

Families of curves with nontrivial endomorphisms in their Jacobians

Jerome William Hoffman

Louisiana State University

April 6, 2015

- 1 The Problem and Background
- 2 Shimura Varieties: Some Examples
- 3 $g=2$
- 4 $g=3$
- 5 Galois representations and automorphic forms

Let X be a **projective nonsingular algebraic curve of genus g** (defined over a field of characteristic 0). Let $A = \text{Jac}(X)$ be its **Jacobian**. This is a principally polarized abelian variety (ppav) of dimension g defined over the same field as X .

Moduli spaces

Let \mathfrak{M}_g be the moduli space (coarse) of smooth projective curves of genus g . This has dimension $3g - 3$ if $g \geq 2$.

Let \mathfrak{A}_g be the moduli space (coarse) of ppav of dimension g . This has dimension $g(g + 1)/2$.

The map $X \mapsto \text{Jac}(X) : \mathfrak{M}_g \rightarrow \mathfrak{A}_g$ is an injection (**Torelli**).

When $g = 2, 3$, we have $3g - 3 = g(g + 1)/2$, so that in these cases, \mathfrak{M}_g and \mathfrak{A}_g are **birationally equivalent**.

Recall: for any abelian variety A , $\text{End}(A) \otimes \mathbb{Q}$ is a **finite-dimensional semisimple algebra with involution** (usually just \mathbb{Q}). The different possible types were classified by **A. A. Albert**.

Consider the set of isomorphism classes of data (A, ϕ, θ, r) where

- 1 A is an abelian variety of dimension g .
- 2 ϕ is a polarization of A , of a fixed type.
- 3 $\theta : R \rightarrow \text{End}(A)$ is a homomorphism from an order in a semi simple algebra of finite dimension over \mathbb{Q} ; θ is compatible with ϕ in a suitable sense.
- 4 r is a rigidification, typically a marking of a finite set of points of finite order on A .

This data is parametrized by a **Shimura variety** (of PEL type) $S(g, \phi, R, r)$.

Shimura Varieties

- 1 As a complex manifold, a Shimura variety is a quotient

$$\Gamma \backslash D$$

where D is a **Hermitian symmetric domain** and $\Gamma \subset \text{Aut}(D) = G$ is an **arithmetic group**. G is the set of real points of a **reductive algebraic group** defined over \mathbb{Q} .

- 2 As an algebraic variety, they have **canonical models** over specific number fields.
- 3 While not all Shimura varieties have straightforward moduli interpretations, those of PEL type do. In particular, there is a universal family

$$\pi : A(g, \phi, R, r) \rightarrow S(g, \phi, R, r)$$

Problem 1. Describe $\pi : A(g, \phi, R, r) \rightarrow S(g, \phi, R, r)$ as **algebraic varieties**. As **complex manifolds** they were made explicit by **Kuga and Shimura**.

Problem 2. There are canonical subvarieties $H \subset S(g, \phi, R, r)$ of **Hodge type**. Describe these algebro-geometrically. Example: find the algebraic coordinates of **CM points**.

Problem 3. Sometimes an **interesting family** of varieties is known. Determine the endomorphism structure of the corresponding **Picard varieties**. Example: **(generalized) hypergeometric families**.

Problem 4. In Problem 3 replace **Picard varieties** by motives of any weight.

Classical modular curves

$S(g = 1, \phi, \text{End} = \mathbb{Z}, r)$ are the classical modular curves. $D = \mathfrak{H}_1$ is the complex upper half plane. $\Gamma \subset \text{SL}_2(\mathbb{Z})$ is a congruence subgroup. The algebraic variety structure is mediated by **automorphic forms/functions**, e.g., the j -function

$$S(1, \phi, \mathbb{Z}, r = \emptyset) = \text{SL}_2(\mathbb{Z}) \backslash \mathfrak{H}_1 \stackrel{j}{\cong} \mathbf{P}^1(\mathbb{C}).$$

Values $j(\tau)$ at CM points $\tau \in \mathfrak{H}_1$ are algebraic integers. Their arithmetic is very interesting, c.f., the **Gross-Zagier formula**.

