Superelliptic curves with large Galois images

Pip Goodman

Mod ℓ representations

Let ℓ be a prime. Let A be a principally polarised abelian variety of dimension g over a number field K.

The ℓ-torsion subgroup of $A(\overline{K})$, that is, $A[\ell] := \{P \in A(\overline{K}) | \ell P = 0\}$ has the structure of $2g$ dimensional vector space over $\mathbb{F}_\ell$:

$$A[\ell] \cong \mathbb{F}_\ell^{2g}.$$

The absolute Galois group G_K acts linearly on this space, giving a representation

$$\rho_\ell \colon G_K \to \mathrm{GL}_{2g}(\ell).$$

Furthermore, the Weil pairing (which is a non-degenerate symplectic pairing) $A[\ell] \times A[\ell] \to \mathbb{F}_\ell^*$, is preserved up to similitude by G_K.

Together with the above, this means our representation lands in the subgroup

$$\rho_\ell \colon G_K \to \mathrm{GSp}_{2g}(\ell).$$

Mod ℓ representations

Let ℓ be a prime. Let A be a principally polarised abelian variety of dimension g over a number field K.

The ℓ-torsion subgroup of $A(\overline{K})$, that is, $A[\ell] := \{P \in A(\overline{K}) | \ell P = 0\}$ has the structure of $2g$ dimensional vector space over $\mathbb{F}_\ell$:

$$A[\ell] \cong \mathbb{F}_\ell^{2g}.$$

The absolute Galois group G_K acts linearly on this space, giving a representation

$$\rho_\ell \colon G_K \to \mathrm{GL}_{2g}(\ell).$$

Furthermore, the Weil pairing (which is a non-degenerate symplectic pairing) $A[\ell] \times A[\ell] \to \mathbb{F}_\ell^*$, is preserved up to similitude by G_K.

Together with the above, this means our representation lands in the subgroup

$$\rho_\ell \colon G_K \to \mathrm{GSp}_{2g}(\ell).$$

Mod ℓ representations

Let ℓ be a prime. Let A be a principally polarised abelian variety of dimension g over a number field K.

The ℓ-torsion subgroup of $A(\overline{K})$, that is, $A[\ell] := \{P \in A(\overline{K}) | \ell P = 0\}$ has the structure of $2g$ dimensional vector space over $\mathbb{F}_\ell$:

$$A[\ell] \cong \mathbb{F}_\ell^{2g}.$$

The absolute Galois group G_K acts linearly on this space, giving a representation

$$\rho_\ell \colon G_K \to \mathrm{GL}_{2g}(\ell).$$

Furthermore, the Weil pairing (which is a non-degenerate symplectic pairing) $A[\ell] \times A[\ell] \to \mathbb{F}_\ell^*$, is preserved up to similitude by G_K.

Together with the above, this means our representation lands in the subgroup

$$\rho_\ell \colon G_K \to \mathrm{GSp}_{2g}(\ell).$$

Images of mod ℓ representations

Serre's Open Image Theorem
Let E/K be an elliptic curve with $\mathrm{End}(E) \cong \mathbb{Z}$. Then for all but finitely many primes ℓ, we have $\mathrm{Gal}(K(E[\ell])/K) = \mathrm{GL}_2(\ell)$.

Theorem (Hall '08)
Let $C : y^2 = f(x)$, where $f \in K[x]$ has degree $2g+1$. Let $J = \mathrm{Jac}(C)$. Suppose $\mathrm{End}(J) \cong \mathbb{Z}$, and f has a double root modulo some prime p. Then for all but finitely many primes ℓ, we have $\mathrm{Gal}(K(J[\ell])/K) = \mathrm{GSp}_{2g}(\ell)$.

Theorem (Anni, V. Dokchitser '20)
Let g be a positive integer so that $2g+2$ satisfies "double Goldbach + ε". Then one may find an explicit hyperelliptic curve defined over $\mathbb{Q}$ of genus g such that the associated mod ℓ images are maximal for all primes ℓ.

