Twists of GL_2-type abelian varieties and Galois images for genus 2

Samuele Anni

BSD Data @ Bristol,
University of Bristol, 28th March 2017

UNIVERSITÄT HEIDELBERG
ZUKUNFT SEIT 1386

WARNING: works in progess

Two topics

- Central values of L-functions of twists of GL_2-type abelian varieties: joint work with Soma Purkait (Tokyo University of Science).
- Residual Galois images for genus 2 and 3

Proposition (Purkait, 2013)

Let E be the elliptic curve 50.b3 (Cremona label 50b1). Let Q_1, Q_2, Q_3, Q_4 be the following positive-definite ternary quadratic forms,

$$Q_1 = 25x^2 + 25y^2 + z^2, \qquad Q_2 = 14x^2 + 9y^2 + 6z^2 + 4yz + 6xz + 2xy,$$
$$Q_3 = 25x^2 + 13y^2 + 2z^2 + 2yz, \qquad Q_4 = 17x^2 + 17y^2 + 3z^2 - 2yz - 2xz + 16xy.$$

Let n be a positive square-free number such that $5 \nmid n$. Then,

$$\mathrm{L}(E_{-n}, 1) = \frac{\mathrm{L}(E_{-1}, 1)}{\sqrt{n}} \cdot c_n^2$$

where E_{-n} is the $-n$-th quadratic twist of E and

$$c_n = \sum_{i=1}^{4} \frac{(-1)^{i-1}}{2} \cdot \#\{(x, y, z) : Q_i(x, y, z) = n\}.$$

How do you prove the proposition?

Use **modularity** and apply **Waldspurger's Theorem**.

Let f_E be the newform associated to E, Waldspurger's Theorem relates the critical value of the L-function of the n-th quadratic twist of f_E to the n-th coefficient of a certain modular form of half-integral weight.

Problem: Waldspurger's recipes for these modular forms of half-integral weight are far from being explicit. In particular, they are expressed in the language of automorphic representations and Hecke characters.

Let k be positive integers with $k \geq 3$ odd. Let χ be an even Dirichlet character with modulus divisible by 4. Let χ_0 be the Dirichlet character

$$\chi_0(n) := \chi(n)\left(\frac{-1}{n}\right)^{(k-1)/2}.$$

Fix a newform f of level N in $S_{k-1}^{\mathrm{new}}(N, \chi^2)$, let ρ be the automorphic representation associated to f and ρ_p be the local component of ρ at p. Let S be the (finite) set of primes p such that ρ_p is not irreducible principal series.

If $p \notin S$, ρ_p is equivalent to $\pi(\mu_{1,p}, \mu_{2,p})$ where $\mu_{1,p}$ and $\mu_{2,p}$ are two continuous characters on $\mathbb{Q}_p$ such that $\mu_{1,p}\mu_{2,p} \neq |\cdot|^{\pm 1}$.

Let (H1) be the following hypothesis:

$$\text{(H1)} \qquad \text{For all } p \notin S,\ \mu_{1,p}(-1) = \mu_{2,p}(-1) = 1.$$

Corollary (Waldspurger)

Let $f \in S_{k-1}^{\mathrm{new}}(N, \chi^2)$ be a newform such that f satisfies (H1). Suppose $h(z) = \sum_{n=1}^{\infty} a_n q^n \in S_{k/2}(M, \chi, f)$ for some $M \geq 1$ such that $N \mid (M/2)$. Suppose that n_1, n_2 be positive square-free integers such that $n_1/n_2 \in {\mathbb{Q}_p}^2$ for all $p \mid N$. Then we have the following relation:

$$a_{n_1}^2 \mathrm{L}(f\chi_0^{-1}\chi_{n_2}, 1)\chi(n_2/n_1)n_2^{k/2-1} = a_{n_2}^2 \mathrm{L}(f\chi_0^{-1}\chi_{n_1}, 1)n_1^{k/2-1}.$$

$$S_{k/2}(M, \chi, f) = \{h \in S'_{k/2}(M, \chi) : T_{p^2}(h) = \lambda_p(f)h \text{ for almost all } p \nmid M\},$$

where $T_p(f) = \lambda_p(f)f$,

Theorem (Shimura)

$S'_{k/2}(M, \chi) = \bigoplus_f S_{k/2}(M, \chi, f)$ where f runs through all newforms $f \in S_{k-1}^{\mathrm{new}}(N, \chi^2)$ with $N \mid (M/2)$ and $\mathrm{cond}(\chi^2) \mid N$.

