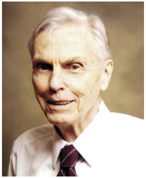
Sato-Tate in dimension 3

Andrew V. Sutherland

Massachusetts Institute of Technology

December 7, 2016

Mikio Sato



John Tate

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

Sato-Tate in dimension 1

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 $N \to \infty$.

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)

Sato-Tate distributions in dimension 1

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 $\mathrm{SU}(2) = \mathrm{USp}(2)$ derived from the ℓ-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).

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

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 $|a_i| \le \binom{2g}{i}$.

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

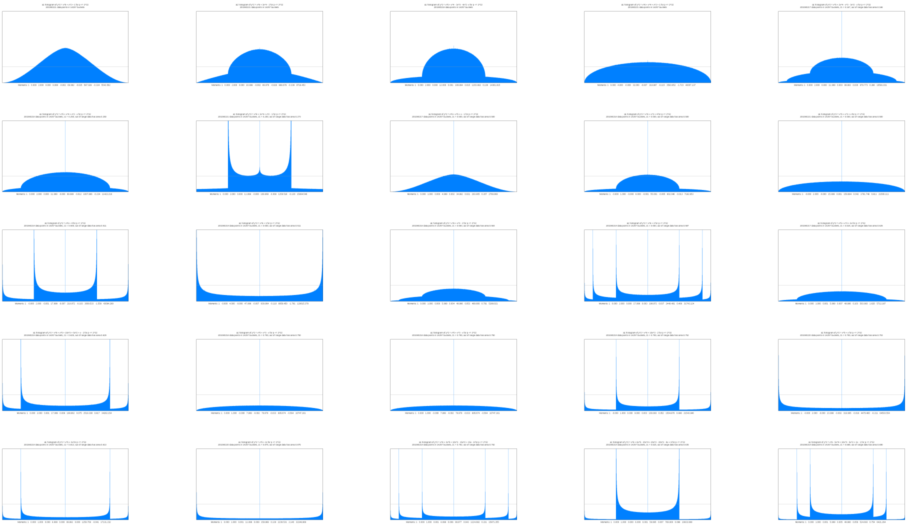
click histogram to animate (requires adobe reader)

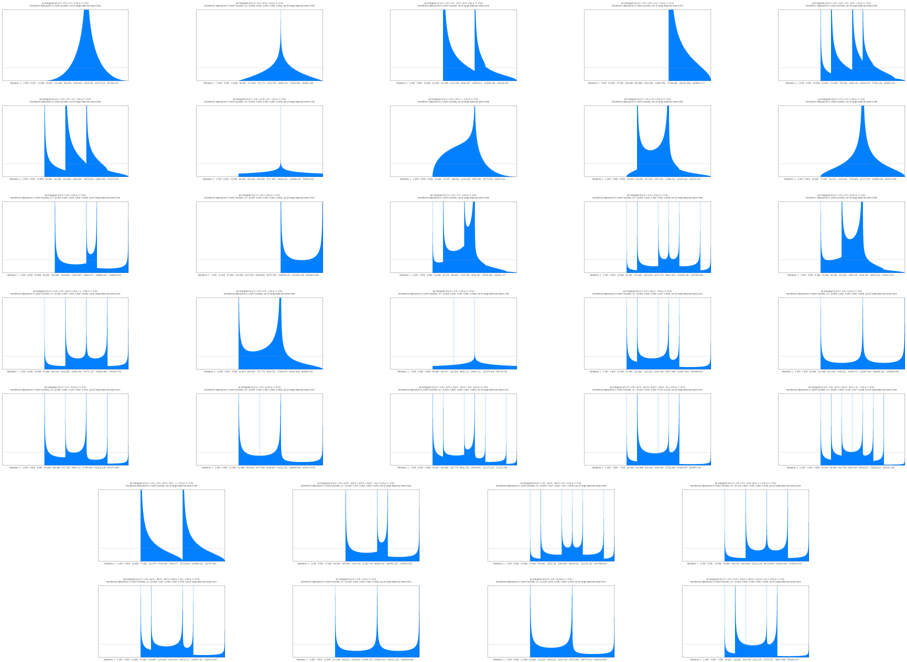
click histogram to animate (requires adobe reader)

click histogram to animate (requires adobe reader)

click histogram to animate (requires adobe reader)

