Sato-Tate in dimension 3

Andrew V. Sutherland

Massachusetts Institute of Technology

December 7, 2016

Joint work with F. Fité, K.S. Kedlaya, and V. Rotger, and with D. Harvey.

Mikio Sato

John Tate
Let $E/\mathbb{Q}$ be an elliptic curve, say,
\[ y^2 = x^3 + Ax + B, \]
and let $p$ be a prime of good reduction (so $p \nmid \Delta(E)$).

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 $t_p$ is an integer in $[-2\sqrt{p}, 2\sqrt{p}]$.

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 $N \to \infty$. 
The histogram of $y^2 = x^3 + x + 1$ for $p \leq 2^{10}$ shows 170 data points in 13 buckets, with $z_1 = 0.029$, indicating out of range data has an area of 0.018.
Histogram of \( y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502 x + 34481611795030556467032985690390720374855944359319180361266008296291939448732243429 \) for \( p \leq 2^{10} \). 172 data points in 13 buckets, \( z_1 = 0.023 \), out of range data has area 0.250.
$a_1$ histogram of $y^2 = x^3 + 1$ for $p \leq 2^{10}$

170 data points in 13 buckets, $z_1 = 0.518$, out of range data has area 0.418

Moments: 1 -0.044 0.934 -0.160 2.754 -0.660 9.051 -2.655 31.232 -10.427 110.831

click histogram to animate (requires adobe reader)
Histogram of $y^2 = x^3 + 1$ over $\mathbb{Q}(\sqrt{-3})$ for split $p \leq 2^{10}$

164 data points in 13 buckets, out of range data has area 0.122
1. Typical case (no CM)

Elliptic curves $E/\mathbb{Q}$ w/o CM have the semi-circular 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 $E$.

A refinement of the Sato-Tate conjecture implies that the distribution of normalized Frobenius traces of $E$ converges to the distribution of traces in its Sato-Tate group $G$ (under its 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>$SU(2)$</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>
<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>$U(1)$</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>
</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

For a smooth projective curve $C/\mathbb{Q}$ of genus $g$ and each prime $p$ of good reduction for $C$ we have the zeta function

$$Z(C_p/\mathbb{F}_p; T) := \exp \left( \sum_{k=1}^{\infty} \#C_p(\mathbb{F}_{p^k}) T^k / k \right) = \frac{L_p(T)}{(1 - T)(1 - pT)},$$

where $L_p \in \mathbb{Z}[T]$ has degree $2g$. 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, and unitary, with $|a_i| \leq \binom{2g}{i}$. 

We now consider the limiting distribution of $a_1, a_2, \ldots, a_g$ over all primes $p \leq N$ of good reduction, as $N \to \infty$. 
a1 histogram of \( y^2 = x^5 - x + 1 \) for \( p \leq 2^{10} \)

187 data points in 13 buckets, \( z_1 = 0.030 \)
a2 histogram of $y^2 = x^5 - x + 1$ for $p <= 2^{10}$
167 data points in 13 buckets

click histogram to animate (requires adobe reader)
Histogram of $y^2 = x^5 + 2x^4 - x^3 - 3x^2 - x$ for $p <= 2^{10}$

188 data points in 13 buckets, $z_1 = 0.196$

Click histogram to animate (requires Adobe Reader)
a2 histogram of $y^2 = x^5 + 2x^4 - x^3 - 3x^2 - x$ for $p \leq 2^{10}$

188 data points in 13 buckets, $z_2 = [0.006 \ 0.000 \ 0.000 \ 0.000 \ 0.012]$
Exceptional distributions for abelian surfaces over $\mathbb{Q}$:
$L$-polynomials of Abelian varieties

Let $A$ be an abelian variety over a number field $k$. Fix a prime $\ell$. The action of $\text{Gal}(\bar{k}/k)$ on the $\ell$-adic Tate module

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

gives rise to a Galois representation

$$\rho_{\ell}: \text{Gal}(\bar{k}/k) \to \text{Aut}_{\mathbb{Q}_{\ell}}(V_{\ell}(A)) \cong \text{GSp}_{2g}(\mathbb{Q}_{\ell})$$

