Integral Frobenius for Modular Abelian Surfaces

Tommaso Giorgio Centeleghe
University of Heidelberg

Annual Conference for the DFG priority project SPP 1489
Osnabrück, October 1st 2015

Let $N \geq 5$ be an integer, consider the group

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},$$

and let $X_0(N)$ be the corresponding modular curve over $\mathbb{Q}$.

$$X_0(N) = Y_0(N) \sqcup \{c_1, \ldots, c_h\},$$

where $Y_0(N)$ parametrizes pairs (E, H) given by an elliptic curve E and a cyclic subgroup $H \subset E$ of order N.

The complex points of $Y_0(N)$ are described by the quotient

$$Y_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash\mathcal{H},$$

where $\mathcal{H}$ is the complex upper half plane, and $\Gamma_0(N)$ acts on it via Möbius transformations.

These objects have remarkable arithmetic properties, they are a rich source of *Galois representations*.

The Jacobian of $X_0(N)$

There is a family of commuting Hecke operators

$$T_\ell : H^0(X_0(N), \Omega^1) \longrightarrow H^0(X_0(N), \Omega^1)$$

indexed by the primes $\ell \nmid N$.

If f is a common eigenvector, then the corresponding eigenvalues

$$\Phi_f = (a_\ell)_{\ell \nmid N}$$

are algebraic integers and generate a totally real number field K_f.

The Jacobian $J_0(N)$ of $X_0(N)$ admits an isogeny decomposition (defined over $\mathbb{Q}$)

$$J_0(N) \sim \prod_{f \in \mathcal{E}_N} A_f$$

into the product of $\mathbb{Q}$-simple abelian varieties A_f parametrized by the set $\mathcal{E}_N$ of common eigenvectors (up to scalar) for the operators T_ℓ.

The Hecke action induces a ring homomorphism

$$\iota_f : \mathbb{Z}[T_2, T_3, \ldots, T_\ell, \ldots]_{\ell \nmid N} \twoheadrightarrow O_f \subseteq \mathrm{End}_{\mathbb{Q}}(A_f)$$

where O_f is the order of K_f generated by the eigenvalues a_ℓ.
Moreover $[K_f : \mathbb{Q}] = \dim(A_f) \Rightarrow A_f$ is an Abelian Variety of GL_2-type.
To simplify the exposition, from now on assume:

1) O_f is the maximal order O_{K_f}
2) K_f has class number one

If ℓ is a prime number, the ℓ-adic Tate module $T_\ell(A_f)$ inherits two actions which commute with each other:

$$\text{Galois action} \quad \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \circlearrowright T_\ell(A_f)$$

$$\text{Hecke action} \quad O_f \otimes \mathbb{Z}_\ell \circlearrowright T_\ell(A_f)$$

Thanks to assumption 1), we have

$$O_f \otimes \mathbb{Z}_\ell = \prod_{\lambda | \ell} O_\lambda$$

where O_λ is the ring of integers of the local field $K_{f,\lambda}$.

The Integral Frobenius

The Hecke action induces a Galois-stable decomposition

$$T_\ell(A_f) = \prod_{\lambda|\ell} T_\lambda(A_f).$$

Since $T_\lambda(A_f)$ has rank two over O_λ, we have a Galois representation

$$\rho_{f,\lambda} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(O_\lambda)$$

that is *unramified* outside ℓN (Igusa).

Eichler-Shimura: if $p \nmid \ell N$, then $\rho_{f,\lambda}(\mathrm{Frob}_p)$ has characteristic polynomial

$$x^2 - a_p x + p.$$

This information determines the conjugacy class of $\rho_{f,\lambda}(\mathrm{Frob}_p)$ in $\mathrm{GL}_2(K_{f,\lambda})$.

What about the *integral* conjugacy class of $\rho_{f,\lambda}(\mathrm{Frob}_p)$ in $\mathrm{GL}_2(O_\lambda)$?

The aim of this project is to make it computable when A_f is a surface. The algorithm we want to construct largely builds upon already existing software.

If the prime ideal $\lambda \subset O_f$ divides the discriminant of $x^2 - a_p x + p$ then the action of Frob_p on the λ-torsion $A_f[\lambda]$ is given by

$$\begin{pmatrix} t & 1 \\ 0 & t \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix},$$

where t is the double root of $x^2 - a_p x + p \mod \lambda$.

We cannot decide a priori which of the two possibilities occur.

The integral Frobenius determines in which of the two situations we are.

Theorem (C.)

Let p be a prime $\nmid N$ and assume that conditions 1) and 2) hold. There exists a matrix

$$\sigma_p \in \mathrm{GL}_2(O_f[1/p])$$

which gives the integral conjugacy class of $\rho_{f,\lambda}(\mathrm{Frob}_p)$ for any prime λ of O_f not dividing p. Moreover, there is a procedure for constructing σ_p from a_p and the ring $\mathrm{End}_{\mathbb{F}_p}(A_{f,p})$, where $A_{f,p}$ denotes the reduction of A_f modulo p.

The reduction mod p map gives an inclusion $O_f \subseteq \mathrm{End}_{\mathbb{F}_p}(A_{f,p})$.
If $\pi_p : A_{f,p} \to A_{f,p}$ denotes the Frobenius isogeny, we then have

$$O_f[\pi_p] \subseteq \mathrm{End}_{\mathbb{F}_p}(A_{f,p}),$$

where $O_f[\pi_p]$ is a certain quadratic extension of O_f. Consider the saturation

$$S_p = (O_f[\pi_p] \otimes \mathbb{Q}) \cap \mathrm{End}_{\mathbb{F}_p}(A_{f,p})$$

of $O_f[\pi_p]$ in $\mathrm{End}_{\mathbb{F}_p}(A_{f,p})$. There is an ideal $b_p \subseteq O_f$ such that

$$O_f[\pi_p] = O_f + b_p S_p.$$

The matrix σ_p of the theorem can be constructed from a_p and b_p.

The strategy for computing with surfaces

Assume now that A_f is an abelian surface. The strategy for computing the matrix σ_p is composed of the following steps:

i) finding (if possible) a principal polarization on A_f defined over $\mathbb{Q}$;
ii) writing A_f as the Jacobian of a genus two curve C_f defined over $\mathbb{Q}$;
iii) computing the endomorphism ring of $\mathrm{Jac}(C_f \bmod p) \simeq A_{f,p}$;
iv) applying the theoretical result to construct σ_p.

The steps i) and ii) are based on an algorithm constructed by González-Jiménez, González and Guàrdia in *"Computations on Modular Jacobian Surfaces", Lecture Notes in Computer Science, 2369 (2002).*

The step iii) employs a software developed by Bisson in *"Computing endomorphism rings of abelian varieties of dimension two", Mathematics of Computation (to appear)*