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 ℓ.
The action of $\mathrm{Gal}(\bar{k}/k)$ on the ℓ-adic Tate module

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

gives rise to a Galois representation

$$\rho_\ell \colon \mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)) \simeq \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$$

For each prime $\mathfrak{p}$ of good reduction for A we have the *L-polynomial*

$$L_\mathfrak{p}(T) := \det(1 - \rho_\ell(\mathrm{Frob}_\mathfrak{p})T), \qquad \bar{L}_\mathfrak{p}(T) := L_\mathfrak{p}(T/\sqrt{\|\mathfrak{p}\|}),$$

which appears as an Euler factor in the L-series

$$L(A,s) := \prod_\mathfrak{p} L_\mathfrak{p}(\|\mathfrak{p}\|^{-s})^{-1}.$$

The Sato-Tate group of an abelian variety

The Zariski closure of the image of

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

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

Definition [Serre]

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

Conjecture [Mumford-Tate, Algebraic Sato-Tate]

$(G_\ell^{\mathrm{zar}})^0 = \mathrm{MT}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, equivalently, $(G_\ell^{1,\mathrm{zar}})^0 = \mathrm{Hg}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.
More generally, $G_\ell^{1,\mathrm{zar}} = \mathrm{AST}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.

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

A refined Sato-Tate conjecture

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

Conjecture

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

In particular, the distribution of normalized Euler factors $\bar{L}_{\mathfrak{p}}(T)$ matches the distribution of characteristic polynomials in $\mathrm{ST}(A)$.

We can test this numerically by comparing statistics of the coefficients $a_1, \ldots, a_g$ of $\bar{L}_{\mathfrak{p}}(T)$ over $\|\mathfrak{p}\| \le N$ to the predictions given by $\mu_{\mathrm{ST}(A)}$.

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 $\mathrm{End}(A_K) = \mathrm{End}(A_{\bar{k}})$.
$\mathrm{Gal}(K/k)$ acts on the $\mathbb{R}$-algebra $\mathrm{End}(A_K)_{\mathbb{R}} = \mathrm{End}(A_K) \otimes_{\mathbb{Z}} \mathbb{R}$.

Definition

The *Galois endomorphism type* of A is the isomorphism class of $[\mathrm{Gal}(K/k), \mathrm{End}(A_K)_{\mathbb{R}}]$, 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 $\mathrm{End}(A_K)_{\mathbb{R}}$ and $G/G^0 \simeq \mathrm{Gal}(K/k)$ (with corresponding actions).

Real endomorphism algebras of abelian surfaces

abelian surface	$\mathbf{End}(A_K)_{\mathbb{R}}$	$\mathbf{ST}(A)^{\mathbf{0}}$
square of CM elliptic curve	$\mathrm{M}_2(\mathbb{C})$	$\mathrm{U}(1)_2$
• QM abelian surface • square of non-CM elliptic curve	$\mathrm{M}_2(\mathbb{R})$	$\mathrm{SU}(2)_2$
• CM abelian surface • product of CM elliptic curves	$\mathbb{C} \times \mathbb{C}$	$\mathrm{U}(1) \times \mathrm{U}(1)$
product of CM and non-CM elliptic curves	$\mathbb{C} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{SU}(2)$
• RM abelian surface • product of non-CM elliptic curves	$\mathbb{R} \times \mathbb{R}$	$\mathrm{SU}(2) \times \mathrm{SU}(2)$
generic abelian surface	$\mathbb{R}$	$\mathrm{USp}(4)$

(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 $\mathrm{USp}(4)$, there are 52 Sato-Tate groups $\mathrm{ST}(A)$ that arise for abelian surfaces A/k over number fields; 34 occur for $k = \mathbb{Q}$.