Images of mod ℓ representations

Serre's Open Image Theorem
Let E/K be an elliptic curve with $\mathrm{End}(E) \cong \mathbb{Z}$. Then for all but finitely many primes ℓ, we have $\mathrm{Gal}(K(E[\ell])/K) = \mathrm{GL}_2(\ell)$.

Theorem (Hall '08)
Let $C : y^2 = f(x)$, where $f \in K[x]$ has degree $2g + 1$. Let $J = \mathrm{Jac}(C)$. Suppose $\mathrm{End}(J) \cong \mathbb{Z}$, and f has a double root modulo some prime p. Then for all but finitely many primes ℓ, we have $\mathrm{Gal}(K(J[\ell])/K) = \mathrm{GSp}_{2g}(\ell)$.

Theorem (Anni, V. Dokchitser '20)
Let g be a positive integer so that $2g + 2$ satisfies "double Goldbach + ε". Then one may find an explicit hyperelliptic curve defined over $\mathbb{Q}$ of genus g such that the associated mod ℓ images are maximal for all primes ℓ.

What about “natural” subgroups of $\mathrm{GSp}_{2g}(\ell)$?

The rough intuition for the image ρ_ℓ is that it should be as big as possible. In other words, it should be $\mathrm{GSp}_{2g}(\ell)$ unless there is a good reason.

What’s a good reason?

What about "natural" subgroups of $\mathrm{GSp}_{2g}(\ell)$?

The rough intuition for the image ρ_ℓ is that it should be as big as possible. In other words, it should be $\mathrm{GSp}_{2g}(\ell)$ unless there is a good reason.

What's a good reason? Endomorphisms!

Natural source of endomorphisms?

Let r be an odd prime, $f \in \mathbb{Q}(\zeta_r)[x]$ without repeated roots.

Let C be the smooth projective curve defined by the affine model

$$y^r = f(x).$$

There is a natural automorphism on C coming from $y \mapsto \zeta_r y$.

This induces an automorphism

$$[\zeta_r] \colon J \to J$$

on the jacobian J of C.

$[\zeta_r]$ gives rise to an automorphism on $J[\ell]$ for each $\ell \neq r$.

This automorphism preserves our the Weil pairing.

Hence the image of

$$G_{\mathbb{Q}(\zeta_r)} \to \mathrm{GSp}_{2g}(\ell)$$

lies in the centraliser of $[\zeta_r] \in \mathrm{GSp}_{2g}(\ell)$.

Natural source of endomorphisms?

Let r be an odd prime, $f \in \mathbb{Q}(\zeta_r)[x]$ without repeated roots.

Let C be the smooth projective curve defined by the affine model

$$y^r = f(x).$$

There is a natural automorphism on C coming from $y \mapsto \zeta_r y$.

This induces an automorphism

$$[\zeta_r]\colon J \to J$$

on the jacobian J of C.

$[\zeta_r]$ gives rise to an automorphism on $J[\ell]$ for each $\ell \neq r$.

This automorphism preserves our the Weil pairing.

Hence the image of

$$G_{\mathbb{Q}(\zeta_r)} \to \mathrm{GSp}_{2g}(\ell)$$

lies in the centraliser of $[\zeta_r] \in \mathrm{GSp}_{2g}(\ell)$.

What does the centraliser of $[\zeta_r]$ look like?

How does one show $\rho_\ell(G_K)$ is “as big as possible”?

A group theory checklist

Theorem (Arias-de-Reyna, Dieulefait, Wiese ’16)
Let $G \leq \mathrm{GSp}_{2g}(\ell)$ be a subgroup containing a transvection, $\ell \geq 5$ prime. If G does not contain $\mathrm{Sp}_{2g}(\ell)$, then one of the following holds:

- G is a reducible subgroup;
- G is an imprimitive subgroup.

Theorem (G.’20)
Let $G \leq \mathrm{GL}_n(\ell^i)$ be a subgroup containing a transvection, $\ell \geq 5$ prime. If G does not contain $\mathrm{SL}_n(\ell^i)$, then one of the following holds:

- G is a reducible subgroup;
- G is an imprimitive subgroup;
- G is contained in $\mathrm{GL}_n(\ell^j)$ with $j < i$;
- G is contained in $\mathrm{GSp}_n(\ell^i)$ or $\mathrm{GU}_n(\ell^{i/2})$.

