Sato-Tate distributions

Andrew V. Sutherland

Massachusetts Institute of Technology

February 4, 2016

Joint work with F. Fité, K.S. Kedlaya, and V. Rotger (part 1), and D. Harvey (part 2).
Let $E/\mathbb{Q}$ be an elliptic curve, which we can write in the form

$$y^2 = x^3 + ax + b,$$

and let $p$ be a prime of good reduction ($4a^3 + 27b^2 \not\equiv 0 \pmod{p}$).

The number of $\mathbb{F}_p$-points on the reduction $E_p$ of $E$ modulo $p$ is

$$\#E_p(\mathbb{F}_p) = p + 1 - t_p,$$

where the trace of Frobenius $t_p \in \mathbb{Z}$ lies in the interval $[-2\sqrt{p}, 2\sqrt{p}]$.

We are interested in the limiting distribution of $x_p = -t_p/\sqrt{p} \in [-2, 2]$, as $p$ varies over primes of good reduction up to $N$, as $N \to \infty$. 
Example: \( y^2 = x^3 + x + 1 \)

<table>
<thead>
<tr>
<th>( p )</th>
<th>( t_p )</th>
<th>( x_p )</th>
<th>( p )</th>
<th>( t_p )</th>
<th>( x_p )</th>
<th>( p )</th>
<th>( t_p )</th>
<th>( x_p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0</td>
<td>0.000000</td>
<td>71</td>
<td>13</td>
<td>-1.542816</td>
<td>157</td>
<td>-13</td>
<td>1.037513</td>
</tr>
<tr>
<td>5</td>
<td>-3</td>
<td>1.341641</td>
<td>73</td>
<td>2</td>
<td>-0.234082</td>
<td>163</td>
<td>-25</td>
<td>1.958151</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>-1.133893</td>
<td>79</td>
<td>-6</td>
<td>0.675053</td>
<td>167</td>
<td>24</td>
<td>-1.857176</td>
</tr>
<tr>
<td>11</td>
<td>-2</td>
<td>0.603023</td>
<td>83</td>
<td>-6</td>
<td>0.658586</td>
<td>173</td>
<td>2</td>
<td>-0.152057</td>
</tr>
<tr>
<td>13</td>
<td>-4</td>
<td>1.109400</td>
<td>89</td>
<td>-10</td>
<td>1.059998</td>
<td>179</td>
<td>0</td>
<td>0.000000</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
<td>0.000000</td>
<td>97</td>
<td>1</td>
<td>-0.101535</td>
<td>181</td>
<td>-8</td>
<td>0.594635</td>
</tr>
<tr>
<td>19</td>
<td>-1</td>
<td>0.229416</td>
<td>101</td>
<td>-3</td>
<td>0.298511</td>
<td>191</td>
<td>-25</td>
<td>1.808937</td>
</tr>
<tr>
<td>23</td>
<td>-4</td>
<td>0.834058</td>
<td>103</td>
<td>17</td>
<td>-1.675060</td>
<td>193</td>
<td>-7</td>
<td>0.503871</td>
</tr>
<tr>
<td>29</td>
<td>-6</td>
<td>1.114172</td>
<td>107</td>
<td>3</td>
<td>-0.290021</td>
<td>197</td>
<td>-24</td>
<td>1.709929</td>
</tr>
<tr>
<td>37</td>
<td>-10</td>
<td>1.643990</td>
<td>109</td>
<td>-13</td>
<td>1.245174</td>
<td>199</td>
<td>-18</td>
<td>1.275986</td>
</tr>
<tr>
<td>41</td>
<td>7</td>
<td>-1.093216</td>
<td>113</td>
<td>-11</td>
<td>1.034793</td>
<td>211</td>
<td>-11</td>
<td>0.757271</td>
</tr>
<tr>
<td>43</td>
<td>10</td>
<td>-1.524986</td>
<td>127</td>
<td>2</td>
<td>-0.177471</td>
<td>223</td>
<td>-20</td>
<td>1.339299</td>
</tr>
<tr>
<td>47</td>
<td>-12</td>
<td>1.750380</td>
<td>131</td>
<td>4</td>
<td>-0.349482</td>
<td>227</td>
<td>0</td>
<td>0.000000</td>
</tr>
<tr>
<td>53</td>
<td>-4</td>
<td>0.549442</td>
<td>137</td>
<td>12</td>
<td>-1.025229</td>
<td>229</td>
<td>-2</td>
<td>0.132164</td>
</tr>
<tr>
<td>59</td>
<td>-3</td>
<td>0.390567</td>
<td>139</td>
<td>14</td>
<td>-1.187465</td>
<td>233</td>
<td>-3</td>
<td>0.196537</td>
</tr>
<tr>
<td>61</td>
<td>12</td>
<td>-1.536443</td>
<td>149</td>
<td>14</td>
<td>-1.146925</td>
<td>239</td>
<td>-22</td>
<td>1.423062</td>
</tr>
<tr>
<td>67</td>
<td>12</td>
<td>-1.466033</td>
<td>151</td>
<td>-2</td>
<td>0.162758</td>
<td>241</td>
<td>22</td>
<td>-1.417145</td>
</tr>
</tbody>
</table>

http://math.mit.edu/~drew/g1SatoTateDistributions.html
click histogram to animate (requires adobe reader)
click histogram to animate (requires adobe reader)
click histogram to animate (requires adobe reader)
click histogram to animate (requires adobe reader)
1. Typical case (no CM)

Elliptic curves $E/\mathbb{Q}$ without CM have the semicircular trace distribution. (This is also known for $E/k$, where $k$ is a totally real number field).

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

2. Exceptional cases (CM)

Elliptic curves $E/k$ with CM have one of two distinct trace distributions, depending on whether $k$ contains the CM field or not.

[classical (Hecke, Deuring)]
Sato-Tate groups in dimension 1

The **Sato-Tate group** of $E$ is a closed subgroup $G$ of $SU(2) = USp(2)$ derived from the $\ell$-adic Galois representation attached to $E$.

The refined Sato-Tate conjecture implies that the distribution of normalized traces of $E_p$ converges to the distribution of traces in the Sato-Tate group of $G$, under the Haar measure.

<table>
<thead>
<tr>
<th>$G$</th>
<th>$G/G^0$</th>
<th>$E$</th>
<th>$k$</th>
<th>$E[a_1^0], E[a_1^2], E[a_1^4], \ldots$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U(1)$</td>
<td>$C_1$</td>
<td>$y^2 = x^3 + 1$</td>
<td>$\mathbb{Q}(\sqrt{-3})$</td>
<td>1, 2, 6, 20, 70, 252, \ldots</td>
</tr>
<tr>
<td>$N(U(1))$</td>
<td>$C_2$</td>
<td>$y^2 = x^3 + 1$</td>
<td>$\mathbb{Q}$</td>
<td>1, 1, 3, 10, 35, 126, \ldots</td>
</tr>
<tr>
<td>$SU(2)$</td>
<td>$C_1$</td>
<td>$y^2 = x^3 + x + 1$</td>
<td>$\mathbb{Q}$</td>
<td>1, 1, 2, 5, 14, 42, \ldots</td>
</tr>
</tbody>
</table>

In dimension 1 there are three possible Sato-Tate groups, two of which arise for elliptic curves defined over $\mathbb{Q}$. 
Zeta functions and $L$-polynomials

Let $C/\mathbb{Q}$ be a nice curve of genus $g$ and $p$ a prime of good reduction. Define the zeta function

$$Z_p(T) := \exp \left( \sum_{r=1}^{\infty} \frac{N_r T^r}{r} \right),$$

where $N_r = \# C_p(\mathbb{F}_p^r)$. This is a rational function of the form

$$Z_p(T) = \frac{L_p(T)}{(1-T)(1-pT)},$$

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

For $g = 1$ we have $L_p(t) = pT^2 + c_1 T + 1$, and for $g = 2$,

$$L_p(T) = p^2 T^4 + c_1 pT^3 + c_2 T^2 + c_1 T + 1.$$
The normalized $L$-polynomial

$$\bar{L}_p(T) := L_p(T/\sqrt{p}) = \sum_{i=0}^{2g} a_i T^i \in \mathbb{R}[T]$$

is monic, reciprocal ($a_i = a_{2g-i}$), and unitary (roots on the unit circle). The coefficients $a_i$ satisfy the Weil bounds $|a_i| \leq \binom{2g}{i}$.