Using results similar in nature to the one in the previous slide (jointly with works of Mao, Baruch-Mao), we are able to compute central values of L-functions of twists of GL_2-type abelian varieties.

We do have exaples in dimensions 2, 3 and 5. The central difficulty is the computation of the relevant space of half integral weight modular forms and in particular the image of the Shimura map and its decomposition.

Example 1

Let $f \in S_2^{\mathrm{new}}(65, \chi_{\mathrm{triv}})$

$f = q + aq^2 + (-a+1)q^3 + q^4 - q^5 + (a-3)q^6 + 2q^7 - aq^8 + (-2a+1)q^9 + O(q^{10})$,

$a = \sqrt{3}$ (LMFDB label 65.2.1.b).
The space $S_{3/2}(260, \chi_{\mathrm{triv}}, f)$ is 2-dimensional and we compute the basis:

$$g_1 := q^5 - q^6 + (a+1)q^{15} - q^{20} + (a+1)q^{21} + q^{24} - aq^{26} + O(q^{30})$$
$$g_2 := q^{11} + (-a-2)q^{15} + (-a-2)q^{19} + (a+1)q^{20} + (-a-1)q^{24} + O(q^{30})$$

For each subset S_i of the set of prime divisors of 65, let

$$D_i := \{D \text{ fund. disc.} : \left(\tfrac{D}{l}\right) = -w_l \Leftrightarrow l \in S_i\}$$

where w_l denotes Atkin-Lehner eigenvalue ($w_5 = 1$ and $w_{13} = -1$).

The space of fundamental disc. is union of such D_i.

In particular for $S_1 = \phi$, we have
$D_1 = \{D \text{ fund. disc.} : \left(\tfrac{D}{5}\right) \neq -1, \left(\tfrac{D}{13}\right) \neq 1\}$.

For each D_i it is possible to give a concrete formula for $L(f, D, 1)$ for $D \in D_i$.
For D_1 the associated form is $g_2 = \sum_{n=0}^{\infty} c_n q^n$ and we have: for $D \in D_1$

- if $D > 0$, $L(f, D, 1) = 0$ and
- if $D < 0$,

$$L(f, D, 1) = \frac{(c_{|D|})^2}{|D|^{1/2} \cdot 2^{1-t_D}} \cdot L(f, -11, 1)(11)^{1/2}$$
$$= \frac{(c_{|D|})^2}{|D|^{1/2}} \cdot \frac{\pi}{2^{2-t_D}} \cdot \frac{< f, f >}{< g_2, g_2 >}.$$

where t_D is the number of primes dividing both 65 and D.

Example 2

Let f be the newform with LMFDB label 63.2.1.b

$$f = q + aq^2 + q^4 - 2aq^5 + q^7 - aq^8 - 6q^{10} + 2aq^{11} + O(q^{12}),$$

$a = \sqrt{3}$.
In this case the space $S_{3/2}(252, \chi_{\mathrm{triv}}, f)$ is 4-dimensional and we compute the basis:

$$g_1 := q + 1/2(a+1)q^7 - 2q^{16} + (a+1)q^{22} + (-2a-1)q^{25} + (a+1)q^{28} + O(q^{30})$$
$$g_2 := q^2 + (a-2)q^{11} + (-a+2)q^{14} + aq^{23} + (a-3)q^{29} + O(q^{30})$$
$$g_3 := q^4 + 1/2(-a-1)q^7 + aq^{16} - q^{28} + (-a-1)q^{43} + q^{64} + 2q^{67} + O(q^{70})$$
$$g_4 := q^8 + (a-2)q^{11} - aq^{23} + aq^{32} + (-a+1)q^{35} + (-a+1)q^{44} + (-a+2)q^{56} + O(q^{70})$$