Siegel modular varieties

$S(g, \phi, \text{End} = \mathbb{Z}, r)$ are the Siegel modular varieties. $D = \mathfrak{H}_g$ is the Siegel half space. $\Gamma \subset \text{Sp}_{2g}(\mathbb{Z})$ is a congruence subgroup. The algebraic variety structure is mediated by **automorphic forms/functions**. There are embeddings

$$S(g, \phi, \mathbb{Z}, r) = \Gamma \backslash \mathfrak{H}_g \hookrightarrow \mathbf{P}^N(\mathbb{C})$$

given by **theta constants**, but these are cumbersome, N is big and there are many equations (determined by **Mumford**).

Shimura curves

$S(g = 2, \phi, R, r)$. Where R is an order in an **indefinite quaternion division algebra B over \mathbb{Q}** . $D = \mathfrak{H}_1$ is the complex upper halfspace. $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ is a **Fuchsian subgroup** determined by the units of norm 1 in R .

These were first studied by **Poincaré**. They are called **Shimura curves**. The contrast to the case of classical modular curves, $\Gamma \backslash \mathfrak{H}_1$ is compact (no **cusps**).

Explicit equations for these have been written down in some cases, by various methods (**Ihara, Kurihara, Jordan-Livné, Hashimoto-Murabayashii, Elkies, Yifan Yang, Fang-Ting Tu...**)
Some universal families of genus 2 QM curves have also been found.

Quaternionic Shimura varieties

Let R be the ring of integers in an **totally real numberfield** K , with $[K : \mathbb{Q}] = d \geq 2$. Let B be a quaternion division algebra over K . Then

$$B \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{H}^g \times M_2(\mathbb{R})^{d-g}, \quad \mathbb{H} = \text{Hamilton's quaternions.}$$

If $g = 0$, the Shimura variety has a moduli interpretation as parametrizing a family of abelian varieties of dimension $2d$ with endomorphisms by an order in B .

If $1 \leq g \leq d - 1$, there is a Shimura variety S , but it does not have a naive moduli interpretation. Nonetheless, **Shimura** constructed embeddings of S into moduli spaces of abelian varieties. In particular, **there are families of abelian varieties parametrized by S .**

Quaternionic Shimura varieties

These have been used to construct Galois representations attached to $B_{\mathbb{A}}$ (M. Ohta).

Examples arise from arithmetic triangle groups; they have been further investigated by P. Beazley-Cohen, Ling Long, Wolfart, and J. Voight.

Problem

Construct families of genus 2 curves

$$X : y^2 = f(x), \quad \deg f(x) = 5 \text{ or } 6.$$

such that $\text{End}(\text{Jac}(X)) \otimes \mathbb{Q}$ is nontrivial, i.e., larger than \mathbb{Q} .

Interesting cases

- 1 $\text{End}(\text{Jac}(X)) \otimes \mathbb{Q} =$ quartic CM field. These are isolated in moduli. Applications to cryptography ([K.Lauter](#)).
- 2 $\text{End}(\text{Jac}(X)) \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{D})$ a real quadratic field. The Shimura variety is a Hilbert modular surface (a [Humbert surface](#)).
- 3 $\text{End}(\text{Jac}(X)) \otimes \mathbb{Q} = B$, an indefinite quaternion division algebra over \mathbb{Q} . This gives a Shimura curve.

Hilbert modular surface for $\mathbb{Q}(\sqrt{5})$

1. A point $\tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \in \mathfrak{H}_2$ with $\tau_1 = \tau_2 + \tau_3$ gives an abelian variety

$$A_\tau := \mathbb{C}^2 / \mathbb{Z}^2 + \mathbb{Z}^2 \tau$$

whose endomorphism ring contains $\mathbb{Q}(\sqrt{5})$ (**Humbert**).

2. The **diagonal surface of Clebsch and Klein**

$$\sum_{i=0}^4 x_i = 0, \quad \sum_{i=0}^4 x_i^3 = 0,$$

is isomorphic to the level 2 covering of the Hilbert modular surface for $\mathbb{Q}(\sqrt{5})$ (**Hirzebruch**).