We now consider the limiting distribution of $a_1, a_2, \ldots, a_g$ over all primes $p \leq N$ of good reduction, as $N \to \infty$.

http://math.mit.edu/~drew/g2SatoTateDistributions.html
click histogram to animate (requires adobe reader)
click histogram to animate (requires adobe reader)
click histogram to animate (requires adobe reader)
Exceptional distributions for abelian surfaces over $\mathbb{Q}$:
Let $A$ be an abelian variety of dimension $g \geq 1$ over a number field $k$, and let us fix a prime $\ell$.

Let $\rho_\ell : G_k \to \text{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)) \simeq \text{GSp}_{2g}(\mathbb{Q}_\ell)$ be the Galois representation arising from the action of $G_k := \text{Gal}(\overline{k}/k)$ on the $\ell$-adic Tate module

$$V_\ell(A) := \lim_{\leftarrow} A[\ell^n] \otimes \mathbb{Q}. $$

For each prime $p$ of good reduction for $A$ we have the $L$-polynomial

$$L_p(T) := \det(1 - \rho_\ell(\text{Frob}_p)T),$$

$$\bar{L}_p(T) := L_p(T/\sqrt{||p||}) = \sum a_i T^i.$$ 

When $A$ is the Jacobian of a genus $g$ curve $C$, this agrees with our earlier definition of $L_p(T)$ as the numerator of the zeta function $Z_p(T)$. 

Andrew V. Sutherland (MIT)  
Sato-Tate distributions  
February 4, 2016 10 / 33
The Sato-Tate problem for an abelian variety

The $\bar{L}_p \in \mathbb{R}[T]$ are monic, symmetric, unitary polynomials of degree $2g$.

Every such polynomial arises as the characteristic polynomial of a conjugacy class in the unitary symplectic group $\text{USp}(2g)$.

Each probability measure on $\text{USp}(2g)$ determines a distribution of conjugacy classes (hence a distribution of characteristic polynomials).

The Sato-Tate problem, in its simplest form, is to find a measure for which these classes are equidistributed.

Conjecturally, such a measure arises as the Haar measure of a compact subgroup $\text{ST}_A$ of $\text{USp}(2g)$.
The Sato-Tate group

Recall that the action of $G_k$ on $V_{\ell}(A)$ induces the representation

$$\rho_{\ell}: G_k \to \text{Aut}_{\mathbb{Q}_\ell}(V_{\ell}(A)) \simeq \text{GSp}_{2g}(\mathbb{Q}_\ell).$$

Let $G_{\ell}^{1,\text{zar}}$ denote the kernel of the similitude character of $\text{GSp}_{2g}(\mathbb{Q}_\ell)$ on the Zariski closure of $\rho_{\ell}(G_k)$. Now fix $\iota: \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$, and define $\text{ST}_A$ to be a maximal compact subgroup of the image $G_{\ell}^{1,\text{zar}}$ under

$$\text{Sp}_{2g}(\mathbb{Q}_\ell) \otimes_{\iota} \mathbb{C} \to \text{Sp}_{2g}(\mathbb{C}).$$

Conjecturally, $\text{ST}_A$ does not depend on $\ell$ or $\iota$; this is known for $g \leq 3$.

**Definition [Serre]**

$\text{ST}_A \subseteq \text{USp}(2g)$ is the Sato-Tate group of $A$. 
The refined Sato-Tate conjecture

Let \( s(p) \) denote the conjugacy class of the image of \( \text{Frob}_p \) in \( \text{ST}_A \).
Let \( \mu_{\text{ST}_A} \) denote the image of the Haar measure on \( \text{Conj}(\text{ST}_A) \),
which does not depend on the choice of \( \ell \) or \( \iota \).

**Conjecture**

The conjugacy classes \( s(p) \) are equidistributed with respect to \( \mu_{\text{ST}_A} \).

In particular, the distribution of \( \bar{L}_p(T) \) matches the distribution of
characteristic polynomials of random matrices in \( \text{ST}_A \).

We can test this numerically by comparing statistics of the coefficients
\( a_1, \ldots, a_g \) of \( \bar{L}_p(T) \) over \( \|p\| \leq N \) to the predictions given by \( \mu_{\text{ST}_A} \).

https://hensel.mit.edu:8000/home/pub/6
The Sato-Tate axioms

The Sato-Tate axioms for abelian varieties (weight-1 motives):

1. \( G \) is closed subgroup of \( \text{USp}(2g) \).
2. **Hodge condition**: \( G \) contains a Hodge circle\(^1\) whose conjugates generate a dense subset of \( G \).
3. **Rationality condition**: for each component \( H \) of \( G \) and each irreducible character \( \chi \) of \( \text{GL}_{2g}(\mathbb{C}) \) we have \( E[\chi(\gamma) : \gamma \in H] \in \mathbb{Z} \).

For any fixed \( g \), the set of subgroups \( G \subseteq \text{USp}(2g) \) that satisfy the Sato-Tate axioms is **finite** up to conjugacy (3 for \( g = 1 \), 55 for \( g = 2 \)).

**Theorem**

For \( g \leq 3 \), the group \( \text{ST}_A \) satisfies the Sato-Tate axioms.

This is expected to hold for all \( g \).

\(^1\)An embedding \( \theta : U(1) \to G^0 \) where \( \theta(u) \) has eigenvalues \( u, u^{-1} \) with multiplicity \( g \).
Galois endomorphism modules

Let $A$ be an abelian variety defined over a number field $k$. Let $K$ be the minimal extension of $k$ in $\bar{k}$ for which $\text{End}(A_K) = \text{End}(A_{\bar{k}})$. $\text{Gal}(K/k)$ acts on the $\mathbb{R}$-algebra $\text{End}(A_K)_\mathbb{R} := \text{End}(A_K) \otimes_{\mathbb{Z}} \mathbb{R}$.

**Definition**

The *Galois (endomorphism module) type* of $A$ is the isomorphism class of $[\text{Gal}(K/k), \text{End}(A_K)_\mathbb{R}]$, where $[G, E] \simeq [G', E']$ iff there are isomorphisms $G \simeq G'$ and $E \simeq E'$ that are compatible with the Galois action.

**Theorem [FKRS 2012]**

For abelian varieties $A/k$ of dimension $g \leq 3$ there is a one-to-one correspondence between Sato-Tate groups and Galois types.