A similar result holds for $\mathrm{GU}_n(\ell^{i/2})$.

A group theory checklist

Theorem (Arias-de-Reyna, Dieulefait, Wiese '16)
Let $G \leq \mathrm{GSp}_{2g}(\ell)$ be a subgroup containing a transvection, $\ell \geq 5$ prime. If G does not contain $\mathrm{Sp}_{2g}(\ell)$, then one of the following holds:

- G is a reducible subgroup;
- G is an imprimitive subgroup.

Theorem (G.'20)
Let $G \leq \mathrm{GL}_n(\ell^i)$ be a subgroup containing a transvection, $\ell \geq 5$ prime. If G does not contain $\mathrm{SL}_n(\ell^i)$, then one of the following holds:

- G is a reducible subgroup;
- G is an imprimitive subgroup;
- G is contained in $\mathrm{GL}_n(\ell^j)$ with $j < i$;
- G is contained in $\mathrm{GSp}_n(\ell^i)$ or $\mathrm{GU}_n(\ell^{i/2})$.

A similar result holds for $\mathrm{GU}_n(\ell^{i/2})$.

Control of inertia subgroups

Let $\mathfrak{p}$ be a prime of $\mathbb{Q}(\zeta_r)$ dividing the rational prime p.

Theorem (T. Dokchitser '18)
Let C be a curve defined by $f(x, y) = 0$ with $f \in \mathbb{Q}(\zeta_r)[x, y]$, satisfying some additional hypothesis.

Then the action of the inertia group $I_{\mathfrak{p}}$ on $V_\ell(\mathrm{Jac}(C))$, $p \neq \ell$, can be deduced from the $\mathfrak{p}$-adic valuations of the coefficients of f.

Furthermore, Tim's results give a regular model of the curve with strict normal crossings. This is important for producing transvections.

So far...

Theorem (G.'20)
Let $d \geq 12$ be a natural number divisible by $2r$ which is also the sum of two distinct primes $q_1 < q_2$.

Suppose there exists a prime $q_2 < q_3 < d$. If $r > 23$ assume the class number of $\mathbb{Q}(\zeta_r)$ is odd and $d = q_3 + 1$.

Then given a polynomial $f \in \mathbb{Q}(\zeta_r)[x]$ of degree d whose coefficients satisfy certain congruence conditions, the image of the representation $\rho_\ell \colon G_{\mathbb{Q}(\zeta_r)} \to \mathrm{Aut}(J[\ell])$ contains the products

- $\mathrm{SL}_n(\ell^i)^{\frac{r-1}{2i}}$ if i the inertia degree of ℓ in $\mathbb{Q}(\zeta_r)$ is odd; and
- $\mathrm{SU}_n(\ell^{i/2})^{\frac{r-1}{i}}$ if i the inertia degree of ℓ in $\mathbb{Q}(\zeta_r)$ is even

for all ℓ outside of a small finite explicit set.

The last mile

The last mile

When looking at $y^3 = f(x)$ of genus g, and primes $p \equiv 1 \mod 3$, I found:

g	3	4	6	7
$\det \circ \rho_\lambda\,(\mathrm{Frob}_{\mathfrak{p}})$	$p\mathfrak{p}$	$p\mathfrak{p}^2$	$p^2\mathfrak{p}^2$	$p^2\mathfrak{p}^3$

CM theory

Let A/K be a g dimensional abelian variety such that $\mathrm{End}^0(A)$ is a field of dimension $2g$ over $\mathbb{Q}$. Such abelian varieties are said to have complex multiplication.

The endomorphism algebra allows us to view the λ-adic representations as being one dimensional, i.e., characters.

The Main Theorem of Complex Multiplication tells us there exists an algebraic Hecke character $\Omega\colon \mathbb{A}_K^* \to \mathbb{C}$ and each of the λ-adic representations can be obtained from Ω.