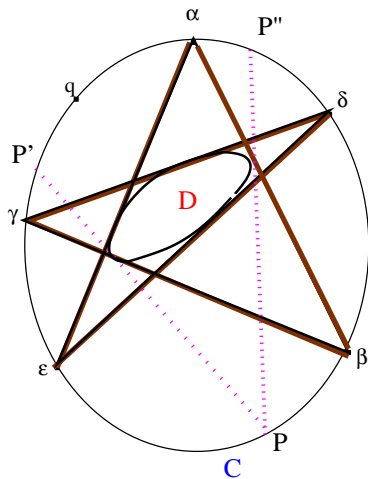
Hilbert modular surface for $\mathbb{Q}(\sqrt{5})$

1 Let

$$\begin{aligned} f(x; a, b, c) = & x^6 - (4 + 2b + 3c)x^5 + (2 + 2b + b^2 - ac)x^4 \\ & - (6 + 4a + 6b - 2b^2 + 5c + 2ac)x^3 \\ & + (1 + b^2 - ac)x^2 + (2 - 2b)x + (c + 1). \end{aligned}$$

The $y^2 = f(x; a, b, c)$ is a universal family of genus 2 curves with RM by $\mathbb{Q}(\sqrt{5})$ (Brumer/Hashimoto).

2 These curves can be constructed from Poncelet 5-gons (Humbert/Mestre).



Humbert 5 = Poncelet 5

Pentagon $\alpha\beta\gamma\delta\epsilon$
 inscribes conic C
 circumscribes conic D

Genus 2 curve X is the
 double cover of C branched
 above $\alpha, \beta, \gamma, \delta, \epsilon$ and
 a point q in C intersect D .

The correspondence

$$P \rightarrow P' + P''$$

lifts to a correspondence

$$\phi \text{ of } X \text{ with } \phi^2 + \phi - 1 = 0$$

in $\text{Jac}(X)$.

Shimura curve for B_6

- ① The maximal order in B is $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\gamma$ where

$$\alpha^2 = -1, \beta^2 = 3, \alpha\beta = -\beta\alpha, \gamma = (1 + \alpha + \beta + \alpha\beta)/2.$$

- ② $S(\mathbb{C}) = \mathcal{O}_1^* \backslash \mathfrak{H} \cong \mathbb{P}^1(\mathbb{C})$.

- ③ The canonical model is the projective conic $x^2 + y^2 + 3z^2 = 0$.

- ④ The graded ring of modular forms for $\Gamma = \mathcal{O}_1^*$ is generated by forms h_4, h_6, h_{12} subject to the relation:

$$h_{12}^2 + 3h_6^4 + h_4^6 = 0.$$

Shimura curve for B_6

Consider the family of genus 2 curves

$$y^2 = x(x^4 - Px^3 + Qx^2 - Rx + 1),$$

where

$$P = -2(s + t), \quad R = -2(s - t)$$

$$Q = \frac{(1 + 2t^2)(11 - 28t^2 + 8t^4)}{3(1 - t^2)(1 - 4t^2)}$$

where $4s^2t^2 - s^2 + t^2 + 2 = 0$. This is a universal family of genus 2 curves whose Jacobians have QM by the maximal order in B_6 (Hashimoto and Murabayashii).

Method I: Automorphic Forms

- 1 **Algebraic moduli** of genus 2 curves $y^2 = f_6(x)$ are given by the **invariant theory of binary sextic forms**. These were determined by **Clebsch**.
- 2 One can reconstruct a genus 2 curve from its Clebsch/Igusa invariants: **Mestre's algorithm**.
- 3 **Analytic moduli** of genus 2 curves are given by a point in Siegel's spaces of degree 2: $\tau \in \mathfrak{H}_2$.
- 4 The bridge between **analytic moduli** and **algebraic moduli** is given by **automorphic forms**, specifically **theta constants**.