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

$$L_p(T) := \det(1 - \rho_{\ell}(\text{Frob}_p)T), \quad \bar{L}_p(T) := L_p(T/\sqrt{\|p\|}),$$

which appears as an Euler factor in the $L$-series

$$L(A, s) := \prod_p L_p(\|p\|^{-s})^{-1}.$$
The Sato-Tate group of an abelian variety

The Zariski closure of the image of

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

is a $\mathbb{Q}_\ell$-algebraic group $G^\text{zar}_\ell \subseteq \text{GSp}_{2g}$ that determines a $\mathbb{C}$-algebraic group $G^{1,\text{zar}}_{\ell,\iota} \subseteq \text{Sp}_{2g}$ after fixing $\iota : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ and intersecting with $\text{Sp}_{2g}$.

**Definition [Serre]**

$\text{ST}(A) \subseteq \text{USp}(2g)$ is a maximal compact subgroup of $G^{1,\text{zar}}_{\ell,\iota}(\mathbb{C})$.

**Conjecture [Mumford-Tate, Algebraic Sato-Tate]**

$$(G^{\text{zar}}_\ell)^0 = \text{MT}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell,$$ equivalently, $$(G^{1,\text{zar}}_\ell)^0 = H_{g}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$ More generally, $G^{1,\text{zar}}_\ell = \text{AST}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.

This conjecture is known for $g \leq 3$ (see Banaszak-Kedlaya 2015).
A refined Sato-Tate conjecture

Let \( s(p) \) denote the conjugacy class of \( \|p\|^{-1/2}M_p \) in \( \text{ST}(A) \), where \( M_p \) is the image of \( \text{Frob}_p \) in \( G_{\text{zar}}(\mathbb{C}) \) (semisimple, by a theorem of Tate), and let \( \mu_{\text{ST}(A)} \) denote the pushforward of the Haar measure to \( \text{Conj}(\text{ST}(A)) \).

Conjecture

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

In particular, the distribution of normalized Euler factors \( \overline{L}_p(T) \) matches the distribution of characteristic polynomials in \( \text{ST}(A) \).

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

Let $A$ be an abelian variety defined over a number field $k$. Let $K$ be the minimal extension of $k$ for which $\text{End}(A_K) = \text{End}(A_{\overline{k}})$. $\text{Gal}(K/k)$ 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 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 [Fité, Kedlaya, Rotger, S 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 $G^0$ is uniquely determined by $\text{End}(A_K)_\mathbb{R}$ and $G/G^0 \simeq \text{Gal}(K/k)$ (with corresponding actions).
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></td>
<td></td>
</tr>
<tr>
<td>• CM abelian surface</td>
<td>$\mathbb{C} \times \mathbb{C}$</td>
<td>$U(1) \times U(1)$</td>
</tr>
<tr>
<td>• product of CM elliptic curves</td>
<td></td>
<td></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 in $\text{USp}(4)$, there are 52 Sato-Tate groups $ST(A)$ that arise for abelian surfaces $A/k$ over number fields; 34 occur for $k = \mathbb{Q}$.

- $\text{U}(1)_2$: $C_1, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6, T, O, J(C_1), J(C_2), J(C_3), J(C_4), J(C_6), J(D_2), J(D_3), J(D_4), J(D_6), J(T), J(O), C_{2,1}, C_{4,1}, C_{6,1}, D_{2,1}, D_{3,2}, D_{4,1}, D_{4,2}, D_{6,1}, D_{6,2}, O_1$

- $\text{SU}(2)_2$: $E_1, E_2, E_3, E_4, E_6, J(E_1), J(E_2), J(E_3), J(E_4), J(E_6)$

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

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

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

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

This theorem says nothing about equidistribution, however this is now known in many special cases [Fité-S 2012, Johansson 2013].
### Real endomorphism algebras of abelian threefolds