Furthermore, the infinity type of Ω is determined by the Shimura-Taniyama formula.

In our situation, we also get an algebraic Hecke character giving rise to the $\det \circ \rho_\lambda$.

CM theory

Let A/K be a g dimensional abelian variety such that $\mathrm{End}^0(A)$ is a field of dimension $2g$ over $\mathbb{Q}$. Such abelian varieties are said to have complex multiplication.

The endomorphism algebra allows us to view the λ-adic representations as being one dimensional, i.e., characters.

The Main Theorem of Complex Multiplication tells us there exists an algebraic Hecke character $\Omega\colon \mathbb{A}_K^* \to \mathbb{C}$ and each of the λ-adic representations can be obtained from Ω.

Furthermore, the infinity type of Ω is determined by the Shimura-Taniyama formula.

In our situation, we also get an algebraic Hecke character giving rise to the $\det \circ \rho_\lambda$.

CM theory

Let A/K be a g dimensional abelian variety such that $\mathrm{End}^0(A)$ is a field of dimension $2g$ over $\mathbb{Q}$. Such abelian varieties are said to have complex multiplication.

The endomorphism algebra allows us to view the λ-adic representations as being one dimensional, i.e., characters.

The Main Theorem of Complex Multiplication tells us there exists an algebraic Hecke character $\Omega\colon \mathbb{A}_K^* \to \mathbb{C}$ and each of the λ-adic representations can be obtained from Ω.

Furthermore, the infinity type of Ω is determined by the Shimura-Taniyama formula.

In our situation, we also get an algebraic Hecke character giving rise to the $\det \circ \rho_\lambda$.

The endomorphism character

Theorem (Fité '20)
Let A/K be an abelian variety with endomorphism algebra $E = \mathrm{End}_K(A) \otimes \mathbb{Q}$ a field. Suppose $K \supseteq E$ and $E/\mathbb{Q}$ are Galois. Then exists an algebraic Hecke character $\Omega\colon \mathbb{A}_E^* \to \mathbb{C}$ whose λ-adic avatars agree with $\det \circ \rho_\lambda$ for

$$\rho_\lambda\colon G_K \to \mathrm{Aut}(T_\lambda(A))$$

and has infinity type determined by the action of $\mathrm{End}(A)$ on $\Omega^0(A)$.

Images

Putting this all together, we can construct genus g curves $y^r = f(x) \in \mathbb{Q}(\zeta_r)[x]$ whose jacobians J satisfy the following:

Theorem (G.'20)
For all but a finite explicit list of primes ℓ, the image of

$$\rho_\ell \colon G_{\mathbb{Q}(\zeta_3)} \to \mathrm{Aut}(J[\ell])$$

is for i odd:

$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GL}_g(\ell)^{\lceil \frac{g}{3} \rceil, 6} \rtimes \langle \chi_\ell \rangle$$

and for i even:

$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GU}_g(\ell)^{\lceil \frac{g}{3} \rceil, 6} . \langle \chi_\ell \rangle.$$

Theorem (G.'20)
Let $\ell \equiv 1 \mod r$. Then for all but a finite explicit list of primes ℓ, we have

$$\bar{\rho}_\lambda(G_{\mathbb{Q}(\zeta_r)}) = \mathrm{GL}_n(\ell)$$

where $n = \frac{2g}{r-1}$.

A few examples

For $d \in \{12, 18, 24\}$ the curves

$$y^3 - \zeta_3^2 \pi y^2 - \zeta_3^2 y = x^d + x^{d-1} + 7x^3 + 14x^2 + 45\zeta_3\pi$$

where $\pi = 1 - \zeta_3$ have maximal image at all but a finite explicit list of primes.

In particular, outside this list, they satisfy

$$\bar{\rho}_\lambda(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GL}_{d-2}(\ell) \text{ for } \ell \equiv 1 \mod 3;$$

and

$$\bar{\rho}_\lambda(G_{\mathbb{Q}(\zeta_3)}) = \Delta\mathrm{U}_{d-2}(\ell) \text{ for } \ell \equiv 5, 29 \mod 36.$$

In fact, if $d = 12, 24$ this holds for $\ell \equiv 5 \mod 12$.

