$\Pr[a_i = j] = z_{i,j}/c,$$

where $c = \#G/G^0$, used to more quickly classify distributions.

Key optimizations

1. Very fast algorithm (100ns per curve) to quickly compute the number of zero traces up to a small bound. This let us quickly discard curves that did not have many zero traces at small primes.

2. Additional group invariants $z_{i,j}$ defined by

$$\Pr[a_i = j] = z_{i,j}/c,$$

where $c = \#G/G^0$, used to more quickly classify distributions.

3. More efficient handling of curves in sextic form allowed us to efficiently compute a_2 moments for every curve. (This is crucial for distinguishing several distributions).

Sato-Tate groups in genus 2 (exhibited)

For each of the 34 genus 2 Sato-Tate groups that can occur over $\mathbb{Q}$, we can exhibit a genus 2 curve with a closely matching $\bar{L}_p$ distribution.

Sato-Tate groups in genus 2 (exhibited)

For each of the 34 genus 2 Sato-Tate groups that can occur over $\mathbb{Q}$, we can exhibit a genus 2 curve with a closely matching $\bar{L}_p$ distribution.

By considering a subset of these curves over suitable number fields, we can obtain the remaining 18 Sato-Tate distributions in genus 2.

Sato-Tate groups in genus 2 (exhibited)

For each of the 34 genus 2 Sato-Tate groups that can occur over $\mathbb{Q}$, we can exhibit a genus 2 curve with a closely matching $\bar{L}_p$ distribution.

By considering a subset of these curves over suitable number fields, we can obtain the remaining 18 Sato-Tate distributions in genus 2.

We now have curves matching all 52 Sato-Tate groups in genus 2.

Sato-Tate groups in genus 2 (exhibited)

For each of the 34 genus 2 Sato-Tate groups that can occur over $\mathbb{Q}$, we can exhibit a genus 2 curve with a closely matching $\bar{L}_p$ distribution.

By considering a subset of these curves over suitable number fields, we can obtain the remaining 18 Sato-Tate distributions in genus 2.

We now have curves matching all 52 Sato-Tate groups in genus 2.

In 51 of 52 cases (all but the generic case) we can *prove* that the distributions match [FKRS11].

ST Group	Genus 2 curve $y^2 = f(x)$	Field	Type [KS]
$C_1 = U(1)$	$x^6 + 1$	$\mathbb{Q}(\sqrt{-3})$	#27
C_2	$x^5 - x$	$\mathbb{Q}(\sqrt{-2})$	#13
C_3	$x^6 + 4$	$\mathbb{Q}(\sqrt{-3})$	#28
C_4	$x^6 + x^5 - 5x^4 - 5x^2 - x + 1$	$\mathbb{Q}(\sqrt{-2})$	#29
C_6	$x^6 + 2$	$\mathbb{Q}(\sqrt{-3})$	#30
D_2	$x^5 + 9x$	$\mathbb{Q}(\sqrt{-2})$	#21
D_3	$x^6 + 2x^3 + 2$	$\mathbb{Q}(\sqrt{-6})$	#12
D_4	$x^5 + 3x$	$\mathbb{Q}(\sqrt{-2})$	#17
D_6	$x^6 + 3x^5 + 10x^3 - 15x^2 + 15x - 6$	$\mathbb{Q}(\sqrt{-3})$	#15
$J(C_1)$	$x^5 - x$	$\mathbb{Q}(i)$	#13
$J(C_2)$	$x^5 - x$	$\mathbb{Q}$	#21
$J(C_3)$	$x^6 + 2x^3 + 2$	$\mathbb{Q}(\sqrt{-3})$	#12
$J(C_4)$	$x^6 + x^5 - 5x^4 - 5x^2 - x + 1$	$\mathbb{Q}$	#17
$J(C_6)$	$x^6 - 15x^4 - 20x^3 + 6x + 1$	$\mathbb{Q}$	#15
$J(D_2)$	$x^5 + 9x$	$\mathbb{Q}$	#23
$J(D_3)$	$x^6 + 2x^3 + 2$	$\mathbb{Q}$	#20
$J(D_4)$	$x^5 + 3x$	$\mathbb{Q}$	#22
$J(D_6)$	$x^6 + 3x^5 + 10x^3 - 15x^2 + 15x - 6$	$\mathbb{Q}$	#24
$D_{6,1}$	$x^6 + 6x^5 - 30x^4 - 40x^3 + 60x^2 + 24x - 8$	$\mathbb{Q}$	#20
$C_{2,1}$	$x^6 + 1$	$\mathbb{Q}$	#13
$C_{4.1}$	$x^5 + 2x$	$\mathbb{Q}(i)$	#21
$C_{6,1}$	$x^6 + 3x^5 - 25x^3 + 30x^2 - 9x + 1$	$\mathbb{Q}$	#12
$D_{2,1}$	$x^5 + x$	$\mathbb{Q}$	#21
$D_{4,1}$	$x^5 + 2x$	$\mathbb{Q}$	#23
D_3^{-}	$x^6 + 4$	$\mathbb{Q}$	#12
D_4^{-}	$x^6 + x^5 + 10x^3 + 5x^2 + x - 2$	$\mathbb{Q}$	#17
D_6^{-}	$x^6 + 2$	$\mathbb{Q}$	#15
T	$x^6 + 6x^5 - 20x^4 + 20x^3 - 20x^2 - 8x + 8$	$\mathbb{Q}(\sqrt{-2})$	#31
O	$x^6 - 5x^4 + 10x^3 - 5x^2 + 2x - 1$	$\mathbb{Q}(\sqrt{-2})$	#32
O_1	$x^6 + 7x^5 + 10x^4 + 10x^3 + 15x^2 + 17x + 4$	$\mathbb{Q}$	#25
$J(T)$	$x^6 + 6x^5 - 20x^4 + 20x^3 - 20x^2 - 8x + 8$	$\mathbb{Q}$	#25
$J(O)$	$x^6 - 5x^4 + 10x^3 - 5x^2 + 2x - 1$	$\mathbb{Q}$	#26