<table>
<thead>
<tr>
<th>abelian threefold</th>
<th>$\text{End}(A_K)_\mathbb{R}$</th>
<th>$\text{ST}(A)^0$</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>$\mathbb{C} \times M_2(\mathbb{C})$</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>$\mathbb{R} \times M_2(\mathbb{C})$</td>
<td>$SU(2) \times SU(2)_2$</td>
</tr>
<tr>
<td>● product of non-CM elliptic curve and QM abelian surface</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 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>$\mathbb{C} \times \mathbb{C} \times \mathbb{R}$</td>
<td>$U(1) \times U(1) \times SU(2)$</td>
</tr>
<tr>
<td>● product of CM elliptic curve and RM abelian surface</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 two non-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>● 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>$\mathbb{R} \times \mathbb{R} \times \mathbb{R}$</td>
<td>$SU(2) \times SU(2) \times SU(2)$</td>
</tr>
<tr>
<td>● product of 3 non-CM elliptic curves</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 CM elliptic curve and abelian surface</td>
<td>$\mathbb{C} \times \mathbb{R}$</td>
<td>$U(1) \times USp(4)$</td>
</tr>
<tr>
<td>product of non-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:

\[ \mathbb{U}(1)^3 \]
\[ \mathbb{SU}(2)^3 \]
\[ \mathbb{U}(1) \times \mathbb{U}(1)^2 \]
\[ \mathbb{U}(1) \times \mathbb{SU}(2)^2 \]
\[ \mathbb{SU}(2) \times \mathbb{U}(1)^2 \]
\[ \mathbb{SU}(2) \times \mathbb{SU}(2)^2 \]
\[ \mathbb{U}(1) \times \mathbb{U}(1) \times \mathbb{U}(1) \]
\[ \mathbb{U}(1) \times \mathbb{U}(1) \times \mathbb{SU}(2) \]
\[ \mathbb{U}(1) \times \mathbb{SU}(2) \times \mathbb{U}(1) \]
\[ \mathbb{SU}(2) \times \mathbb{SU}(2) \times \mathbb{SU}(2) \]
\[ \mathbb{U}(1) \times \text{USp}(4) \]
\[ \mathbb{SU}(2) \times \text{USp}(4) \]
\[ \mathbb{U}(3) \]
\[ \text{USp}(6) \]
Partial classification of component groups

| $G_0$                      | $G/G_0$     | $|G/G_0|$ divides |
|----------------------------|-------------|-----------------|
| USp(6)                     | C_1         | 1               |
| U(3)                       | C_2         | 2               |
| SU(2) $\times$ USp(4)      | C_1         | 1               |
| U(1) $\times$ USp(4)       | C_2         | 2               |
| SU(2) $\times$ SU(2) $\times$ SU(2) | S_3        | 6               |
| U(1) $\times$ SU(2) $\times$ SU(2) | D_2        | 4               |
| U(1) $\times$ U(1) $\times$ SU(2) | D_4        | 8               |
| U(1) $\times$ U(1) $\times$ U(1) | C_2 $\wr$ S_3 | 48             |
| SU(2) $\times$ SU(2)_2     | D_4, D_6    | 8, 12           |
| SU(2) $\times$ U(1)_2      | D_6 $\times$ C_2, S_4 $\times$ C_2 | 48 |
| U(1) $\times$ SU(2)_2      | D_4 $\times$ C_2, D_6 $\times$ C_2 | 16, 24 |
| U(1) $\times$ 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                      | (to be determined) | 336, 1728 |

(disclaimer: work in progress, subject to verification)
Given a curve $C/\mathbb{Q}$ of genus $g$, we want to compute the normalized $L$-polynomials $\overline{L}_p(T)$ at all good primes $p \leq N$.

### Complexity per prime
(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>$p^3 (\log p)^2$</td>
</tr>
<tr>
<td>group computation</td>
<td>$p^{1/4} \log p$</td>
<td>$p^{3/4} \log p$</td>
<td>$p \log p$</td>
</tr>
<tr>
<td>$p$-adic cohomology</td>
<td>$p^{1/2}(\log p)^2$</td>
<td>$p^{1/2}(\log p)^2$</td>
<td>$p^{1/2}(\log p)^2$</td>
</tr>
<tr>
<td>CRT (Schoof-Pila)</td>
<td>$(\log p)^5$</td>
<td>$(\log p)^8$</td>
<td>$(\log p)^{12?}$</td>
</tr>
<tr>
<td>average poly-time</td>
<td>$(\log p)^4$</td>
<td>$(\log p)^4$</td>
<td>$(\log p)^4$</td>
</tr>
</tbody>
</table>
Genus 3 curves

The canonical embedding of a genus 3 curve into $\mathbb{P}^2$ is either

1. a degree-2 cover of a smooth conic (hyperelliptic case);
2. a smooth plane quartic (generic case).