More precisely, the identity component $\text{ST}^0_A$ is determined by $\text{End}(A_K)_\mathbb{R}$, and there is a natural isomorphism $\text{ST}_A / \text{ST}^0_A \simeq \text{Gal}(K/k)$. 
Real endomorphism algebras of abelian surfaces

<table>
<thead>
<tr>
<th>abelian surface</th>
<th>$\text{End}(A_K)_\mathbb{R}$</th>
<th>$\text{ST}_A^0$</th>
</tr>
</thead>
<tbody>
<tr>
<td>square of CM elliptic curve</td>
<td>$M_2(\mathbb{C})$</td>
<td>$U(1)^2$</td>
</tr>
<tr>
<td>• QM abelian surface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• square of non-CM elliptic curve</td>
<td>$M_2(\mathbb{R})$</td>
<td>$SU(2)^2$</td>
</tr>
<tr>
<td>• CM abelian surface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• product of CM elliptic curves</td>
<td>$\mathbb{C} \times \mathbb{C}$</td>
<td>$U(1) \times U(1)$</td>
</tr>
<tr>
<td>product of CM and non-CM elliptic curves</td>
<td>$\mathbb{C} \times \mathbb{R}$</td>
<td>$U(1) \times SU(2)$</td>
</tr>
<tr>
<td>• RM abelian surface</td>
<td>$\mathbb{R} \times \mathbb{R}$</td>
<td>$SU(2) \times SU(2)$</td>
</tr>
<tr>
<td>• product of non-CM elliptic curves</td>
<td></td>
<td></td>
</tr>
<tr>
<td>generic abelian surface</td>
<td>$\mathbb{R}$</td>
<td>$USp(4)$</td>
</tr>
</tbody>
</table>

(factors in products are assumed to be non-isogenous)
Sato-Tate groups in dimension 2

**Theorem [Fité-Kedlaya-Rotger-S 2012]**

Up to conjugacy, 55 subgroups of $\text{USp}(4)$ satisfy the Sato-Tate axioms:

- $\text{U}(1)_{2}$: $C_1, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6, T, O,$
  $J(C_1), J(C_2), J(C_3), J(C_4), J(C_6),$ 
  $J(D_2), J(D_3), J(D_4), J(D_6), J(T), J(O),$ 
  $C_{2,1}, C_{4,1}, C_{6,1}, D_{2,1}, D_{3,2}, D_{4,1}, D_{4,2}, D_{6,1}, D_{6,2}, O_1$

- $\text{SU}(2)_{2}$: $E_1, E_2, E_3, E_4, E_6, J(E_1), J(E_2), J(E_3), J(E_4), J(E_6)$

- $\text{U}(1) \times \text{U}(1)$: $F, F_a, F_c, F_{a,b}, F_{ab}, F_{ac}, F_{ab,c}, F_{a,b,c}$

- $\text{U}(1) \times \text{SU}(2)$: $\text{U}(1) \times \text{SU}(2), N(\text{U}(1) \times \text{SU}(2))$

- $\text{SU}(2) \times \text{SU}(2)$: $\text{SU}(2) \times \text{SU}(2), N(\text{SU}(2) \times \text{SU}(2))$

- $\text{USp}(4)$: $\text{USp}(4)$

Of these, exactly 52 arise as $\text{STA}$ for an abelian surface $A$ (34 over $\mathbb{Q}$).

This theorem says nothing about equidistribution, however this is now known in many special cases [FS 2012, Johansson 2013].
**Theorem** [Fité-Kedlaya-Rotger-S 2012]

Up to conjugacy, 55 subgroups of $\text{USp}(4)$ satisfy the Sato-Tate axioms:

<table>
<thead>
<tr>
<th>Subgroup</th>
<th>Complementary Subgroups</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U(1)_2$</td>
<td>$C_1, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6, T, O, J(C_1), J(C_2), J(C_3), J(C_4), J(C_6), J(D_2), J(D_3), J(D_4), J(D_6), J(T), J(O)$, $C_{2,1}, C_{4,1}, C_{6,1}, D_{2,1}, D_{3,2}, D_{4,1}, D_{4,2}, D_{6,1}, D_{6,2}, O_1$</td>
</tr>
<tr>
<td>$SU(2)_2$</td>
<td>$E_1, E_2, E_3, E_4, E_6, J(E_1), J(E_2), J(E_3), J(E_4), J(E_6)$</td>
</tr>
<tr>
<td>$U(1) \times U(1)$</td>
<td>$F, F_a, F_c, F_{a,b}, F_{ab}, F_{ac}, F_{ab,c}, F_{a,b,c}$</td>
</tr>
<tr>
<td>$U(1) \times SU(2)$</td>
<td>$U(1) \times SU(2), N(U(1) \times SU(2))$</td>
</tr>
<tr>
<td>$SU(2) \times SU(2)$</td>
<td>$SU(2) \times SU(2), N(SU(2) \times SU(2))$</td>
</tr>
<tr>
<td>$USp(4)$</td>
<td>$USp(4)$</td>
</tr>
</tbody>
</table>

Of these, exactly 52 arise as $ST_A$ for an abelian surface $A$ ($34$ over $\mathbb{Q}$).

This theorem says nothing about equidistribution, however this is now known in many special cases [FS 2012, Johansson 2013].
Sato-Tate groups in dimension 2 with $G^0 = U(1)_2$.

<table>
<thead>
<tr>
<th>$d$</th>
<th>$c$</th>
<th>$G$</th>
<th>$G/G^0$</th>
<th>$z_1$</th>
<th>$z_2$</th>
<th>$M[a^2_1]$</th>
<th>$M[a^2_2]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>$C_1$</td>
<td>$C_1$</td>
<td>0</td>
<td>0</td>
<td>8, 96, 1280, 17920</td>
<td>4, 18, 88, 454</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>$C_2$</td>
<td>$C_2$</td>
<td>1</td>
<td>0</td>
<td>4, 48, 640, 8960</td>
<td>2, 10, 44, 230</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>$C_3$</td>
<td>$C_3$</td>
<td>0</td>
<td>0</td>
<td>4, 36, 440, 6020</td>
<td>2, 8, 34, 164</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>$C_4$</td>
<td>$C_4$</td>
<td>1</td>
<td>0</td>
<td>4, 36, 400, 5040</td>
<td>2, 8, 32, 150</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>$C_6$</td>
<td>$C_6$</td>
<td>1</td>
<td>0</td>
<td>4, 36, 400, 4900</td>
<td>2, 8, 32, 148</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>$D_2$</td>
<td>$D_2$</td>
<td>3</td>
<td>0</td>
<td>2, 24, 320, 4480</td>
<td>1, 6, 22, 118</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>$D_3$</td>
<td>$D_3$</td>
<td>3</td>
<td>0</td>
<td>2, 18, 220, 3010</td>
<td>1, 5, 17, 85</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
<td>$D_4$</td>
<td>$D_4$</td>
<td>5</td>
<td>0</td>
<td>2, 18, 200, 2520</td>
<td>1, 5, 16, 78</td>
</tr>
<tr>
<td>1</td>
<td>12</td>
<td>$D_6$</td>
<td>$D_6$</td>
<td>7</td>
<td>0</td>
<td>2, 18, 200, 2450</td>
<td>1, 5, 16, 77</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>$J(C_1)$</td>
<td>$C_2$</td>
<td>1</td>
<td>1</td>
<td>4, 48, 640, 8960</td>
<td>1, 11, 40, 235</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>$J(C_2)$</td>
<td>$D_2$</td>
<td>3</td>
<td>1</td>
<td>2, 24, 320, 4480</td>
<td>1, 7, 22, 123</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>$J(C_3)$</td>
<td>$C_6$</td>
<td>3</td>
<td>1</td>
<td>2, 18, 220, 3010</td>
<td>1, 5, 16, 85</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
<td>$J(C_4)$</td>
<td>$C_4 \times C_2$</td>
<td>5</td>
<td>1</td>
<td>2, 18, 200, 2520</td>
<td>1, 5, 16, 79</td>
</tr>
<tr>
<td>1</td>
<td>12</td>
<td>$J(C_6)$</td>
<td>$C_6 \times C_2$</td>
<td>7</td>
<td>1</td>
<td>2, 18, 200, 2450</td>
<td>1, 5, 16, 77</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
<td>$J(D_2)$</td>
<td>$D_2 \times C_2$</td>
<td>7</td>
<td>1</td>
<td>1, 12, 160, 2240</td>
<td>1, 5, 13, 67</td>
</tr>
<tr>
<td>1</td>
<td>12</td>
<td>$J(D_3)$</td>
<td>$D_6$</td>
<td>9</td>
<td>1</td>
<td>1, 9, 110, 1505</td>
<td>1, 4, 10, 48</td>
</tr>
<tr>
<td>1</td>
<td>16</td>
<td>$J(D_4)$</td>
<td>$D_4 \times C_2$</td>
<td>13</td>
<td>1</td>
<td>1, 9, 100, 1260</td>
<td>1, 4, 10, 45</td>
</tr>
<tr>
<td>1</td>
<td>24</td>
<td>$J(D_6)$</td>
<td>$D_6 \times C_2$</td>
<td>19</td>
<td>1</td>
<td>1, 9, 100, 1225</td>
<td>1, 4, 10, 44</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>$C_{2,1}$</td>
<td>$C_2$</td>
<td>1</td>
<td>0</td>
<td>4, 48, 640, 8960</td>
<td>3, 11, 48, 235</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>$C_{4,1}$</td>
<td>$C_4$</td>
<td>3</td>
<td>0</td>
<td>2, 24, 320, 4480</td>
<td>1, 5, 22, 115</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>$C_{6,1}$</td>
<td>$C_6$</td>
<td>3</td>
<td>0</td>
<td>2, 18, 220, 3010</td>
<td>1, 5, 18, 85</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>$D_{2,1}$</td>
<td>$D_2$</td>
<td>3</td>
<td>0</td>
<td>2, 18, 320, 4480</td>
<td>2, 7, 26, 123</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
<td>$D_{4,1}$</td>
<td>$D_4$</td>
<td>7</td>
<td>0</td>
<td>1, 12, 160, 2240</td>
<td>1, 4, 13, 63</td>
</tr>
<tr>
<td>1</td>
<td>12</td>
<td>$D_{6,1}$</td>
<td>$D_6$</td>
<td>9</td>
<td>0</td>
<td>1, 9, 110, 1505</td>
<td>1, 4, 11, 48</td>
</tr>
<tr>
<td>1</td>
<td>6</td>
<td>$D_{3,2}$</td>
<td>$D_3$</td>
<td>3</td>
<td>0</td>
<td>2, 18, 220, 3010</td>
<td>2, 6, 21, 90</td>
</tr>
<tr>
<td>1</td>
<td>8</td>
<td>$D_{4,2}$</td>
<td>$D_4$</td>
<td>5</td>
<td>0</td>
<td>2, 18, 200, 2520</td>
<td>2, 6, 20, 83</td>
</tr>
<tr>
<td>1</td>
<td>12</td>
<td>$D_{6,2}$</td>
<td>$D_6$</td>
<td>7</td>
<td>0</td>
<td>2, 18, 200, 2450</td>
<td>2, 6, 20, 82</td>
</tr>
<tr>
<td>1</td>
<td>12</td>
<td>$T$</td>
<td>$A_4$</td>
<td>3</td>
<td>0</td>
<td>2, 12, 120, 1540</td>
<td>1, 4, 12, 52</td>
</tr>
<tr>
<td>1</td>
<td>24</td>
<td>$O$</td>
<td>$S_4$</td>
<td>9</td>
<td>0</td>
<td>2, 12, 100, 1050</td>
<td>1, 4, 11, 45</td>
</tr>
<tr>
<td>1</td>
<td>24</td>
<td>$O_1$</td>
<td>$S_4$</td>
<td>15</td>
<td>0</td>
<td>1, 6, 60, 770</td>
<td>1, 3, 8, 30</td>
</tr>
<tr>
<td>1</td>
<td>24</td>
<td>$J(T)$</td>
<td>$A_4 \times C_2$</td>
<td>15</td>
<td>1</td>
<td>1, 6, 60, 770</td>
<td>1, 3, 7, 29</td>
</tr>
<tr>
<td>1</td>
<td>48</td>
<td>$J(O)$</td>
<td>$S_4 \times C_2$</td>
<td>33</td>
<td>1</td>
<td>1, 6, 50, 525</td>
<td>1, 3, 7, 26</td>
</tr>
</tbody>
</table>
Sato-Tate groups in dimension 2 with $G^0 \neq U(1)_2$.