For D fundamental disc. such that $D = -D' < 0$ and $\left(\frac{D'}{3}\right) = -1$,

$$L(f, -D', 1) = \kappa \cdot \frac{(c_{D'})^2}{{D'}^{1/2}} \cdot \pi \frac{< f, f >}{< g_4, g_4 >},$$

and for D fundamental disc. such that $D = -D' < 0$ and $\left(\frac{D'}{3}\right) = 1$,

$$L(f, -D', 1) = \kappa \cdot \frac{(c_{D'})^2}{{D'}^{1/2}} \cdot \pi \frac{< f, f >}{< g_3, g_3 >},$$

where $\kappa = 1/4$ if $(7, D) = 1$, else $\kappa = 1/2$.

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
Let A be a principally polarized abelian variety over $\mathbb{Q}$ of dimension g.

Let ℓ be a prime and $A[\ell]$ the ℓ-torsion subgroup:

$$A[\ell] := \{P \in A(\overline{\mathbb{Q}}) \mid [\ell]P = 0\} \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}.$$

$A[\ell]$ is a $2g$-dimensional $\mathbb{F}_\ell$-vector space, as well as a $G_{\mathbb{Q}}$-module.
The polarization induces a symplectic pairing, the mod ℓ **Weil pairing** on $A[\ell]$, that is Galois invariant. This gives a representation

$$\overline{\rho}_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}(A[\ell], \langle\ ,\ \rangle) \cong \mathrm{GSp}_{2g}(\mathbb{F}_\ell).$$

Theorem (Serre)

Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension g. Assume that $g = 2$, 6 or g is odd and, furthermore, assume that $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$. Then there exists a bound B_A such that for all primes $\ell > B_A$ the representation $\overline{\rho}_{A,\ell}$ is surjective.

The conclusion of the theorem is known to be false for general g (counterexample by Mumford for $g = 4$).

Open question

Is it possble to have a **uniform bound** B_g depending only on g?

Genus 2 & 3

Goal

Write an algorithm to determine the image of a mod ℓ Galois representation associated to the Jacobian of a curve of genus 2 or 3 over $\mathbb{Q}$ and collect data for B_2 and B_3.

Status:

- Genus 2: there is a method presented by Dieulefait but it is not effective: bounds for certifying the image are needed;
- Genus 3: algorithm from Anni-Lemos-Siksek for the semistable case.

Genus 2

Mitchell 1914: Classification of maximal proper subgroups G of $\mathrm{PSp}(4, \mathbb{F}_\ell)$ (ℓ odd)

Classification as groups of transformations of the projective space:

- a group having an invariant point and plane
- a group having an invariant parabolic congruence
- a group having an invariant hyperbolic congruence
- a group having an invariant elliptic congruence
- a group having an invariant quadric
- a group having an invariant twisted cubic
- a group G containing a normal elementary abelian subgroup E of order 16, with: $G/E \cong A_5$ or S_5
- a group G isomorphic to A_6, S_6 or A_7.

In each case it is possible to give criteria for the characteristic polynomials of images of Frobenius at unramified primes.

The algorithm uses modularity for two dimensional Jordan–Hölder factors.

Genus 3

Theorem (A., Lemos and Siksek)

Let A be a semistable principally polarized abelian variety of dimension $d \geq 1$ over $\mathbb{Q}$ and let $\ell \geq \max(5, d+2)$ be prime.

Suppose the image of $\overline{\rho}_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}_{2d}(\mathbb{F}_\ell)$ contains a transvection.

Then $\overline{\rho}_{A,\ell}$ is either reducible or surjective.

An "algorithm" for the genus 3 case

We now let $A/\mathbb{Q}$ be a **principally polarized abelian threefold**.