Method I: Automorphic Forms

- 1 The explicit expressions of the Igusa/Clebsch invariants as Siegel modular forms were given by **Thomae**, **Bolza** and **Igusa**.
- 2 Idea: one can convert the relatively simple formulas for Shimura subvarieties of \mathfrak{H}_2 into algebraic equations in the Igusa/Clebsch invariants. This has been implemented by **Runge** and **Gruenewald**.

Method I: Humbert surface for $D = 5$

- ① The Satake compactification of $\mathfrak{A}_2[2]$ has a model in \mathbf{P}^5 given by

$$s_1 = 0, \quad s_2^2 - 4s_4 = 0, \quad s_k = \sum_{i=1}^6 x_i^k,$$

where x_i is a linear combination of theta constants. Each s_i is a **Siegel modular form** of weight $2i$.

- ② In $\mathfrak{A}_2[2]$ Humbert surfaces of discriminant 5 have equations

$$2p_{2,j} + p_{1,j}^2 = 0, \quad j = 1, \dots, 6,$$

where $p_{k,j}$ is k th elementary symmetric function on the 5 coordinates excluding x_j .

Method I: Humbert surface for $D = 5$

- ① The Satake compactification of $\mathfrak{A}_2[2]$ has a model in \mathbf{P}^5 given by

$$s_1 = 0, \quad s_2^2 - 4s_4 = 0, \quad s_k = \sum_{i=1}^6 x_i^k,$$

where x_i is a linear combination of theta constants. Each s_i is a **Siegel modular form** of weight $2i$.

- ② In $\mathfrak{A}_2[2]$ Humbert surfaces of discriminant 5 have equations

$$2p_{2,j} + p_{1,j}^2 = 0, \quad j = 1, \dots, 6,$$

where $p_{k,j}$ is k th elementary symmetric function on the 5 coordinates excluding x_j .

Method I: Shimura curves; A. Besser

- ① In $\mathfrak{A}_2[2]$, Shimura curves of discriminant 6 have equations

$$3x_i^2 = s_2, \quad x_i = -x_j, \quad 1 \leq i < j \leq 6.$$

- ② In $\mathfrak{A}_2[2]$, Shimura curves of discriminant 10 have equations

$$x_i + 5x_j = 0, \quad 3x_i^2 = s_2, \quad 1 \leq i \neq j \leq 6.$$

- ③ In $\mathfrak{A}_2[2]$, Shimura curves of discriminant 15 have equations

$$15(x_i + x_j)^2 = 4(s_2 + 3x_i x_j), \quad 6x_i + 5x_j + 5x_k = 0, \\ 1 \leq i \neq j \neq k \neq i \leq 6.$$

Method II: Kummer Surfaces. Elkies and Kumar

- 1 If X is a genus 2 curve then the Kummer surface $\text{Km}(X)$ is the nonsingular model of $\text{Jac}(X)/\pm id$. This is a **K3 surface of high rank** : $\text{rank}(\text{NS}(\text{Km}(X))) \geq 17$.
- 2 If $\text{Jac}(X)$ has additional endomorphisms, then the rank of $\text{Km}(X)$ should go up.

Dolgachev and A. Kumar proved:

Theorem

There is an isomorphism $\psi : \mathfrak{M}_2 \rightarrow \mathcal{E}_{E_8, E_7}$, where \mathcal{E}_{E_8, E_7} is the moduli space of elliptic K3 surfaces with an E_8 -fibre at ∞ and an E_7 -fibre at 0.

Let A be the elliptic K3 surface with equation

$$y^2 = x^3 - t^3 \left(\frac{l_4}{12} + 1 \right) x + t^5 \left(\frac{l_{10}}{4} t^2 + \frac{l_2 l_4 - 3l_6}{108} t + \frac{l_2}{24} \right),$$

which has fibres of type E_8 and E_7 respectively at $t = \infty$ and $t = 0$.

Let C be the genus 2 curve with Igusa-Clebsch invariants

$(l_2 : l_4 : l_6 : l_{10})$. **Then A and $\text{Km}(C)$ are Shioda-Inose twins.**

Theorem

Consider the lattice of rank 18: $L_D := E_8(-1)^2 \oplus \mathcal{O}_D$. Let \mathcal{F}_{L_D} be the moduli space of K3 surface that are lattice polarized by L_D . Then there is a surjective birational morphism $\mathcal{F}_{L_D} \rightarrow \mathcal{H}_D$.