Average polynomial-time implementations available for the first case:

- rational hyperelliptic model [Harvey-S 2014];
- no rational hyperelliptic model [Harvey-Massierer-S 2016].

Here we address the second case.

Prior work has all been based on $p$-adic cohomology:

[Lauder 2004], [Castryck-Denef-Vercauteren 2006],
[Abott-Kedlaya-Roe 2006], [Harvey 2010], [Tuitman-Pancrantz 2013],
[Tuitman 2015], [Costa 2015], [Tuitman-Castryck 2016], [Shieh 2016]
New algorithm

Let $C_p / \mathbb{F}_p$ be a smooth plane quartic defined by $f(x, y, z) = 0$. For $n \geq 0$ let $f_{i,j,k}^n$ denote the coefficient of $x^i y^j z^k$ in $f^n$.

The Hasse–Witt matrix of $C_p$ is the $3 \times 3$ matrix

$$W_p := \begin{bmatrix}
    f_{p-1,p-1,2p-2}^{p-1} & f_{2p-1,p-1,p-2}^{p-1} & f_{p-1,2p-1,p-2}^{p-1} \\
    f_{p-2,p-1,2p-1}^{p-1} & f_{2p-2,p-1,p-1}^{p-1} & f_{p-2,2p-1,p-1}^{p-1} \\
    f_{p-1,p-2,2p-1}^{p-1} & f_{2p-1,p-2,p-1}^{p-1} & f_{p-1,2p-2,p-1}^{p-1}
\end{bmatrix}.$$ 

This is the matrix of the $p$-power Frobenius acting on $H^1(C_p, O_{C_p})$ (and the Cartier-Manin operator acting on the space of regular differentials). As proved by Manin, we have

$$L_p(T) \equiv \det(I - TW_p) \mod p,$$

Our strategy is to compute $W_p$ then lift $L_p(T)$ from $(\mathbb{Z}/p\mathbb{Z})[T]$ to $\mathbb{Z}[T]$. 
Target coefficients of $f_p^{-1}$ for $p = 7$:
Coefficient relations

Let $\partial_x = x \frac{\partial}{\partial x}$ (degree-preserving). The relations

$$f^{p-1} = f \cdot f^{p-2} \quad \text{and} \quad \partial_x f^{p-1} = - (\partial_x f) f^{p-2}$$

yield the relation

$$\sum_{i' + j' + k' = 4} (i + i') f_{i', j', k'} f_{p-2}^{p-2} = 0.$$  

among nearby coefficients of $f^{p-2}$ (a triangle of side length 5).

Replacing $\partial_x$ by $\partial_y$ yields a similar relation (replace $i + i'$ with $j + j'$).
Coefficient triangle

For $p = 7$ with $i = 12, j = 5, k = 7$ the related coefficients of $f^{p-2}$ are:
Moving the triangle

Now consider a bigger triangle with side length 7. Our relations allow us to move the triangle around:

An initial “triangle” at the edge can be efficiently computed using coefficients of $f(x, 0, z)^{p-2}$. 
Computing one Hasse-Witt matrix

Nondegeneracy: we need $f(1, 0, 0), f(0, 1, 0), f(0, 0, 1)$ nonzero and $f(0, y, z), f(x, 0, z), f(x, y, 0)$ squarefree (easily achieved for large $p$).

The basic strategy to compute $W_p$ is as follows:

- There is a $28 \times 28$ matrix $M_j$ that shifts our 7-triangle from $y$-coordinate $j$ to $j + 1$; its coefficients depend on $j$ and $f$. In fact a $16 \times 16$ matrix $M_i$ suffices (use smoothness of $C$).
- Applying the product $M_0 \cdots M_{p-2}$ to an initial triangle on the edge and applying a final adjustment to shift from $f^{p-2}$ to $f^{p-1}$ gets us one column of the Hasse-Witt matrix $W_p$.
- By applying the same product (or its inverse) to different initial triangles we can compute all three columns of $W_p$.