And another one

For $\ell \neq 2, 3, 7, 41, 701, 103950138625391659317 9$, or
$43925848740498753191116327084384430459193646663905973125796869758880866205107 35$
$1354930470916194229999769267625792575400330624106332584372975559484695436136367$
$118772361796350659366993443881953314038538101272367583$
the superelliptic curve

$$y^7 = x^{14} + \pi x^{13} + 2\pi^7 x^7 + 6\pi^{12} x^2 + 246\pi^7$$

where $\pi = 1 - \zeta_7$, has maximal image at ℓ.

If $\lambda | \ell$ with $\ell \equiv 1 \mod 7$, we have

$$\bar{\rho}_\lambda(G_{\mathbb{Q}(\zeta_7)}) = \mathrm{GL}_{12}(\ell)$$

and for $\ell \equiv 13 \mod 28$

$$\bar{\rho}_\lambda(G_{\mathbb{Q}(\zeta_7)}) = \Delta\mathrm{U}_{12}(\ell).$$

You might also like...

Generalised symmetric Chabauty

Question (Zureick-Brown)
Is it possible to determine the cubic points (that is, cubic over $\mathbb{Q}$) on $X_0(65)$, despite its infinitely many quadratic points?

Theorem (Box, Gajović, G. '21)
Let $N \in \{53, 57, 61, 65, 67, 73\}$. Then the cubic points on $X_0(N)$ are known. Moreover the isolated quartic points on $X_0(65)$ are known.

To prove this, we extended Siksek's "symmetric Chabauty" and implemented our methods in *Magma*.

Theorem (Box '21)
Elliptic curves over totally real quartic fields not containing $\sqrt{5}$ are modular.

Theorem (Banwait, Derickx)
For p prime $X_0(p)(\mathbb{Q}(\zeta_7)^+) \neq \emptyset \iff X_0(p)(\mathbb{Q}) \neq \emptyset$.

Generalised symmetric Chabauty

Question (Zureick-Brown)
Is it possible to determine the cubic points (that is, cubic over $\mathbb{Q}$) on $X_0(65)$, despite its infinitely many quadratic points?

Theorem (Box, Gajović, G. '21)
Let $N \in \{53, 57, 61, 65, 67, 73\}$. Then the cubic points on $X_0(N)$ are known. Moreover the isolated quartic points on $X_0(65)$ are known.

To prove this, we extended Siksek's "symmetric Chabauty" and implemented our methods in *Magma*.

Theorem (Box '21)
Elliptic curves over totally real quartic fields not containing $\sqrt{5}$ are modular.

Theorem (Banwait, Derickx)
For p prime $X_0(p)(\mathbb{Q}(\zeta_7)^+) \neq \emptyset \iff X_0(p)(\mathbb{Q}) \neq \emptyset$.

Generalised symmetric Chabauty

Question (Zureick-Brown)
Is it possible to determine the cubic points (that is, cubic over $\mathbb{Q}$) on $X_0(65)$, despite its infinitely many quadratic points?

Theorem (Box, Gajović, G. '21)
Let $N \in \{53, 57, 61, 65, 67, 73\}$. Then the cubic points on $X_0(N)$ are known. Moreover the isolated quartic points on $X_0(65)$ are known.

To prove this, we extended Siksek's "symmetric Chabauty" and implemented our methods in *Magma*.

Theorem (Box '21)
Elliptic curves over totally real quartic fields not containing $\sqrt{5}$ are modular.

Theorem (Banwait, Derickx)
For p prime $X_0(p)(\mathbb{Q}(\zeta_7)^+) \neq \emptyset \iff X_0(p)(\mathbb{Q}) \neq \emptyset$.

Notation

- K a number field
- $f \in K[x]$ a polynomial without repeated roots
- C_f hyperelliptic curve associated to f
- J_f the jacobian of C_f

Theorem (Zarhin '00)
Let $f \in K[x]$ have degree $n \geq 5$ and Galois group S_n or A_n. Then $\mathrm{End}(J_f) \cong \mathbb{Z}$.