ST Group	Genus 2 curve $y^2 = f(x)$	Field	Type [KS]
$F = U(1) \times U(1)$	$x^6 + 3x^3 + x^2 - 1$	$\mathbb{Q}(i, \sqrt{2})$	#33
F_a	$x^6 + 3x^3 + x^2 - 1$	$\mathbb{Q}(i)$	#34
F_{ab}	$x^6 + 3x^3 + x^2 - 1$	$\mathbb{Q}(\sqrt{2})$	#35
F_{ac}	$x^5 + 1$	$\mathbb{Q}$	#19
$F_{a,b}$	$x^6 + 3x^4 + x^2 - 1$	$\mathbb{Q}$	#8
$E_1 = \mathrm{SU}(2)$	$x^6 + x^4 + x^2 + 1$	$\mathbb{Q}$	#5
E_2	$x^5 + x^4 + 2x^3 - 2x^2 - 2x + 2$	$\mathbb{Q}$	#11
E_3	$x^5 + x^4 - 3x^3 - 4x^2 - x$	$\mathbb{Q}$	#4
E_4	$x^5 + x^4 + x^2 - x$	$\mathbb{Q}$	#7
E_6	$x^5 + 2x^4 - x^3 - 3x^2 - x$	$\mathbb{Q}$	#6
$J(E_1)$	$x^5 + x^3 + x$	$\mathbb{Q}$	#11
$J(E_2)$	$x^5 + x^3 - x$	$\mathbb{Q}$	#18
$J(E_3)$	$x^6 + x^3 + 4$	$\mathbb{Q}$	#10
$J(E_4)$	$x^5 + x^3 + 2x$	$\mathbb{Q}$	#16
$J(E_6)$	$x^6 + x^3 - 2$	$\mathbb{Q}$	#14
$\mathrm{U}(1) \times \mathrm{SU}(2)$	$x^6 + 3x^4 - 2$	$\mathbb{Q}(i)$	#36
$N(\mathrm{U}(1) \times \mathrm{SU}(2))$	$x^6 + 3x^4 - 2$	$\mathbb{Q}$	#3
$\mathrm{SU}(2) \times \mathrm{SU}(2)$	$x^6 + x^2 + 1$	$\mathbb{Q}$	#2
$N(\mathrm{SU}(2) \times \mathrm{SU}(2))$	$x^6 + x^5 + x - 1$	$\mathbb{Q}$	#9
$\mathrm{USp}(4)$	$x^5 + x + 1$	$\mathbb{Q}$	#1

Telescopes for Mathematicians

Andrew V. Sutherland

Massachusetts Institute of Technology

September 2, 2011

`http://math.mit.edu/~drew`