Abelian surfaces with fixed three torsion

Shiva Chidambaram

University of Chicago

shivac@uchicago.edu

Joint work with Frank Calegari and David P. Roberts

Fourteenth Algorithmic Number Theory Symposium

June 30, 2020

Introduction

- C - smooth curve over $\mathbb{Q}$ of genus g.
- $A = \mathrm{Jac}(C)$ is a principally polarised abelian variety of dimension g.
- $\overline{\rho} : G_{\mathbb{Q}} \longrightarrow \mathrm{GSp}(2g, \mathbb{F}_p)$ is the Galois representation on the p-torsion subgroup $A[p]$. The similitude character corresponds to the mod p cyclotomic character under $\overline{\rho}$.

Conversely...

Given $\overline{\rho}$ with cyclotomic similitude character, can we find all ppavs A whose p-torsion is given by $\overline{\rho}$? What is this moduli space?

Genus 1

$X(p)$ - modular curve with full level p-structure. It corresponds to $\overline{\rho}_0 = \mathbb{Z}/p \oplus \mu_p$.

$X(p)$ has genus 0 only for $p = 2, 3, 5$. Moreover, for these values of p, it is isomorphic to $\mathbf{P}^1$ over $\mathbb{Q}$.

For general $\overline{\rho}$ with cyclotomic determinant, the moduli space $X(\overline{\rho})$ of pairs (E, i) where E is an elliptic curve and $i : E[p] \xrightarrow{\simeq} \overline{\rho}$ is a symplectic isomorphism, is a twist of $X(p)$.

Theorem (Rubin-Silverberg)

$X(\overline{\rho})$ is rational for $p = 2, 3, 5$. The Magma command `RubinSilverbergPolynomials(n,j)` *describes the family.*

Prior work in genus 2

Theorem (Bruin-Nasserden)

The moduli space $\mathcal{A}_2(3)$ is rational, and there is an explicit description of the universal curve over this space.

Theorem (Calegari-C)

The moduli space $\mathcal{A}_2(\overline{\rho})$ is not rational in general. But it always has a unirational cover of degree at most 6.

Theorem (Boxer-Calegari-Gee-Pilloni)

The moduli space $\mathcal{M}_2^w(\overline{\rho})$ of genus 2 curves with a Weierstrass point and three torsion isomorphic to $\overline{\rho}$ is rational.

Main result

Let $C : y^2 = x^5 + ax^3 + bx^2 + cx + d$ be a smooth genus 2 curve.

Theorem (Calegari-C-Roberts)

There are explicit polynomials $A, B, C, D \in \mathbb{Q}[a, b, c, d, s, t, u, v]$ homogenous of degrees $12, 18, 24, 30$ in the variables s, t, u, v parametrizing all Weierstrass curves giving rise to same 3-torsion.

$$\mathbf{P}^3(\mathbb{Q}) \ni (s : t : u : v) \mapsto C' : y^2 = x^5 + A\,x^3 + B\,x^2 + C\,x + D.$$

- The curve corresponding to the point $(1 : 0 : 0 : 0)$ is C.
- This describes the universal curve over $\mathcal{M}_2^w(\overline{\rho})$.
- The polynomials A, B, C and D have respectively $14604, 112763, 515354$ and 1727097 terms.
- The coefficients are in fact in $\mathbb{Z}\left[\frac{1}{5}\right]$.

Transferring modularity

Corollary

Suppose C has good ordinary reduction at 3, and $A = \mathrm{Jac}(C)$ satisfies the conditions of [BCGP18 Prop. 10.1.1. and 10.1.3.] so that C is modular. Then, if C' is a curve in the above family and has good reduction at 3, C' is also modular.

One can thus produce infinitely many modular abelian surfaces, by considering $(s : t : u : v) \in \mathbf{P}^3(\mathbb{Q})$ which reduce to $(1 : 0 : 0 : 0) \in \mathbf{P}^3(\mathbb{F}_3)$.

Example (Calegari-C-Ghitza)

$C : y^2 = (x^2 + 2x + 2)(x^2 + 2)x;\ (a, b, c, d) = \left(\frac{12}{5}, \frac{12}{5^2}, \frac{292}{5^3}, \frac{-3672}{5^5}\right).$

$C' : y^2 = (2x^4 + 2x^2 + 1)(2x + 3);\ (A, B, C, D) = \left(\frac{2^7}{5}, \frac{2^{11}57}{5^2}, \frac{-2^{12}503}{5^3}, \frac{2^{17}17943}{5^5}\right).$

We realize these as occuring in a family, with C given by $(1 : 0 : 0 : 0)$ and C' given by $\left(\frac{129}{125}, \frac{11}{25}, \frac{3}{100}, \frac{1}{20}\right)$.

Questions?

