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 26, 2020

Torsion in abelian varieties

Let C be a smooth genus g curve over $\mathbb{Q}$.
Let $A = \mathrm{Jac}\, C = \mathrm{Pic}^o(C)$ be its Jacobian variety. A is a principally polarized abelian variety over $\mathbb{Q}$ of dimension g.

Over $\mathbb{C}$, A is a torus. $A \simeq \mathbb{C}^g/\Lambda$ for some lattice Λ.
So $A[p] \simeq (\mathbb{Z}/p)^{2g}$ as abelian groups.

The polarisation induces a non-degenerate alternating bilinear pairing on $A[p]$ called the **Weil pairing**.

The Galois action on $A[p]$, being equivariant with respect to the Weil pairing, gives a representation

$$\overline{\rho} : G_{\mathbb{Q}} \longrightarrow \mathrm{GSp}(2g, \mathbb{F}_p)$$

with similitude character equal to the mod p cyclotomic character.

Questions

Can we parametrize all ppavs A of dimension g which have the same p-torsion representation?

This is a very hard problem in general.

Theorem

The moduli space $\mathcal{A}_g(p)$ of ppavs of dimension g with full level p structure is geometrically rational only for $(g, p) =$

$$(1,2), \quad (1,3), \quad (1,5), \quad (2,2), \quad (2,3), \quad (3,2).$$

Rubin-Silverberg constructed explicit families of elliptic curves with fixed p-torsion representations for $p = 3$ and 5.

Main result

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** *genus 2 curves with the 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 $C : y^2 = x^5 + ax^3 + bx^2 + cx + d$.
- The polynomials A, B, C and D have respectively $14604, 112763, 515354$ and 1727097 terms.
- The coefficients are in fact in $\mathbb{Z}\left[\frac{1}{5}\right]$.

*It is all curves with a Weierstrass point. This moduli space is rational, as opposed to $\mathcal{M}_2(\overline{\rho})$.

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 starting with a C as above, and considering for example, the points $(s : t : u : v) \in \mathbf{P}^3(\mathbb{Q})$ which reduce to $(1 : 0 : 0 : 0) \in \mathbf{P}^3(\mathbb{F}_3)$.

Subrepresentation inside 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 $\mathbb{Q}(\zeta_p)$. So we work with $\mathrm{Gal}(K|\mathbb{Q}(\zeta_p))$ and keep track of descent.

Elliptic curves

Let $E : y^2 = f(x) = x^3 + ax + b$ over $\mathbb{Q}$.

Example (p = 2)

- A division polynomial is $f(x)$, whose splitting field K has Galois group S_3 over $\mathbb{Q}$. Roots of f generate the unique 2-dim irrep V of S_3 because trace is 0.
- Conversely, given V inside K, it has a unique element (upto scalars) fixed by a chosen order 2 subgroup of S_3. Its minimal polynomial is $g(x) = x^3 + Ax + B$, and the elliptic curve $y^2 = g(x)$ has the same 2-torsion.

Example (p = 3)

A division polynomial is $p(z) = z^8 + 18az^4 + 108bz^2 - 27a^2$, whose roots generate a 2-dim irrep of $\mathrm{SL}(2, \mathbb{F}_3)$ inside the splitting field $K = \mathbb{Q}(\zeta_3)[\mathrm{SL}(2, \mathbb{F}_3)]$. How to find the other copies?

Complex reflection groups

We have a map $V \to K$ of representations given by the roots of the division polynomial. It 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.

In this situation, the V-isotypical piece inside $\mathrm{Sym}(V)$ is a free module over the invariant algebra $\mathrm{Sym}(V)^G$ of rank equal to $\dim V$.

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

Invariants and covariants

(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

For any copy of V in K, the invariants suitably normalized give Weierstrass coefficients of the corresponding curve.

Three torsion of genus 2 curves

Let $C : y^2 = x^5 + a\ x^3 + b\ x^2 + c\ x + d$ over $\mathbb{Q}$ and $\Delta = \operatorname{disc} C$.
Let $A = \operatorname{Jac} C$.

There is a polynomial $p_{40}(z) =$

$$z^{40} + 15120a\ z^{38} + 2620800b\ z^{37} - 504(70277a^2 - 831820c)\ z^{36}$$
$$- 1965600(2529ab - 33550d)\ z^{35} + \cdots$$

which describes the field cut out by $\mathbf{P}\overline{\rho} : G_{\mathbb{Q}} \longrightarrow \mathrm{PGSp}(4, \mathbb{F}_3)$.

The polynomial $p_{40}(z^2)$ describes $K = \mathbb{Q}(A[3]) = \overline{\mathbb{Q}}^{\ker \overline{\rho}}$.

Contrasting genus 1 and 2

★ The degree 240 polynomial $p_{40}(z^6)$ is nicer. Its splitting field is $K(\Delta^{1/3})$, whose Galois group over $\mathbb{Q}(\zeta_3)$ is the exceptional complex reflection group $G = \mathrm{Sp}(4, \mathbb{F}_3) \times \mathbb{Z}/3\mathbb{Z}$.

- Its roots generate the 4-dimensional reflection representation of G.

★ The family we obtain also has the field $\mathbb{Q}(\Delta^{1/3})$ fixed, even though this is not contained in $K = \mathbb{Q}(A[3])$. A genus 2 curve $C : y^2 = f(x)$ also does not determine $\mathbb{Q}(\Delta^{1/3})$ because scaling by t changes Δ by t^{40}. So this is okay.

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]

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.