Therefore, to construct the Humbert surface \mathcal{H}_D for $\mathcal{O}_D \subset \mathbb{Q}(\sqrt{D})$ one attempts to realize L_D as the **Néron-Severi lattice** of an **elliptic K3 surface**. One might have to modify this to a new elliptic K3 surface so as to have fibers of type E_7 and E_8 (2 and 3 neighbors).

Method II: Kummer Surfaces. $D = 5$

The elliptic surface is

$$y^2 = x^3 + \frac{1}{4}t^3(-3g^2t + 4)x - \frac{1}{4}t^5(4h^2t^2 + (4h + g^3)t + (4g + 1))$$

The Hilbert modular surface (double cover of the Humbert surface \mathcal{H}_5) is

$$z^2 = 2(6250h^2 - 4500g^2h - 1350gh - 108h - 972g^5 - 324g^4 - 27g^3)$$

The Igusa-Clebsch invariants are

$$(I_2 : I_4 : I_6 : I_{10}) = (6(4g + 1), 9g^2, 9(4h + 9g^3 + 2g^2), 4h^2).$$

Method II: Shimura curve with $D = 6$

The elliptic surface is

$$y^2 = x^3 + tx^2 + 2bt^3(t-1)x + b^2t^5(t-1)^2$$

The Shimura curve is $X(6)/\langle w_2, w_3 \rangle \cong \mathbf{P}^1$ with coordinate b . This is the arithmetic triangle group $(2,4,6)$. $X(6)$ has the model $s^2 + 27r^2 + 16 = 0$, where $b = r^2$.

The Igusa-Clebsch invariants are

$$(I_2 : I_4 : I_6 : I_{10}) = (24(b+1), 36b, 72b(5b+4), 4b^3).$$

There are CM points of discriminants $-3, -4, -24, -19$ respectively at $b = \infty, 0, -16/27, 81/64$.

Genus 3 curves

\mathfrak{M}_3 and \mathfrak{A}_3 are birationally equivalent, but now there is a distinction between **hyperelliptic** and **nonhyperelliptic** curves.

A hyperelliptic curve has an equation

$$y^2 = f_8(x), \quad \deg f_8 = 8.$$

There are many models of nonhyperelliptic genus 3 curves, the simplest being the **the canonical model**, which is a smooth projective plane quartic

$$F_4(x, y, z) = 0.$$

Genus 3 curves: moduli

Algebraic moduli of genus 3 hyperelliptic curves is given by the **invariant theory of binary octic forms**. These were determined by Shioda.

As in the case of genus 2, these invariants can be expressed in terms of **Siegel modular forms of degree 3** (**theta constants: Thomae's formulas**).

Algebraic moduli of genus 3 nonhyperelliptic curves is given by the **invariant theory of ternary quartic forms**.

Studied by many people, e.g., **E. Noether**, the complete determination of these is quite recent - **Dixmier-Ohno invariants**.

Genus 3 curves: moduli

In principle, these invariants can be expressed in terms of **Siegel modular forms of degree 3**.

The necessary formulas are implicit in 19th century works, especially **Frobenius and Schottky**, but to my knowledge, they are not in the modern literature (but see **Dolgachev-Ortland** and **Looijenga**).

Genus 3 curves: endomorphisms of Jacobians

Some interesting cases:

- 1 A degree 6 CM number field.
- 2 An imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ (Picard modular case).
- 3 A totally real cubic number field (Hilbert modular case).

Picard's family

Picard studied the family of genus 3 curves:

$$C_{a,b} : y^3 = x(x-1)(x-a)(x-b)$$

$\text{End}(\text{Jac}(C_{a,b}))$ contains $R = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$.

The parameter space is isomorphic to $\Gamma \backslash \mathbb{B}_2$ where $\Gamma \subset \text{SU}(2, 1; R)$ is a congruence subgroup, $\mathbb{B}_2 \subset \mathbb{C}^2$, the unit ball.