<table>
<thead>
<tr>
<th>$d$</th>
<th>$c$</th>
<th>$G$</th>
<th>$G/G^0$</th>
<th>$z_1$</th>
<th>$z_2$</th>
<th>$M[a_1^2]$</th>
<th>$M[a_2]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>$E_1$</td>
<td>$C_1$</td>
<td>0</td>
<td>0, 0, 0, 0, 0</td>
<td>4, 32, 320, 3584</td>
<td>3, 10, 37, 150</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>$E_2$</td>
<td>$C_2$</td>
<td>1</td>
<td>0, 0, 0, 0, 0</td>
<td>2, 16, 160, 1792</td>
<td>1, 6, 17, 78</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>$E_3$</td>
<td>$C_3$</td>
<td>0</td>
<td>0, 0, 0, 0, 0</td>
<td>2, 12, 110, 1204</td>
<td>1, 4, 13, 52</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>$E_4$</td>
<td>$C_4$</td>
<td>1</td>
<td>0, 0, 0, 0, 0</td>
<td>2, 12, 100, 1008</td>
<td>1, 4, 11, 46</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>$E_6$</td>
<td>$C_6$</td>
<td>1</td>
<td>0, 0, 0, 0, 0</td>
<td>2, 12, 100, 980</td>
<td>1, 4, 11, 44</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>$J(E_1)$</td>
<td>$C_2$</td>
<td>1</td>
<td>0, 0, 0, 0, 0</td>
<td>2, 16, 160, 1792</td>
<td>2, 6, 20, 78</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>$J(E_2)$</td>
<td>$D_2$</td>
<td>3</td>
<td>0, 0, 0, 0, 0</td>
<td>1, 8, 80, 896</td>
<td>1, 4, 10, 42</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>$J(E_3)$</td>
<td>$D_3$</td>
<td>3</td>
<td>0, 0, 0, 0, 0</td>
<td>1, 6, 55, 602</td>
<td>1, 3, 8, 29</td>
</tr>
<tr>
<td>3</td>
<td>8</td>
<td>$J(E_4)$</td>
<td>$D_4$</td>
<td>5</td>
<td>0, 0, 0, 0, 0</td>
<td>1, 6, 50, 504</td>
<td>1, 3, 7, 26</td>
</tr>
<tr>
<td>3</td>
<td>12</td>
<td>$J(E_6)$</td>
<td>$D_6$</td>
<td>7</td>
<td>0, 0, 0, 0, 0</td>
<td>1, 6, 50, 490</td>
<td>1, 3, 7, 25</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>$F$</td>
<td>$C_1$</td>
<td>0</td>
<td>0, 0, 0, 0, 0</td>
<td>4, 36, 400, 4900</td>
<td>2, 8, 32, 148</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$F_a$</td>
<td>$C_2$</td>
<td>0</td>
<td>0, 0, 0, 0, 1</td>
<td>3, 21, 210, 2485</td>
<td>2, 6, 20, 82</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$F_c$</td>
<td>$C_2$</td>
<td>1</td>
<td>0, 0, 0, 0, 0</td>
<td>2, 18, 200, 2450</td>
<td>1, 5, 16, 77</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>$F_{ab}$</td>
<td>$C_2$</td>
<td>1</td>
<td>0, 0, 0, 0, 1</td>
<td>2, 18, 200, 2450</td>
<td>2, 6, 20, 82</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>$F_{ac}$</td>
<td>$C_4$</td>
<td>3</td>
<td>0, 0, 2, 0, 1</td>
<td>1, 9, 100, 1225</td>
<td>1, 3, 10, 41</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>$F_{a,b}$</td>
<td>$D_2$</td>
<td>1</td>
<td>0, 0, 0, 0, 3</td>
<td>2, 12, 110, 1260</td>
<td>2, 5, 14, 49</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>$F_{ab,c}$</td>
<td>$D_2$</td>
<td>3</td>
<td>0, 0, 0, 0, 1</td>
<td>1, 9, 100, 1225</td>
<td>1, 4, 10, 44</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>$F_{a,b,c}$</td>
<td>$D_4$</td>
<td>5</td>
<td>0, 0, 2, 0, 3</td>
<td>1, 6, 55, 630</td>
<td>1, 3, 7, 26</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>$G_4$</td>
<td>$C_1$</td>
<td>0</td>
<td>0, 0, 0, 0, 0</td>
<td>3, 20, 175, 1764</td>
<td>2, 6, 20, 76</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>$N(G_4)$</td>
<td>$C_2$</td>
<td>0</td>
<td>0, 0, 0, 0, 1</td>
<td>2, 11, 90, 889</td>
<td>2, 5, 14, 46</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>$G_6$</td>
<td>$C_1$</td>
<td>0</td>
<td>0, 0, 0, 0, 0</td>
<td>2, 10, 70, 588</td>
<td>2, 5, 14, 44</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>$N(G_6)$</td>
<td>$C_2$</td>
<td>1</td>
<td>0, 0, 0, 0, 0</td>
<td>1, 5, 35, 294</td>
<td>1, 3, 7, 23</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>USp(4)</td>
<td>$C_1$</td>
<td>0</td>
<td>0, 0, 0, 0, 0</td>
<td>1, 3, 14, 84</td>
<td>1, 2, 4, 10</td>
</tr>
</tbody>
</table>
### Genus 2 curves realizing Sato-Tate groups with $G^0 = \text{U}(1)_2$

