Genus 3 curves with nontrivial multiplications: Questions

Jerome William Hoffman

Louisiana State University

April 14, 2015

Slides can be found at

https://www.math.lsu.edu/∼hoffman/tex/EndJac/EndJacQuestions2.pdf

Let X be a projective nonsingular algebraic curve of genus g (defined over a field of characteristic 0). Let $A = \mathrm{Jac}(X)$ 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 $X \mapsto \mathrm{Jac}(X) : \mathfrak{M}_g \to \mathfrak{A}_g$ 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, $\mathrm{End}(A) \otimes \mathbb{Q}$ is a finite-dimensional semisimple algebra with involution (usually just $\mathbb{Q}$). The different possible types were classified by A. A. Albert.

Problem

Fix an order R in an admissible algebra in the above sense. Write down universal families of curves X of genus 3 such that $\mathrm{End}(\mathrm{Jac}(X))$ contains R.

To be more precise, we want to find equations Shimura varieties and the families of abelian varieties (principally polarized of dimension 3) that they parametrize.

Problem

Construct families of genus 2 curves

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

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

Interesting cases

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

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.
3. Example: $\tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \in \mathfrak{H}_2$ 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).

Method I: Rosenhain Invariants; Thomae's formulas

We can write a genus 2 curve as

$$y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$$

Then

$$\lambda_1 = \frac{\theta_{0000}^2\theta_{0010}^2}{\theta_{0011}^2\theta_{0001}^2}, \quad \lambda_2 = \frac{\theta_{0010}^2\theta_{1100}^2}{\theta_{0001}^2\theta_{1111}^2}, \quad \lambda_3 = \frac{\theta_{0000}^2\theta_{1100}^2}{\theta_{0011}^2\theta_{1111}^2},$$

where $\theta_m = \theta_m(0,\tau)$, $m = (m', m'') \in \mathbb{Z}^4$, $\tau \in \mathfrak{H}_2$, $z \in \mathbb{C}^2$ and

$$\theta_{\boldsymbol{m}}(z,\tau) = \sum_{\boldsymbol{p}\in\mathbb{Z}^2} \mathbf{e}\left(\frac{1}{2}\left(p+\frac{m'}{2}\right)\tau\,{}^{\boldsymbol{t}}\left(p+\frac{m'}{2}\right) + \left(p+\frac{m'}{2}\right){}^{\boldsymbol{t}}\left(z+\frac{m''}{2}\right)\right).$$

$\mathbf{e}(w) := \exp(2\pi i w)$.

Method I: Humbert surface for $D = 5$

1. A 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

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

where $p_{k,j}$ is kth 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
$$3x_i^2 = s_2,\ x_i = -x_j, \quad 1 \leq i < j \leq 6.$$
2. In $\mathfrak{A}_2[2]$, Shimura curves of discriminant 10 have equations
$$x_i + 5x_j = 0,\ 3x_i^2 = s_2, \quad 1 \leq i \neq j \leq 6.$$
3. In $\mathfrak{A}_2[2]$, Shimura curves of discriminant 15 have equations
$$15(x_i + x_j)^2 = 4(s_2 + 3x_ix_j),\ 6x_i + 5x_j + 5x_k = 0,$$
$$1 \leq i \neq j \neq k \neq i \leq 6.$$

Method II: Kummer Surfaces. Besser; Elkies and Kumar

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

Dolgachev and A. Kumar proved:

Theorem

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

Let A be the elliptic K3 surface with equation

$$y^2 = x^3 - t^3\left(\frac{I_4}{12}+1\right)x + t^5\left(\frac{I_{10}}{4}t^2 + \frac{I_2 I_4 - 3I_6}{108}t + \frac{I_2}{24}\right),$$

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 $(I_2 : I_4 : I_6 : I_{10})$. Then A and $\mathrm{Km}(C)$ 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 $\mathcal{F}_{L_D} \to \mathcal{H}_D$.

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: Humbert surface with $D = 5$

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).

Problem: genus 3 hyperelliptic moduli

Give the analog of Mestre's algorithm for constructing a hyperelliptic curve of genus 3 from its Shioda invariants.

Genus 3 curves: nonhyperelliptic moduli

Let $(\mathbf{P}^7_2)^{ss}$ be the subset of $(\mathbf{P}^2)^7$ which is semistable in the sense of Mumford's Geometric Invariant theory for the canonical action of PGL_3.
Then there is a canonical isomorphism

$$(\mathbf{P}^7_2)^{ss} \cong \mathfrak{M}_3[2] \ - \mathcal{H}yp_3[2],$$

where $\mathfrak{M}_3[2]$ is the moduli space of genus 3 curves with a level 2 structure on their Jacobians, and $\mathcal{H}yp_3[2]$ is the hyperelliptic locus.