This is a **generalized hypergeometric family**.

A Hilbert modular family

Joint with:

Dun Liang

Zhibin Liang

Ryotaro Okazaki

Yukiko Sakai

Haohao Wang

We have constructed a universal (3-dimensional) family of nonhyperelliptic curves C with the property that $\text{End}(\text{Jac}(C))$ contains $\mathbb{Z}[\zeta_7 + \bar{\zeta}_7]$, the integers in a cubic number field.

A Hilbert modular family

The construction is based on a method of Shimada and Ellenberg. Basic idea: Let G be a finite group acting on a curve Y . If $H \subset G$ is a subgroup we let $X = Y/H$. We get an action of the “Hecke algebra” $\mathbb{Q}[H \backslash G / H]$ on $\text{Jac}(X)$.

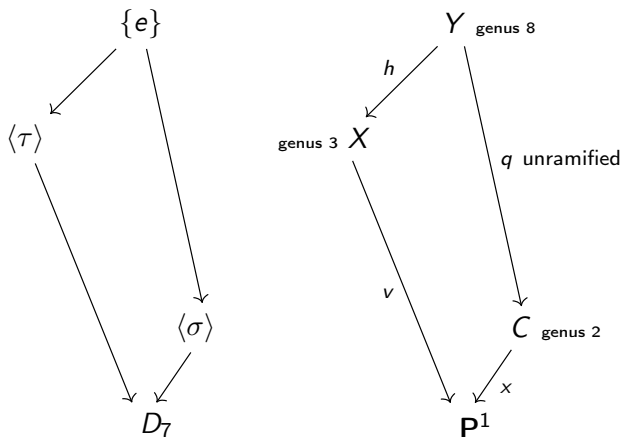
$\mathbb{Q}[H \backslash G / H] \subset \mathbb{Q}[G]$ is the subalgebra generated by $\tau_H g \tau_H$ where

$$\tau_H = \frac{1}{\#H} \sum_{h \in H} h.$$

Our case:

$$G = D_7 = \langle \sigma, \tau \mid \sigma^7 = \tau^2 = 1, \tau \sigma \tau = \sigma^6 \rangle$$

and $H = \langle \tau \rangle$. $\mathbb{Q}[H \backslash G / H] = \mathbb{Q}[\zeta_7^+]$.



A Diophantine equation

Problem. Find solutions to the following equation:

$$a(x)^2 - s(x)b(x)^2 = c(x)^7$$

where a, b, c, s are polynomials in one variable of respective degrees 7, 4, 2, 6.

Why? Let $C : y^2 = s(x)$, a genus 2 curve. Let $\varphi = a(x) + b(x)y$, an element of its function field $k(C) = k(x, y)$. Then $k(x, y, \sqrt[7]{\varphi})$ is an unramified cyclic Galois extension of $k(x, y)$ of degree 7.

If X is a (smooth, projective) curve of genus g , say defined over \mathbb{Q} , there are l -adic representations

$$\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathbf{GSp}(H^1(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_l)) = \mathbf{GSp}_{2g}(\mathbb{Q}_l).$$

In general, one expects that the image is all of $\mathbf{GSp}_{2g}(\mathbb{Q}_l)$. If $\text{End}(\text{Jac}(X)) \otimes \mathbb{Q}$ is larger than \mathbb{Q} , the Galois image will be smaller.

For instance, in our case (genus 3 with endomorphisms by a totally real cubic number field K) we get Galois representations of \mathbf{GL}_2 -type.