<table>
<thead>
<tr>
<th>Group</th>
<th>Curve $y^2 = f(x)$</th>
<th>$k$</th>
<th>$K$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_1$</td>
<td>$x^6 + 1$</td>
<td>$\mathbb{Q}(\sqrt{-3})$</td>
<td>$\mathbb{Q}(\sqrt{-3})$</td>
</tr>
<tr>
<td>$C_2$</td>
<td>$x^5 - x$</td>
<td>$\mathbb{Q}(\sqrt{-2})$</td>
<td>$\mathbb{Q}(i, \sqrt{2})$</td>
</tr>
<tr>
<td>$C_3$</td>
<td>$x^6 + 4$</td>
<td>$\mathbb{Q}(\sqrt{-3})$</td>
<td>$\mathbb{Q}(\sqrt{-3}, \sqrt{2})$</td>
</tr>
<tr>
<td>$C_4$</td>
<td>$x^6 + x^5 - 5x^4 - 5x^2 - x + 1$</td>
<td>$\mathbb{Q}(\sqrt{-2})$</td>
<td>$\mathbb{Q}(\sqrt{-2}, a); a^4 + 17a^2 + 68 = 0$</td>
</tr>
<tr>
<td>$C_6$</td>
<td>$x^6 + 2$</td>
<td>$\mathbb{Q}(\sqrt{-3})$</td>
<td>$\mathbb{Q}(\sqrt{-3}, \sqrt{2})$</td>
</tr>
<tr>
<td>$D_2$</td>
<td>$x^5 + 9x$</td>
<td>$\mathbb{Q}(\sqrt{-2})$</td>
<td>$\mathbb{Q}(i, \sqrt{2}, \sqrt{3})$</td>
</tr>
<tr>
<td>$D_3$</td>
<td>$x^6 + 10x^3 - 2$</td>
<td>$\mathbb{Q}(\sqrt{-2})$</td>
<td>$\mathbb{Q}(\sqrt{-3}, \sqrt{6}, -2)$</td>
</tr>
<tr>
<td>$D_4$</td>
<td>$x^6 + 3x^5 - 10x^3 - 15x^2 + 15x - 6$</td>
<td>$\mathbb{Q}(\sqrt{-3})$</td>
<td>$\mathbb{Q}(i, \sqrt{2}, \sqrt{3}, a); a^3 + 3a - 2 = 0$</td>
</tr>
<tr>
<td>$D_6$</td>
<td>$x^6 + 6x^5 - 20x^4 + 20x^3 - 20x^2 - 8x + 8$</td>
<td>$\mathbb{Q}(\sqrt{-2})$</td>
<td>$\mathbb{Q}(\sqrt{-2}, a, b); a^3 - 7a + 7 = b^4 + 4b^2 + 8b + 8 = 0$</td>
</tr>
<tr>
<td>$O$</td>
<td>$x^6 - 5x^4 + 10x^3 - 5x^2 + 2x - 1$</td>
<td>$\mathbb{Q}(\sqrt{-2})$</td>
<td>$\mathbb{Q}(\sqrt{-2}, \sqrt{-11}, a, b); a^3 - 4a + 4 = b^4 + 22b + 22 = 0$</td>
</tr>
</tbody>
</table>

- $J(C_1)$: $x^5 - x$ | $\mathbb{Q}(i)$ | $\mathbb{Q}(i, \sqrt{2})$
- $J(C_2)$: $x^5 - x$ | $\mathbb{Q}(\sqrt{-3})$ | $\mathbb{Q}(\sqrt{-3}, \sqrt{6}, -2)$
- $J(C_3)$: $x^6 + 10x^3 - 2$ | $\mathbb{Q}(\sqrt{-2})$ | $\mathbb{Q}(i, \sqrt{2}, \sqrt{3})$
- $J(C_4)$: $x^6 + x^5 - 5x^4 - 5x^2 - x + 1$ | $\mathbb{Q}(i, \sqrt{3}, a); a^3 + 3a^2 - 1 = 0$
- $J(C_6)$: $x^6 - 15x^4 - 20x^3 + 6x + 1$ | $\mathbb{Q}(i, \sqrt{2}, \sqrt{3})$
- $J(D_2)$: $x^5 + 9x$ | $\mathbb{Q}(\sqrt{-3}, \sqrt{6}, -2)$
- $J(D_3)$: $x^6 + 10x^3 - 2$ | $\mathbb{Q}(\sqrt{-3}, \sqrt{6}, -2)$
- $J(D_4)$: $x^5 + 3x$ | $\mathbb{Q}(\sqrt{-3}, \sqrt{6}, -2)$
- $J(D_6)$: $x^6 + 3x^5 + 10x^3 - 15x^2 + 15x - 6$ | $\mathbb{Q}(\sqrt{-2})$ | $\mathbb{Q}(\sqrt{-2}, a, b); a^3 - 7a + 7 = b^4 + 4b^2 + 8b + 8 = 0$
- $J(T)$: $x^6 + 6x^5 - 20x^4 + 20x^3 - 20x^2 - 8x + 8$ | $\mathbb{Q}(\sqrt{-2})$ | $\mathbb{Q}(\sqrt{-2}, \sqrt{-11}, a, b); a^3 - 4a + 4 = b^4 + 22b + 22 = 0$
- $J(O)$: $x^6 - 5x^4 + 10x^3 - 5x^2 + 2x - 1$ | $\mathbb{Q}(\sqrt{-2})$ | $\mathbb{Q}(\sqrt{-2}, \sqrt{-11}, a, b); a^3 - 4a + 4 = b^4 + 22b + 22 = 0$

- $C_{2,1}$: $x^6 + 1$ | $\mathbb{Q}(\sqrt{-3})$
- $C_{4,1}$: $x^5 + 2x$ | $\mathbb{Q}(i, \sqrt{3})$
- $C_{6,1}$: $x^6 + 6x^5 - 30x^4 + 20x^3 + 15x^2 - 12x + 1$ | $\mathbb{Q}(\sqrt{-3}, a); a^3 - 3a + 1 = 0$
- $D_{2,1}$: $x^5 + x$ | $\mathbb{Q}(i, \sqrt{2})$
- $D_{4,1}$: $x^5 + 2x$ | $\mathbb{Q}(\sqrt{-2})$
- $D_{6,1}$: $x^6 + 6x^5 - 30x^4 - 40x^3 + 60x^2 + 24x - 8$ | $\mathbb{Q}(\sqrt{-2}, \sqrt{-3}, a); a^3 - 9a + 6 = 0$
- $D_{3,2}$: $x^6 + 4$ | $\mathbb{Q}(\sqrt{-3}, \sqrt{3})$
- $D_{4,2}$: $x^6 + x^5 + 10x^3 + 5x^2 + x - 2$ | $\mathbb{Q}(\sqrt{-2}, a); a^4 - 14a^2 + 28a - 14 = 0$
- $D_{6,2}$: $x^6 + 2$ | $\mathbb{Q}(\sqrt{-3}, \sqrt{6})$
- $O_1$: $x^6 + 7x^5 + 10x^4 + 10x^3 + 15x^2 + 17x + 4$ | $\mathbb{Q}(\sqrt{-2}, a, b); a^3 + 5a + 10 = b^4 + 4b^2 + 8b + 2 = 0$
Genus 2 curves realizing Sato-Tate groups with $G^0 \neq U(1)_2$