Given $(p_1, \ldots, p_7) \in (\mathbf{P}^7_2)^{ss}$, blowing up these 7 points gives a delPezzo surface $\mathcal{F}$ together with a degree 2 map $\mathcal{F} \to \mathbf{P}^2$, which is branched along a smooth quartic curve (of genus 3), C. This C is birationally equivalent to a sextic curve $S \subset \mathbf{P}^2$ which has nodes at $p_1, \ldots, p_7$.

Genus 3 curves: nonhyperelliptic moduli

Schottky showed that the nodal sextic S had equations

$$L_{a,b}L_{c,d}Q_{a,c}Q_{b,d} - L_{a,c}L_{b,d}Q_{a,b}Q_{c,d} = 0,$$

where $\{a, b, c, d\} \subset \{1, 2, 3, 4, 5, 6, 7\}$ and

$$\begin{aligned} L_{a,b} &= \text{the line connecting } a, b. \\ Q_{a,b} &= \text{the conic through } \{1,2,3,4,5,6,7\} - \{a, b\}. \end{aligned}$$

Moreover, he showed that the coefficients in the $L_{a,b}$, $Q_{a,b}$ where given by explicit expressions in the theta constants attached to the period matrix $\tau \in \mathfrak{H}_3$ of the curve C (or S).

Problem: nonhyperelliptic moduli as Siegel modular forms

Give a modern treatment of these results of Frobenius and Schottky.

These results express the algebraic moduli of nonhyperelliptic genus 3 curves as automorphic forms on $\mathfrak{H}_3$

Theorem: Kondō and Looijenga

There is an isomorphism between the algebra of regular functions on the space of quartic polynomials in 3 variables invariant under $\mathrm{SL}(3, \mathbb{C})$ and a space of meromorphic automorphic forms on the complex 6-ball.

Thus the moduli of nonhyperelliptic genus 3 curves is essentially a quotient $\Gamma \backslash \mathbb{B}_6$, for an arithmetic subgroup $\Gamma \subset \mathrm{U}(6, 1)$.

Problem: nonhyperelliptic moduli and automorphic forms

Relate these 2 different descriptions of moduli space of nonhyperelliptic genus 3 curves via automorphic forms.

Theorem: Kondō, Looijenga and Artebani

The moduli space of nonhyperelliptic curves of genus 3 is a period domain for a family of K3 surfaces.

Problem: nonhyperelliptic moduli and K3 surfaces

Describe the K3 surfaces corresponding to curves of genus 3 with nontrivial multiplications.

The model here are the results of Elkies and Kumar in genus 2.

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).

Problem: endomorphisms of Jacobians

Write down equations for the Shimura varieties belonging to the above endomorphism algebra and the universal families of genus 3 to which they correspond.

Very few explicit examples are known.

Picard's family

Picard studied the family of genus 3 curves:

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

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

The parameter space is isomorphic to $\Gamma \backslash \mathbb{B}_2$ where $\Gamma \subset \mathrm{SU}(2,1;R)$ 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 $\mathrm{End}(\mathrm{Jac}(\mathrm{C}))$ 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 $\mathrm{Jac}(X)$.

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

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

Our case:

$$G = D_7 =< \sigma, \tau \mid \sigma^7 = \tau^2 = 1, \tau\sigma\tau = \sigma^6 >$$

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

$$
\begin{tikzcd}
 & \{e\} \arrow[dl] \arrow[ddr] & \\
\langle\tau\rangle \arrow[ddr] & & \\
 & & \langle\sigma\rangle \arrow[dl] \\
 & D_7 &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & Y_{\text{ genus } 8} \arrow[dl, "h"'] \arrow[ddr, "q \text{ unramified}"] & \\
{}_{\text{genus } 3}\, X \arrow[ddr, "v"'] & & \\
 & & C_{\text{ genus } 2} \arrow[dl, "x"] \\
 & \mathbf{P}^1 &
\end{tikzcd}
$$

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

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

In general, one expects that the image is all of $\mathbf{GSp}_{2g}(\mathbb{Q}_l)$.

If $\mathrm{End}(\mathrm{Jac}(X)) \otimes \mathbb{Q}$ 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 $\mathbb{Z}[\zeta_7 + \bar{\zeta}_7]$

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

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

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

where $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GSp}(H^1_{\mathrm{et}}(X \otimes \overline{\mathbb{Q}}, \mathbb{Q}_l))$ is the canonical Galois representation in étale cohomology, and Frob_p=Frobenius.

Zeta function and Galois representation for X

Since the Jacobian of X has endomorphisms in the field $K = \mathbb{Q}(\zeta_7 + \overline{\zeta}_7)$, 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!