A curve X with multiplication by $\mathbb{Z}[\zeta_7 + \bar{\zeta}_7]$

$$\begin{aligned}
 &x^4 + \frac{345x^3y}{4} - \frac{16038x^3z}{7} + \frac{14499x^2y^2}{14} - \frac{553623}{4}x^2yz + \frac{4273137x^2z^2}{2} \\
 &+ \frac{2153679xy^3}{28} + \frac{28315359}{7}xy^2z + \frac{659015811}{7}xyz^2 - \frac{6866481456xz^3}{7} \\
 &- \frac{28405935y^4}{7} - 20973087y^3z - \frac{10692058320y^2z^2}{7} - \frac{205496736912yz^3}{7} \\
 &+ \frac{1321162646760z^4}{7} = 0
 \end{aligned}$$

Zeta function and Galois representation for X

We compute the **zeta function** of the scheme X/\mathbb{Z} :

$$Z(X/\mathbb{F}_p, x) = \exp \left(\sum_{\nu \geq 1} N_\nu x^\nu / \nu \right) \\ = \frac{1 + a_p x + b_p x^2 + c_p x^3 + p b_p x^4 + p^2 a_p x^5 + p^3 x^6}{(1-x)(1-px)}$$

for the primes $p \neq 2, 3, 7, 73, 109, 829, 967$ where $N_\nu = \#X(\mathbb{F}_{p^\nu})$.
The numerator in the above expression equals

$$h_p(x) := \det \left(1 - x\rho(\text{Frob}_p) \mid H_{\text{et}}^1(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_l) \right), \quad l \neq p$$

where $\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GSp}(H_{\text{et}}^1(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_l))$ is the canonical **Galois representation in étale cohomology**, and $\text{Frob}_p = \text{Frobenius}$.

Zeta function and Galois representation for X

Since the Jacobian of X has endomorphisms in the field $K = \mathbb{Q}(\zeta_7 + \bar{\zeta}_7)$, this Galois representation is of \mathbf{GL}_2 -type. This implies that the characteristic polynomials $h_p(x)$ factor as $g_p(x)g_p^\sigma(x)g_p^{\sigma^2}(x)$ for a quadratic polynomial $g_p(x) \in \mathbb{Z}_K[x]$, where $\mathbb{Z}_K = \mathbb{Z}[t]/(t^3 + t^2 - 2t - 1)$ is the ring of integers of K and σ generates the Galois group of K over \mathbb{Q} .

p	$g_p(x)$	Trace
5	$1 - tx + 5x^2$	-1
11	$1 - tx + 11x^2$	-1
13	$1 + (3 - t)x + 13x^2$	-10
17	$1 + (-1 - 4t)x + 17x^2$	-1
19	$1 + (6 - 3t - 2t^2)x + 19x^2$	-11
23	$1 + (8 - t - 3t^2)x + 23x^2$	-10
29	$1 + (8 - 5t - 6t^2)x + 29x^2$	1
31	$1 + (7 - t - 2t^2)x + 31x^2$	-12
37	$1 + (6 - 4t - 5t^2)x + 37x^2$	3
41	$1 + 8x + 41x^2$	-24
43	$1 + (4 - t - 2t^2)x + 43x^2$	-3

Table : Factorization of $h_p(x) = g_p(x)g_p^\sigma(x)g_p^{\sigma^2}(x)$, trace of Frob_p at good primes. $\mathbb{Z}_K = \mathbb{Z}[t]/(t^3 + t^2 - 2t - 1)$.

p	$g_p(x)$	Trace
47	$1 + (10 - t - 4t^2)x + 47x^2$	-11
53	$1 + (6 + 2t - 5t^2)x + 53x^2$	9
59	$1 + (10 - 6t - 9t^2)x + 59x^2$	9
61	$1 + (-2 + 3t)x + 61x^2$	9
67	$1 + (4 - t - 2t^2)x + 67x^2$	-3
71	$1 + (10 - 4t - 5t^2)x + 71x^2$	-9
79	$1 + (7 - 8t - 9t^2)x + 79x^2$	16
83	$1 + (1 - 3t - 6t^2)x + 83x^2$	24
89	$1 + (19 - t - 11t^2)x + 89x^2$	-3

Table : Factorization of $h_p(x) = g_p(x)g_p^\sigma(x)g_p^{\sigma^2}(x)$, trace of Frob_p at good primes. $\mathbb{Z}_K = \mathbb{Z}[t]/(t^3 + t^2 - 2t - 1)$.

Thanks to

Ling Long, Luca Candelori, Jennifer Li
and Robert Perlis!