<table>
<thead>
<tr>
<th>Group</th>
<th>Curve $y^2 = f(x)$</th>
<th>$k$</th>
<th>$K$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F$</td>
<td>$x^6 + 3x^4 + x^2 - 1$</td>
<td>$\mathbb{Q}(i, \sqrt{2})$</td>
<td>$\mathbb{Q}(i, \sqrt{2})$</td>
</tr>
<tr>
<td>$F_a$</td>
<td>$x^6 + 3x^4 + x^2 - 1$</td>
<td>$\mathbb{Q}(i)$</td>
<td>$\mathbb{Q}(i, \sqrt{2})$</td>
</tr>
<tr>
<td>$F_{ab}$</td>
<td>$x^6 + 3x^4 + x^2 - 1$</td>
<td>$\mathbb{Q}(\sqrt{2})$</td>
<td>$\mathbb{Q}(i, \sqrt{2})$</td>
</tr>
<tr>
<td>$F_{ac}$</td>
<td>$x^5 + 1$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}(a); a^4 + 5a^2 + 5 = 0$</td>
</tr>
<tr>
<td>$F_{a,b}$</td>
<td>$x^6 + 3x^4 + x^2 - 1$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}(i, \sqrt{2})$</td>
</tr>
<tr>
<td>$E_1$</td>
<td>$x^6 + x^4 + x^2 + 1$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}$</td>
</tr>
<tr>
<td>$E_2$</td>
<td>$x^6 + 3x^4 + 3x^2 - x + 1$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}(\sqrt{2})$</td>
</tr>
<tr>
<td>$E_3$</td>
<td>$x^5 + x^4 - 3x^3 - 4x^2 - x$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}(a); a^3 - 3a + 1 = 0$</td>
</tr>
<tr>
<td>$E_4$</td>
<td>$x^5 + x^4 + x^2 - x$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}(a); a^4 - 5a^2 + 5 = 0$</td>
</tr>
<tr>
<td>$E_6$</td>
<td>$x^5 + 2x^4 - 3x^2 - x$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}(\sqrt{7}, a); a^3 - 7a - 7 = 0$</td>
</tr>
<tr>
<td>$J(E_1)$</td>
<td>$x^5 + x^3 + x$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}(i)$</td>
</tr>
<tr>
<td>$J(E_2)$</td>
<td>$x^5 + x^3 - x$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}(i, \sqrt{2})$</td>
</tr>
<tr>
<td>$J(E_3)$</td>
<td>$x^6 + x^3 + 4$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}(\sqrt{-3}, \sqrt{2})$</td>
</tr>
<tr>
<td>$J(E_4)$</td>
<td>$x^5 + x^3 + 2x$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}(i, 4\sqrt{2})$</td>
</tr>
<tr>
<td>$J(E_6)$</td>
<td>$x^6 + x^3 - 2$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}(\sqrt{-3}, 6\sqrt{-2})$</td>
</tr>
<tr>
<td>$G_{1,3}$</td>
<td>$x^6 + 3x^4 - 2$</td>
<td>$\mathbb{Q}(i)$</td>
<td>$\mathbb{Q}(i)$</td>
</tr>
<tr>
<td>$N(G_{1,3})$</td>
<td>$x^6 + 3x^4 - 2$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}(i)$</td>
</tr>
<tr>
<td>$G_{3,3}$</td>
<td>$x^6 + x^2 + 1$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}$</td>
</tr>
<tr>
<td>$N(G_{3,3})$</td>
<td>$x^6 + x^5 + x - 1$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}(i)$</td>
</tr>
<tr>
<td>USp(4)</td>
<td>$x^5 - x + 1$</td>
<td>$\mathbb{Q}$</td>
<td>$\mathbb{Q}$</td>
</tr>
</tbody>
</table>
Part Two
Searching for curves

We surveyed the \( \bar{L} \)-polynomial distributions of genus 2 curves

\[
y^2 = x^5 + c_4 x^4 + c_3 x^3 + c_2 x^2 + c_1 x + c_0, \\
y^2 = x^6 + c_5 x^5 + c_4 x^4 + c_3 x^3 + c_2 x^2 + c_1 x + c_0,
\]

with integer coefficients \(|c_i| \leq 128\). More than \(2^{48}\) curves.

We found over 10 million non-isomorphic curves with exceptional distributions, including at least 3 apparent matches for each of the 34 Sato-Tate groups that can occur over \(\mathbb{Q}\).

Representative examples were computed to high precision \(N = 2^{30}\).

For each example, the field \(K\) was then determined, allowing the Galois type, and hence the Sato-Tate group, to be provably identified.
Exhibiting Sato-Tate groups of abelian surfaces

The 34 Sato-Tate groups that can arise for an abelian surface over $\mathbb{Q}$ are all realized by Jacobians of genus 2 curves.

By extending the base field from $\mathbb{Q}$ to a suitable subfield $k$ of $K$, we can restrict $G/G^0 \simeq \text{Gal}(K/k)$ to any normal subgroup of $\text{Gal}(K/k)$ (base extension does not change the identity component $G^0$).

This allows us to realize all 52 Sato-Tate groups using base extensions of 34 curves defined over $\mathbb{Q}$ (in fact, 9 suffice).

Serre asks: can all 52 can be realized over a single base field $k$?

Theorem (Fité-Guitart 2015)

All 52 possible Sato-Tate groups arise for abelian surfaces defined over

$$k := \mathbb{Q}(\sqrt{-10}, \sqrt{-51}, \sqrt{-163}, \sqrt{-67}, \sqrt{817}, \sqrt{-57}).$$
Computing zeta functions
Algorithms to compute $L_p(T)$ for low genus hyperelliptic curves

<table>
<thead>
<tr>
<th>algorithm</th>
<th>$g = 1$</th>
<th>$g = 2$</th>
<th>$g = 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>point enumeration</td>
<td>$p \log p$</td>
<td>$p^2 \log p$</td>
<td>$p^3 \log p$</td>
</tr>
<tr>
<td>group computation</td>
<td>$p^{1/4} \log p$</td>
<td>$p^{3/4} \log p$</td>
<td>$p^{5/4} \log p$</td>
</tr>
<tr>
<td>$p$-adic cohomology</td>
<td>$p^{1/2} \log^2 p$</td>
<td>$p^{1/2} \log^2 p$</td>
<td>$p^{1/2} \log^2 p$</td>
</tr>
<tr>
<td>CRT (Schoof-Pila)</td>
<td>$\log^5 p$</td>
<td>$\log^8 p$</td>
<td>$\log^{12} p$</td>
</tr>
</tbody>
</table>

Complexity (ignoring factors of $O(\log \log p)$)

<table>
<thead>
<tr>
<th>algorithm</th>
<th>$g = 1$</th>
<th>$g = 2$</th>
<th>$g = 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>point enumeration</td>
<td>$p \log p$</td>
<td>$p^2 \log p$</td>
<td>$p^3 \log p$</td>
</tr>
<tr>
<td>group computation</td>
<td>$p^{1/4} \log p$</td>
<td>$p^{3/4} \log p$</td>
<td>$p^{5/4} \log p$</td>
</tr>
<tr>
<td>$p$-adic cohomology</td>
<td>$p^{1/2} \log^2 p$</td>
<td>$p^{1/2} \log^2 p$</td>
<td>$p^{1/2} \log^2 p$</td>
</tr>
<tr>
<td>CRT (Schoof-Pila)</td>
<td>$\log^5 p$</td>
<td>$\log^8 p$</td>
<td>$\log^{12} p$</td>
</tr>
</tbody>
</table>

(see [Kedlaya-S 2008])
An average polynomial-time algorithm

All of these methods perform separate computations for each $p$. But we want to compute $L_p(T)$ for all good $p \leq N$ using reductions of the same curve in each case. Can we take advantage of this?