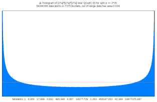
$\mathrm{U}(1)_2$:	$C_1, C_2, C_3, C_4, C_6, D_2, D_3, D_4, D_6, T, O,$ $J(C_1), J(C_2), J(C_3), J(C_4), J(C_6),$ $J(D_2), J(D_3), J(D_4), J(D_6), J(T), J(O),$ $C_{2,1}, C_{4,1}, C_{6,1}, D_{2,1}, D_{3,2}, D_{4,1}, D_{4,2}, D_{6,1}, D_{6,2}, O_1$
$\mathrm{SU}(2)_2$:	$E_1, E_2, E_3, E_4, E_6, J(E_1), J(E_2), J(E_3), J(E_4), J(E_6)$
$\mathrm{U}(1) \times \mathrm{U}(1)$:	$F, F_a, F_{a,b}, F_{ab}, F_{ac}$
$\mathrm{U}(1) \times \mathrm{SU}(2)$:	$\mathrm{U}(1) \times \mathrm{SU}(2),\ N(\mathrm{U}(1) \times \mathrm{SU}(2))$
$\mathrm{SU}(2) \times \mathrm{SU}(2)$:	$\mathrm{SU}(2) \times \mathrm{SU}(2),\ N(\mathrm{SU}(2) \times \mathrm{SU}(2))$
$\mathrm{USp}(4)$:	$\mathrm{USp}(4)$

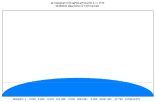
This theorem says nothing about equidistribution, however this is now known in many special cases [Fité-S 2012, Johansson 2013].

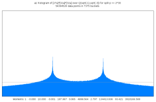
Real endomorphism algebras of abelian threefolds

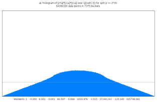
abelian threefold	$\mathbf{End}(A_K)_{\mathbb{R}}$	$\mathbf{ST}(A)^{\mathbf{0}}$
cube of a CM elliptic curve	$\mathrm{M}_3(\mathbb{C})$	$\mathrm{U}(1)_3$
cube of a non-CM elliptic curve	$\mathrm{M}_3(\mathbb{R})$	$\mathrm{SU}(2)_3$
product of CM elliptic curve and square of CM elliptic curve	$\mathbb{C} \times \mathrm{M}_2(\mathbb{C})$	$\mathrm{U}(1) \times \mathrm{U}(1)_2$
• product of CM elliptic curve and QM abelian surface • product of CM elliptic curve and square of non-CM elliptic curve	$\mathbb{C} \times \mathrm{M}_2(\mathbb{R})$	$\mathrm{U}(1) \times \mathrm{SU}(2)_2$
product of non-CM elliptic curve and square of CM elliptic curve	$\mathbb{R} \times \mathrm{M}_2(\mathbb{C})$	$\mathrm{SU}(2) \times \mathrm{U}(1)_2$
• product of non-CM elliptic curve and QM abelian surface • product of non-CM elliptic curve and square of non-CM elliptic curve	$\mathbb{R} \times \mathrm{M}_2(\mathbb{R})$	$\mathrm{SU}(2) \times \mathrm{SU}(2)_2$
• CM abelian threefold • product of CM elliptic curve and CM abelian surface • product of three CM elliptic curves	$\mathbb{C} \times \mathbb{C} \times \mathbb{C}$	$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$
• product of non-CM elliptic curve and CM abelian surface • product of non-CM elliptic curve and two CM elliptic curves	$\mathbb{C} \times \mathbb{C} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{SU}(2)$
• product of CM elliptic curve and RM abelian surface • product of CM elliptic curve and two non-CM elliptic curves	$\mathbb{C} \times \mathbb{R} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$
• RM abelian threefold • product of non-CM elliptic curve and RM abelian surface • product of 3 non-CM elliptic curves	$\mathbb{R} \times \mathbb{R} \times \mathbb{R}$	$\mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$
product of CM elliptic curve and abelian surface	$\mathbb{C} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{USp}(4)$
product of non-CM elliptic curve and abelian surface	$\mathbb{R} \times \mathbb{R}$	$\mathrm{SU}(2) \times \mathrm{USp}(4)$
quadratic CM abelian threefold	$\mathbb{C}$	$\mathrm{U}(3)$
generic abelian threefold	$\mathbb{R}$	$\mathrm{USp}(6)$

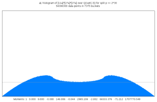
Connected Sato-Tate groups of abelian threefolds:

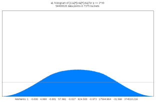

$\mathrm{U}(1)_3$

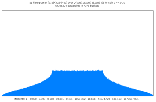

$\mathrm{SU}(2)_3$

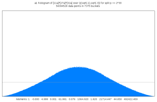

$\mathrm{U}(1)\times\mathrm{U}(1)_2$

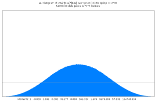

$\mathrm{U}(1)\times\mathrm{SU}(2)_2$

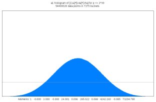

$\mathrm{SU}(2)\times\mathrm{U}(1)_2$

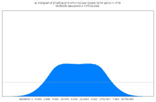

$\mathrm{SU}(2)\times\mathrm{SU}(2)_2$

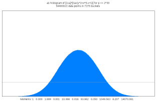

$\mathrm{U}(1)\times\mathrm{U}(1)\times\mathrm{U}(1)$

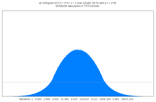

$\mathrm{U}(1)\times\mathrm{U}(1)\times\mathrm{SU}(2)$

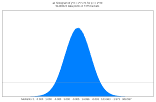

$\mathrm{U}(1)\times\mathrm{SU}(2)\times\mathrm{U}(1)$


$\mathrm{SU}(2)\times\mathrm{SU}(2)\times\mathrm{SU}(2)$


$\mathrm{U}(1)\times\mathrm{USp}(4)$


$\mathrm{SU}(2)\times\mathrm{USp}(4)$


$\mathrm{U}(3)$


$\mathrm{USp}(6)$

Partial classification of component groups

G_0	$G/G_0 \hookrightarrow$	$\lvert G/G_0\rvert$ divides
$\mathrm{USp}(6)$	C_1	1
$\mathrm{U}(3)$	C_2	2
$\mathrm{SU}(2)\times\mathrm{USp}(4)$	C_1	1
$\mathrm{U}(1)\times\mathrm{USp}(4)$	C_2	2
$\mathrm{SU}(2)\times\mathrm{SU}(2)\times\mathrm{SU}(2)$	S_3	6
$\mathrm{U}(1)\times\mathrm{SU}(2)\times\mathrm{SU}(2)$	D_2	4
$\mathrm{U}(1)\times\mathrm{U}(1)\times\mathrm{SU}(2)$	D_4	8
$\mathrm{U}(1)\times\mathrm{U}(1)\times\mathrm{U}(1)$	$\mathrm{C}_2\wr\mathrm{S}_3$	48
$\mathrm{SU}(2)\times\mathrm{SU}(2)_2$	$\mathrm{D}_4,\ \ \mathrm{D}_6$	$8,\ 12$
$\mathrm{SU}(2)\times\mathrm{U}(1)_2$	$\mathrm{D}_6\times\mathrm{C}_2,\ \ \mathrm{S}_4\times\mathrm{C}_2$	48
$\mathrm{U}(1)\times\mathrm{SU}(2)_2$	$\mathrm{D}_4\times\mathrm{C}_2,\ \ \mathrm{D}_6\times\mathrm{C}_2$	$16,\ 24$
$\mathrm{U}(1)\times\mathrm{U}(1)_2$	$\mathrm{D}_6\times\mathrm{C}_2\times\mathrm{C}_2,\ \ \mathrm{S}_4\times\mathrm{C}_2\times\mathrm{C}_2$	96
$\mathrm{SU}(2)_3$	$\mathrm{D}_6,\ \ \mathrm{S}_4$	24
$\mathrm{U}(1)_3$	(to be determined)	$336,\ 1728$

(disclaimer: work in progress, subject to verification)

Algorithms to compute zeta functions

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 $p \le N$.

algorithm	complexity per prime (ignoring factors of $O(\log\log p)$) $g = 1$	 $g = 2$	 $g = 3$
point enumeration	$p\log p$	$p^2\log p$	$p^3(\log p)^2$
group computation	$p^{1/4}\log p$	$p^{3/4}\log p$	$p\log p$
p-adic cohomology	$p^{1/2}(\log p)^2$	$p^{1/2}(\log p)^2$	$p^{1/2}(\log p)^2$
CRT (Schoof-Pila)	$(\log p)^5$	$(\log p)^8$	$(\log p)^{12?}$
average poly-time	$(\log p)^4$	$(\log p)^4$	$(\log p)^4$

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 $f^n_{i,j,k}$ denote the coefficient of $x^iy^jz^k$ in f^n.