Assumptions

(A) A is semistable;

(B) $\ell \geq 5$;

(C) there is a prime q such that the special fibre of the Néron model for A at q has toric dimension 1.

(D) ℓ does not divide $\gcd(\{q \cdot \#\Phi_q : q \in S\})$, where S is the set of primes q satisfying (C) and Φ_q is the group of connected components of the special fibre of the Néron model of A at q.

Under these assumptions the image of $\overline{\rho}_{A,\ell}$ contains a transvection. Then $\overline{\rho}_{A,\ell}$ is either reducible or surjective.

“Algorithm”

Practical method which should, in most cases, produce a small integer B (depending on A) such that for $\ell \nmid B$, the representation $\overline{\rho}_{A,\ell}$ is irreducible and, hence, surjective.

2-dimensional Jordan–Hölder factors

Lemma

Suppose the $G_{\mathbb{Q}}$-module $A[\ell]$ does not have any 1-dimensional Jordan–Hölder factors, but has either a 2-dimensional or 4-dimensional irreducible subspace U. Then $A[\ell]$ has a 2-dimensional Jordan–Hölder factor W with determinant χ.

Let N be the conductor of A. Let W be a 2-dimensional Jordan–Hölder factor of $A[\ell]$ with determinant χ.
The representation

$$\tau : G_{\mathbb{Q}} \to \mathrm{GL}(W) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$$

is odd (as the determinant is χ), irreducible (as W is a Jordan–Hölder factor) and 2-dimensional.
By Serre's modularity conjecture (Khare, Wintenberger, Dieulefait, Kisin Theorem), this representation is **modular**:

$$\tau \cong \overline{\rho}_{f,\ell}$$

it is equivalent to the mod ℓ representation attached to a newform f of level $M \mid N$ and weight 2.

Let $H_{M,p}$ be the p-th Hecke polynomial for the new subspace $S_2^{\mathrm{new}}(M)$ of cusp forms of weight 2 and level M:

$$H_{M,p} = \prod (x - c_p(g)),$$

where g runs through the newforms of weight 2 and level M. Write

$$H'_{M,p}(x) = x^d H_{M,p}(x + p/x) \in \mathbb{Z}[x],$$

where $d = \deg(H_{M,p}) = \dim(S_2^{\mathrm{new}}(M))$.

Let

$$R(M,p) = \mathrm{Res}(P_p, H'_{M,p}) \in \mathbb{Z}\,,$$

where Res denotes resultant an P_p is the local Weil polynomial. If $R(M,p) \neq 0$ then we have a bound on ℓ.

The integers $R(M,p)$ can be very large. Given a non-empty set T of rational primes p of good reduction for A, let

$$R(M,T) = \gcd(\{p \cdot R(M,p) \ : \ p \in T\}).$$

In practice, we have found that for a suitable choice of T, the value $R(M,T)$ is fairly small.

Let

$$B_2'(T) = \mathrm{lcm}(R(M,T))$$

where M runs through the divisors of N such that $\dim(S_2^{\mathrm{new}}(M)) \neq 0$, and let

$$B_2(T) = \mathrm{lcm}(B_1(T), B_2'(T))$$

where $B_1(T)$ is given as before.

Lemma

Let T be a non-empty set of rational primes of good reduction for A, and suppose $\ell \nmid B_2(T)$. Then $A[\ell]$ does not have 1-dimensional Jordan–Hölder factors, and does not have irreducible 2- or 4-dimensional subspaces.

We fail to bound ℓ in the above lemma if $R(M, p) = 0$ for all primes p of good reduction.

Here are two situations where this can happen:

- $A \cong_{\mathbb{Q}} E \times A'$ where E is an elliptic curve and A' an abelian surface.
- A is of GL_2-type.

Note that in both these situations $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \neq \mathbb{Z}$.

We expect, but are unable to prove, that if $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$ then there will be primes p such that $R(M, p) \neq 0$.

Twists of GL_2-type abelian varieties and Galois images for genus 2

Samuele Anni

BSD Data @ Bristol,
University of Bristol, 28th March 2017

Thanks!