**Theorem (Harvey 2012)**

*There exists a deterministic algorithm that, given a hyperelliptic curve $y^2 = f(x)$ of genus $g$ with a rational Weierstrass point and an integer $N$, computes $L_p(T)$ for all good primes $p \leq N$ in time*

$$O\left(g^{8+\epsilon}N \log^{3+\epsilon} N\right),$$

*assuming the coefficients of $f \in \mathbb{Z}[x]$ have size bounded by $O(\log N)$.*

Average time is $O\left(g^{8+\epsilon} \log^{4+\epsilon} N\right)$ per prime, polynomial in $g$ and $\log p$. Recently generalized to arithmetic schemes.
An average polynomial-time algorithm

<table>
<thead>
<tr>
<th>algorithm</th>
<th>complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( g = 1 )</td>
</tr>
<tr>
<td>point enumeration</td>
<td>( p \log p )</td>
</tr>
<tr>
<td>group computation</td>
<td>( p^{1/4} \log p )</td>
</tr>
<tr>
<td>( p )-adic cohomology</td>
<td>( p^{1/2} \log^2 p )</td>
</tr>
<tr>
<td>CRT (Schoof-Pila)</td>
<td>( \log^5 p )</td>
</tr>
<tr>
<td>Average polytime</td>
<td>( \log^4 p )</td>
</tr>
</tbody>
</table>

But is it practical?
The Hasse-Witt matrix of a hyperelliptic curve

The Hasse-Witt matrix of a hyperelliptic curve \( y^2 = f(x) \) over \( \mathbb{F}_p \) of genus \( g \) is the \( g \times g \) matrix \( W_p = [w_{ij}] \) with entries

\[
  w_{ij} = f_{pi-j}^{(p-1)/2} \mod p \quad (1 \leq i, j \leq g).
\]

The \( w_{ij} \) can each be computed using recurrence relations between the coefficients of \( f^n \) and those of \( f^{n-1} \).

The congruence

\[
  L_P(T) \equiv \det(I - TW_p) \mod p
\]

allows us to determine the coefficients \( a_1, \ldots, a_g \) of \( L_p(T) \) modulo \( p \). This is enough to compute \( \#C_p(\mathbb{F}_p) \) for \( p > 16g^2 \).

The algorithm can be extended to compute \( L_p(T) \) modulo higher powers of \( p \) (and thereby obtain \( L_p \in \mathbb{Z}[T] \)), but for \( g \leq 3 \) it’s easier to derive \( L_p(T) \) from \( L_p(T) \mod p \) using computations in \( \text{Jac}(C) \).
Complexity

Theorem (Harvey-S 2014)

Given a hyperelliptic curve $y^2 = f(x)$ of genus $g$, and an integer $N$, one can compute the Hasse-Witt matrices $W_p$ for all good primes $p \leq N$ in

$$O(g^3 N \log^3 N \log \log N) \text{ time} \quad \text{and} \quad O(g^2 N) \text{ space},$$

assuming $g$ and the bit-size of each coefficient of $f$ are $O(\log N)$.

The complexity is close to optimal (nearly quasi-linear in output size).

Extends to computing $L_p \in \mathbb{Z}[T]$ in $O(g^{4+\epsilon} N \log^{3+\epsilon} N)$ time.

In progress: smooth plane quartics.
<table>
<thead>
<tr>
<th>$N$</th>
<th>genus 2</th>
<th>genus 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>smalljac</td>
<td>hwlpoly</td>
</tr>
<tr>
<td>$2^{14}$</td>
<td>0.2</td>
<td>0.1</td>
</tr>
<tr>
<td>$2^{15}$</td>
<td>0.6</td>
<td>0.3</td>
</tr>
<tr>
<td>$2^{16}$</td>
<td>1.7</td>
<td>0.9</td>
</tr>
<tr>
<td>$2^{17}$</td>
<td>5.5</td>
<td>2.2</td>
</tr>
<tr>
<td>$2^{18}$</td>
<td>19.2</td>
<td>5.3</td>
</tr>
<tr>
<td>$2^{19}$</td>
<td>78.4</td>
<td>12.5</td>
</tr>
<tr>
<td>$2^{20}$</td>
<td>271</td>
<td>27.8</td>
</tr>
<tr>
<td>$2^{21}$</td>
<td>1120</td>
<td>64.5</td>
</tr>
<tr>
<td>$2^{22}$</td>
<td>2820</td>
<td>155</td>
</tr>
<tr>
<td>$2^{23}$</td>
<td>9840</td>
<td>357</td>
</tr>
<tr>
<td>$2^{24}$</td>
<td>31900</td>
<td>823</td>
</tr>
<tr>
<td>$2^{25}$</td>
<td>105000</td>
<td>1890</td>
</tr>
<tr>
<td>$2^{26}$</td>
<td>349000</td>
<td>4250</td>
</tr>
<tr>
<td>$2^{27}$</td>
<td>1210000</td>
<td>9590</td>
</tr>
<tr>
<td>$2^{28}$</td>
<td>4010000</td>
<td>21200</td>
</tr>
<tr>
<td>$2^{29}$</td>
<td>13200000</td>
<td>48300</td>
</tr>
<tr>
<td>$2^{30}$</td>
<td>45500000</td>
<td>108000</td>
</tr>
</tbody>
</table>

(Intel Xeon E5-2697v2 2.7 GHz CPU seconds).
Naïve approach

For each good prime $p < N$ we want to compute the entries

$$w_{ij} = f_{p^{i-j}}^{(p-1)/2} \mod p \quad (1 \leq i, j \leq g).$$

of the Hasse-Witt matrix $W_p = [w_{ij}]$.

So we could iteratively compute $f, f^2, f^3, \ldots, f^{(N-1)/2}$ in $\mathbb{Z}[x]$ and just reduce the $x^{pi-j}$ coefficients of $f(x)^{(p-1)/2} \mod p$ for each prime $p \leq N$.

But the polynomials $f^n$ are huge, each has $\Omega(n^2)$ bits.
It would take $\Omega(N^3)$ time to compute $f, \ldots, f^{(N-1)/2}$ in $\mathbb{Z}[x]$.

So this is a terrible idea...

But we don’t need all the coefficients of $f^n$, we only need one, and we only need to know its value modulo $p = 2n + 1$. 
A better approach

For any integer $n \geq 0$ the equations

\[ f^{n+1} = f \cdot f^n \quad \text{and} \quad (f^{n+1})' = (n + 1)f' f^n \]

yield the relations

\[ f_k^{n+1} = \sum_{j=0}^{d} f_j f_{k-j}^{n} \quad \text{and} \quad k f_k^{n+1} = (n + 1) \sum_{j=0}^{d} j f_j f_{k-j}^{n}, \]

where $f_k^n$ denotes the coefficient of $x^k$ in $f^n$. Subtracting $k$ times the first from the second and solving for $f_k^n$ yields the identity

\[ f_k^n = \frac{1}{k f_0} \sum_{j=1}^{d} (nj + j - k) f_j f_{k-j}^{n}, \quad (1) \]

which is valid for all positive integers $k$ and $n$ (assuming $f_0 \neq 0$).
If we now define
\[ v_k^n := [f_{k-d+1}, \ldots, f_k^n] \in \mathbb{Z}^d, \]
then the last \( g \) entries of \( v_{p-1}^{(p-1)/2} \mod p \) form the first row of \( W_p \), and
\[ f_k^n \equiv \frac{1}{2k f_0} \sum_{j=1}^{d} (j - 2k) f_j f_k^{n-j} \mod p, \]
holds for \( k \leq p - 1 = 2n \). Starting from \( v_0^n = [0, \ldots, 0, f_0^n] \), we compute
\[ v_{p-1}^n \equiv \frac{v_0^n}{2^{p-1}(p-1)! f_0^{p-1}} \prod_{k=1}^{p-1} M_k \equiv -v_0^n \prod_{i=1}^{p-1} M_k \mod p, \]
where the \( d \times d \) matrices
\[ M_k := \begin{bmatrix} 0 & \cdots & 0 & (d - 2k) f_d \\ 2k f_0 & \cdots & 0 & (d - 1 - 2k) f_{d-1} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 2k f_0 & (1 - 2k) f_1 \end{bmatrix} \]
do not depend on \( p \)!
Computing a sequence of reduced partial products