We have thus reduced the problem to computing $M_1 \cdots M_{p-2} \mod p$. 
An average polynomial-time algorithm

Now let $\mathbb{C}/\mathbb{Q}$ be smooth plane quartic $f(x, y, z) = 0$ with $f \in \mathbb{Z}[x, y, z]$. We want to compute $W_p$ for all good $p \leq N$.

Key idea

The matrices $M_j$ do not depend on $p$; view them as integer matrices. It suffices to compute $M_0 \cdots M_{p-2} \mod p$ for all good $p \leq N$.

Using an accumulating remainder tree we can compute all of these partial products in time $O(N(\log N)^{3+o(1)})$.

This yields an average time of $O((\log p)^{4+o(1)})$ per prime to compute the $W_p$ for all good $p \leq N$.*

*We may need to skip $O(1)$ primes $p$ where $C_p$ is degenerate; these can be handled separately using an $\tilde{O}(p^{1/2})$ algorithm based on the same ideas.
Accumulating remainder tree

Given matrices $M_0, \ldots, M_{n-1}$ and moduli $m_1, \ldots, m_n$, to compute

\[
\begin{align*}
M_0 \mod m_1 \\
M_0M_1 \mod m_2 \\
M_0M_1M_2 \mod m_3 \\
M_0M_1M_2M_3 \mod m_4 \\
\cdots \\
M_0M_1 \cdots M_{n-2}M_{n-1} \mod m_n
\end{align*}
\]

multiply adjacent pairs and recursively compute

\[
\begin{align*}
(M_0M_1) \mod m_2m_3 \\
(M_0M_1)(M_2M_3) \mod m_4m_5 \\
\cdots \\
(M_0M_1) \cdots (M_{n-2}M_{n-1}) \mod m_{n-1}m_n
\end{align*}
\]

and adjust the results as required.
## Timings for genus 3 curves

<table>
<thead>
<tr>
<th>$N$</th>
<th>costa-AKR</th>
<th>non-hyp-avgpoly</th>
<th>hyp-avgpoly</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^{12}$</td>
<td>18.2</td>
<td>1.1</td>
<td>0.1</td>
</tr>
<tr>
<td>$2^{13}$</td>
<td>49.1</td>
<td>2.6</td>
<td>0.2</td>
</tr>
<tr>
<td>$2^{14}$</td>
<td>142</td>
<td>5.8</td>
<td>0.5</td>
</tr>
<tr>
<td>$2^{15}$</td>
<td>475</td>
<td>13.6</td>
<td>1.5</td>
</tr>
<tr>
<td>$2^{16}$</td>
<td>1,670</td>
<td>30.6</td>
<td>4.6</td>
</tr>
<tr>
<td>$2^{17}$</td>
<td>5,880</td>
<td>70.9</td>
<td>12.6</td>
</tr>
<tr>
<td>$2^{18}$</td>
<td>22,300</td>
<td>158</td>
<td>25.9</td>
</tr>
<tr>
<td>$2^{19}$</td>
<td>78,100</td>
<td>344</td>
<td>62.1</td>
</tr>
<tr>
<td>$2^{20}$</td>
<td>297,000</td>
<td>760</td>
<td>147</td>
</tr>
<tr>
<td>$2^{21}$</td>
<td>1,130,000</td>
<td>1,710</td>
<td>347</td>
</tr>
<tr>
<td>$2^{22}$</td>
<td>4,280,000</td>
<td>3,980</td>
<td>878</td>
</tr>
<tr>
<td>$2^{23}$</td>
<td>16,800,000</td>
<td>8,580</td>
<td>1,950</td>
</tr>
<tr>
<td>$2^{24}$</td>
<td>66,800,000</td>
<td>18,600</td>
<td>4,500</td>
</tr>
<tr>
<td>$2^{25}$</td>
<td>244,000,000</td>
<td>40,800</td>
<td>10,700</td>
</tr>
<tr>
<td>$2^{26}$</td>
<td>972,000,000</td>
<td>91,000</td>
<td>24,300</td>
</tr>
</tbody>
</table>

(Intel Xeon E7-8867v3 3.3 GHz CPU seconds).