Theorem (Elkin, Zarhin '06,'08)
Suppose $n = q + 1$, where $q \geq 5$ is a prime power congruent to ± 3 or 7 modulo 8. Suppose that $f(x)$ is irreducible and $\mathrm{Gal}(f) \cong \mathrm{PSL}_2(\mathbb{F}_q)$. Then either

1. $\mathrm{End}^0(J_f) = \mathbb{Q}$ or a quadratic field; or
2. $q \equiv 3, 7 \mod 8$ and $\mathrm{End}^0(J_f) \cong M_g(\mathbb{Q}(\sqrt{-q}))$.

Endomorphism algebras

Notation

- K a number field
- $f \in K[x]$ a polynomial without repeated roots
- C_f hyperelliptic curve associated to f
- J_f the jacobian of C_f

Theorem (Zarhin '00)
Let $f \in K[x]$ have degree $n \geq 5$ and Galois group S_n or A_n. Then $\mathrm{End}(J_f) \cong \mathbb{Z}$.

Theorem (Elkin, Zarhin '06,'08)
Suppose $n = q + 1$, where $q \geq 5$ is a prime power congruent to ± 3 or 7 modulo 8. Suppose that $f(x)$ is irreducible and $\mathrm{Gal}(f) \cong \mathrm{PSL}_2(\mathbb{F}_q)$. Then either

1. $\mathrm{End}^0(J_f) = \mathbb{Q}$ or a quadratic field; or
2. $q \equiv 3, 7 \mod 8$ and $\mathrm{End}^0(J_f) \cong M_g(\mathbb{Q}(\sqrt{-q}))$.

Let A/K be an abelian variety of dimension g.

Theorem (G.'19)
Suppose ℓ and $p = 2g+1$ are primes satisfying $\langle \ell \rangle = (\mathbb{Z}/p\mathbb{Z})^*$.
Suppose $\mathrm{Gal}(K(A[\ell])/K)$ contains an element of order p. Then either

1. $\mathrm{End}^0(A)$ is a number field totally inert at ℓ; or
2. $\mathrm{End}^0(A) \cong M_a(F)$ where $F \subsetneq \mathbb{Q}(\zeta_p)$ is a CM field and $a = \frac{2g}{[F:\mathbb{Q}]}$.

Corollary (G.'19)
Suppose $g = 2$, and $\mathrm{Gal}(K(A[2])/K)$ contains an element of order 5.
Then $\mathrm{End}^0(A)$ is a number field totally inert at 2.

Let A/K be an abelian variety of dimension g.

Theorem (G.'19)
Suppose ℓ and $p = 2g + 1$ are primes satisfying $\langle \ell \rangle = (\mathbb{Z}/p\mathbb{Z})^*$.
Suppose $\mathrm{Gal}(K(A[\ell])/K)$ contains an element of order p. Then either

1. $\mathrm{End}^0(A)$ is a number field totally inert at ℓ; or
2. $\mathrm{End}^0(A) \cong M_a(F)$ where $F \subsetneq \mathbb{Q}(\zeta_p)$ is a CM field and $a = \frac{2g}{[F:\mathbb{Q}]}$.

Corollary (G.'19)
Suppose $g = 2$, and $\mathrm{Gal}(K(A[2])/K)$ contains an element of order 5.
Then $\mathrm{End}^0(A)$ is a number field totally inert at 2.

The result below is key in establishing the previous theorem.

The endomophism field

Let A/K be an abelian variety of dimension g. Denote by L/K the minimal extension over which all endomorphisms of A are defined.

E.g. $E: y^2 = x^3 - 2$ has $g = 1$ and $L = \mathbb{Q}(\zeta_3)$.

Theorem (G.'19)

Suppose $p = 2g + 1$ is a prime divisor of $[L : K]$. Then $\mathrm{End}^0(A) \cong M_a(F)$ where $F \subsetneq \mathbb{Q}(\zeta_p)$ is a CM field and $a = \frac{2g}{[F:\mathbb{Q}]}$.