Computing the first row of $W_p$ for all $p < N$ reduces to compute the sequence of reduced partial products

$$M_1 M_2 \mod 3$$
$$M_1 M_2 M_3 M_4 \mod 5$$
$$M_1 M_2 M_3 M_4 M_5 M_6 \mod 7$$
$$\vdots$$
$$M_1 M_2 M_3 M_4 M_5 M_6 \cdots M_{N-2} \mod N - 1$$

Doing this naively would take time quasi-quadratic in $N$.

But quasi-linear time is achieved with an accumulating remainder tree.
Accumulating remainder trees

**Input:** integer matrices $M_0, \ldots, M_{N-1}$ and moduli $m_0, \ldots, m_{N-1}$.

**Output:** $A_0, A_1, \ldots, A_{N-1}$, where $A_i := \prod_{j<i} M_j \mod m_i$.

**Algorithm:**

1. If $N = 1$ then output $A_0 := 1$ and terminate (base case).
2. Use $M'_i := M_{2i}M_{2i+1}$ and $m'_i := m_{2i}m_{2i+1}$ to recursively compute $A'_1, \ldots, A'_{N/2}$.
3. Output

$$A_i := \begin{cases} A'_{i/2} \mod m_i & i \text{ even;} \\ A'_{(i-1)/2}M_{i-1} \mod m_i & i \text{ odd.} \end{cases}$$

Using FFT-multiplication, this runs in quasi-linear time.

The space complexity can be improved using a *remainder forest*. 
click histogram to animate (requires adobe reader)
click histogram to animate (requires adobe reader)
click histogram to animate (requires adobe reader)
click histogram to animate (requires adobe reader)
click histogram to animate (requires adobe reader)
### Real endomorphism algebras of abelian threefolds

<table>
<thead>
<tr>
<th>abelian threefold</th>
<th>( \text{End}(A_K)_\mathbb{R} )</th>
<th>( \text{ST}^0_A )</th>
</tr>
</thead>
<tbody>
<tr>
<td>cube of a CM elliptic curve</td>
<td>( M_3(\mathbb{C}) )</td>
<td>( U(1)_3 )</td>
</tr>
<tr>
<td>cube of a non-CM elliptic curve</td>
<td>( M_3(\mathbb{R}) )</td>
<td>( SU(2)_3 )</td>
</tr>
<tr>
<td>product of CM elliptic curve and square of CM elliptic curve</td>
<td>( \mathbb{C} \times M_2(\mathbb{C}) )</td>
<td>( U(1) \times U(1)_2 )</td>
</tr>
<tr>
<td>• product of CM elliptic curve and QM abelian surface</td>
<td>( \mathbb{C} \times M_2(\mathbb{R}) )</td>
<td>( U(1) \times SU(2)_2 )</td>
</tr>
<tr>
<td>• product of CM elliptic curve and square of non-CM elliptic curve</td>
<td>( \mathbb{R} \times M_2(\mathbb{C}) )</td>
<td>( SU(2) \times U(1)_2 )</td>
</tr>
<tr>
<td>product of non-CM elliptic curve and square of CM elliptic curve</td>
<td>( \mathbb{R} \times M_2(\mathbb{R}) )</td>
<td>( SU(2) \times SU(2)_2 )</td>
</tr>
<tr>
<td>• CM abelian threefold</td>
<td>( \mathbb{C} \times \mathbb{C} \times \mathbb{C} )</td>
<td>( U(1) \times U(1) \times U(1) )</td>
</tr>
<tr>
<td>• product of CM elliptic curve and CM abelian surface</td>
<td>( \mathbb{C} \times \mathbb{C} \times \mathbb{R} )</td>
<td>( U(1) \times U(1) \times SU(2) )</td>
</tr>
<tr>
<td>• product of non-CM elliptic curve and two CM elliptic curves</td>
<td>( \mathbb{C} \times \mathbb{R} \times \mathbb{R} )</td>
<td>( U(1) \times SU(2) \times SU(2) )</td>
</tr>
<tr>
<td>• product of CM elliptic curve and RM abelian surface</td>
<td>( \mathbb{R} \times \mathbb{R} \times \mathbb{R} )</td>
<td>( SU(2) \times SU(2) \times SU(2) )</td>
</tr>
<tr>
<td>• RM abelian threefold</td>
<td>( \mathbb{R} \times \mathbb{R} \times \mathbb{R} )</td>
<td>( SU(2) \times SU(2) \times SU(2) )</td>
</tr>
<tr>
<td>• product of non-CM elliptic curve and RM abelian surface</td>
<td>( \mathbb{C} \times \mathbb{R} )</td>
<td>( U(1) \times USp(4) )</td>
</tr>
<tr>
<td>• product of CM elliptic curve and abelian surface</td>
<td>( \mathbb{R} \times \mathbb{R} )</td>
<td>( SU(2) \times USp(4) )</td>
</tr>
<tr>
<td>quadratic CM abelian threefold</td>
<td>( \mathbb{C} )</td>
<td>( U(3) )</td>
</tr>
<tr>
<td>generic abelian threefold</td>
<td>( \mathbb{R} )</td>
<td>( USp(6) )</td>
</tr>
</tbody>
</table>
Connected Sato-Tate groups of abelian threefolds:

- $U(1)_3$
- $SU(2)_3$
- $U(1) \times U(1)_2$
- $U(1) \times SU(2)_2$
- $SU(2) \times U(1)_2$
- $SU(2) \times SU(2)_2$
- $U(1) \times U(1) \times U(1)$
- $U(1) \times U(1) \times SU(2)$
- $U(1) \times SU(2) \times U(1)$
- $SU(2) \times SU(2) \times SU(2)$
- $U(1) \times USp(4)$
- $SU(2) \times USp(4)$
- $U(3)$
- $USp(6)$
Partial classification of component groups

| $G_0$                      | $G/G_0 \hookrightarrow$ | $|G/G_0|$ divides |
|----------------------------|--------------------------|-----------------|
| USp(6)                     | $C_1$                    | 1               |
| U(3)                       | $C_2$                    | 2               |
| SU(2) × USp(4)             | $C_1$                    | 1               |
| U(1) × USp(4)              | $C_2$                    | 2               |
| SU(2) × SU(2) × SU(2)      | $S_3$                    | 6               |
| U(1) × SU(2) × SU(2)       | $D_2$                    | 4               |
| U(1) × U(1) × SU(2)        | $D_4$                    | 8               |
| U(1) × U(1) × U(1)         | $C_2 \wr S_3$            | 48              |
| SU(2) × SU(2)_2            | $D_4$, $D_6$             | 8, 12           |
| SU(2) × U(1)_2             | $D_6 \times C_2$, $S_4 \times C_2$ | 48 |
| U(1) × SU(2)_2             | $D_4 \times C_2$, $D_6 \times C_2$ | 16, 24 |
| U(1) × U(1)_2              | $D_6 \times C_2 \times C_2$, $S_4 \times C_2 \times C_2$ | 96 |
| SU(2)_3                    | $D_6$, $S_4$             | 24              |
| U(1)_3                     | ...                      | 336, 432        |

(disclaimer: this is work in progress subject to verification)