The *Hasse–Witt matrix* of C_p is the 3×3 matrix

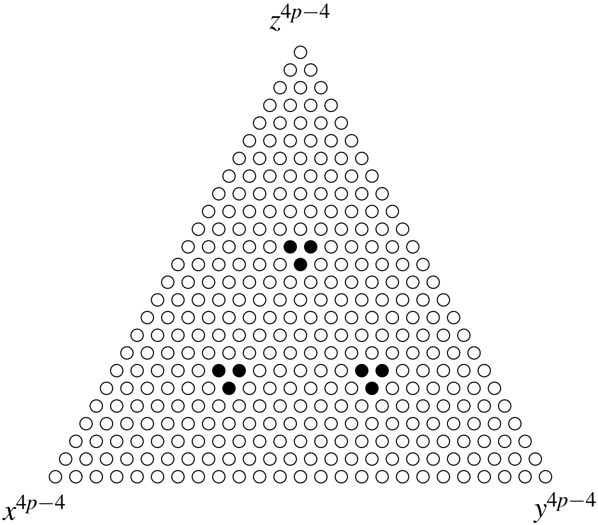
$$W_p := \begin{bmatrix} f^{p-1}_{p-1,p-1,2p-2} & f^{p-1}_{2p-1,p-1,p-2} & f^{p-1}_{p-1,2p-1,p-2} \\ f^{p-1}_{p-2,p-1,2p-1} & f^{p-1}_{2p-2,p-1,p-1} & f^{p-1}_{p-2,2p-1,p-1} \\ f^{p-1}_{p-1,p-2,2p-1} & f^{p-1}_{2p-1,p-2,p-1} & f^{p-1}_{p-1,2p-2,p-1} \end{bmatrix}.$$

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

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

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

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

yield the relation

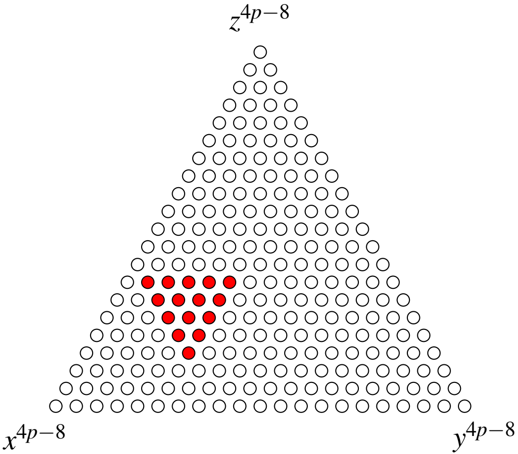
$$\sum_{i'+j'+k'=4} (i+i') f_{i',j',k'} f^{p-2}_{i-i',j-j',k-k'} = 0.$$

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

Replacing ∂_x by ∂_y yields a similar relation (replace $i+i'$ with $j+j'$).

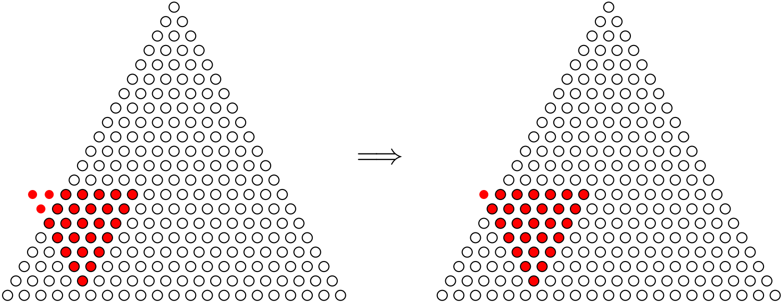
Coefficient triangle

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 28×28 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 16×16 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 $M_1 \cdots M_{p-2} \bmod p$.

An average polynomial-time algorithm

Now let $C/\mathbb{Q}$ 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 $p\le N$.

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 $p\le N$.

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 $p\le N$.*

*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

$$\begin{aligned} M_0 &\bmod m_1 \\ M_0 M_1 &\bmod m_2 \\ M_0 M_1 M_2 &\bmod m_3 \\ M_0 M_1 M_2 M_3 &\bmod m_4 \\ &\cdots \\ M_0 M_1 \cdots M_{n-2} M_{n-1} &\bmod m_n \end{aligned}$$

multiply adjacent pairs and recursively compute

$$\begin{aligned} (M_0 M_1) &\bmod m_2 m_3 \\ (M_0 M_1)(M_2 M_3) &\bmod m_4 m_5 \\ &\cdots \\ (M_0 M_1) \cdots (M_{n-2} M_{n-1}) &\bmod m_{n-1} m_n \end{aligned}$$

and adjust the results as required.

Timings for genus 3 curves

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

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