Subrepresentations in torsion field

- Write down a division polynomial that cuts out an extension $K|\mathbb{Q}$ with Galois group G that is generically $\mathrm{GSp}(2g, \mathbb{F}_p)$.
- $K = \mathbb{Q}[G]$ as a G-representation and the roots of this polynomial generate a representation V inside $\mathbb{Q}[G]$ of small dimension.
- For the small (g, p) we consider, this V is irreducible.

This process is reversible and any copy of V inside K gives an abelian variety with the same p-torsion. Since the isotypical component is $V \otimes V^*$, this identifies the moduli space with $\mathbf{P}(V^*)$.

Computational problem

Given V inside $K = \mathbb{Q}[G]$, how to find the "other" copies of it inside K explicitly?

Remark. Usually V is defined over $F = \mathbb{Q}(\zeta_p)$. So we work with $G = \mathrm{Gal}(K|F)$ and keep track of descent.

Invariant theory of reflection groups

A map $V \to K$ of representations induces a map $\mathrm{Sym}(V) \to K$. So it is enough to find the V-isotypical piece inside $\mathrm{Sym}(V)$.

Theorem (Chevalley-Shephard-Todd)

A pair (G, V) consisting of a finite group G with a representation V is a complex reflection group if and only if $\mathrm{Sym}(V)^G$ is a polynomial algebra.

The isotypical piece of an irrep π inside $\mathrm{Sym}(V)$ is a free module over the invariant algebra $\mathrm{Sym}(V)^G$ of rank equal to $\dim \pi$.

We are (almost) in this situation, and so we exploit the invariant theory of complex reflection groups.

Invariants, covariants and contravariants

(g,p)	**(1,2)**	**(1,3)**	**(2,3)**
Group G	S_3	$\mathrm{SL}(2,\mathbb{F}_3)$	$\mathrm{Sp}(4,\mathbb{F}_3) \times \mathbb{Z}/3\mathbb{Z}$
The invariant algebra $\mathrm{Sym}(V)^G$ has generators in degrees	2 3	4 6	12 18 24 30
V-isotypical piece has generators in degrees	1 2	1 3	1 7 13 19
V^*-isotypical piece has generators in degrees	1 2	3 5	11 17 23 29

Main computation

Let $C : y^2 = x^5 + ax^3 + bx^2 + cx + d$, $A = \mathrm{Jac}(C)$, $\Delta = \mathrm{disc}\, C$.

★ The degree 240 polynomial $p_{40}(z^6)$ is nicer than the 3-division polynomial $p_{40}(z^2)$. Its splitting field is $K(\Delta^{1/3})$ with Galois group over F given by $G = \mathrm{Sp}(4, \mathbb{F}_3) \times \mathbb{Z}/3\mathbb{Z}$.

- Roots generate the 4-dimensional reflection representation $V = F[z_1, z_2, z_3, z_4]_1$, where we map z_4 to a root.
- We find covariants $\alpha_k \in F[z_1, z_2, z_3, z_4]_k$ for $k = 1, 7, 13, 19$.
- A general covariant $\alpha = s\alpha_1 + t\alpha_7 + u\alpha_{13} + v\alpha_{19}$ gives a copy of V inside K, by sending $z_4 \mapsto \alpha$.
- The corresponding invariants suitably normalized give Weierstrass coefficients of our family.

Further remarks

- Contravariants parametrize the moduli space $\mathcal{M}_2^{w*}(\overline{\rho})$ of Weierstrass curves with an anti-symplectic isomorphism of three torsion with $\overline{\rho}$.
- Richelot isogenies swap the two moduli spaces.
- Using Shioda's polynomials for $W(E_7)$ and $W(E_8)$, one can in principle tackle versions of this problem for $p = 2$ and $g = 3, 4$, but the results are expected to be huge.

Thank you

References

George Boxer, Frank Calegari, Toby Gee, and Vincent Pilloni. (2018)
Abelian surfaces over totally real fields are potentially modular.
Preprint. arXiv:1812.09269 [math.NT]

Nils Bruin and Brett Nasserden. (2018)
Arithmetic aspects of the Burkhardt quartic threefold.
J. Lond. Math. Soc. (2), 98(3) : 536-556.

Frank Calegari and Shiva Chidambaram. (2020)
Rationality of twists of $\mathcal{A}_2(3)$.
Preprint.

Tom Fisher. (2012)
The Hessian of a genus one curve.
Proceedings of the London Mathematical Society, 104(3) : 613-648.

K. Rubin and A. Silverberg. (1995)
Families of elliptic curves with constant mod p representations.
Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, 148 - 161. Int. Press, Cambridge, MA.

Tetsuji Shioda. (1991)
Construction of elliptic curves with high rank via the invariants of the Weyl groups.
J. Math. Soc. Japan, 43(4) : 673-719.