Endomorphisms of Jacobians of Modular Curves and an Application

1. Introduction

Let Γ be a congruence group with $\Gamma_1(N) \leq \Gamma \leq \Gamma_0(N)$,

$X_\Gamma = \Gamma\backslash\mathfrak{H}^*$ be the associated modular curve,

$X = X_{\Gamma,\mathbb{Q}}$ its canonical model over $\mathbb{Q}$,

$J = J_X$, its Jacobian variety of dimension g_X,

$\mathbb{E} = \mathrm{End}^0_{\mathbb{Q}}(J) = \mathrm{End}_{\mathbb{Q}}(J) \otimes \mathbb{Q}$, its endomorphism algebra.

Problem 1: Determine $\mathbb{E}$, i.e. find explicit generators for $\mathbb{E}$.

Recall: The Hecke operators (correspondences) T_n on X give rise to a commutative subalgebra called the Hecke algebra,

$$\mathbb{T} \;=\; \langle T_n : n \geq 1 \rangle_{\mathbb{Q}} \;\subset\; \mathbb{E}.$$

It contains the (semi-simple) subalgebra

$$\mathbb{T}' \;=\; \langle T_n : n \geq 1, (n, N) = 1 \rangle_{\mathbb{Q}} \;\subset\; \mathbb{T} \;\subset\; \mathbb{E}.$$

Then we have

$$\begin{aligned} \dim_{\mathbb{Q}} \mathbb{T} \;&=\; \dim J, && \text{(Shimura)} \\ \dim_{\mathbb{Q}} \mathbb{T}' \;&=\; \#\mathcal{N}(\Gamma), && \text{(Atkin-Lehner)} \end{aligned}$$

where $\mathcal{N}(\Gamma) \subset S_2(\Gamma)$ denotes the set of normalized newforms of weight 2 of all levels, i.e. if $f \in \mathcal{N}(\Gamma)$, then f is a normalized newform of level $N_f | N$.

Note: If $N = p$ is prime, then by Ribet we have that $\mathbb{T}' = \mathbb{T} = \mathbb{E}$, but in general these three algebras are different.

Reason: For each pair (M, d) with $Md|N$, there is a degeneracy morphism (Mazur)

$$B_{M,d} : X \to X_M,$$

where X_M is the corresponding curve of level M, and these give rise to new endomorphisms

$$D_{M,d} := B^*_{M,1} \circ (B_{M,d})_*, \ {}^tD_{M,d} := B^*_{M,d} \circ (B_{M,1})_* \in \mathrm{End}(J_X).$$

Theorem 1: $\mathbb{E} = \langle \mathbb{T}', \{D_{M,d}, {}^tD_{M,d} : Md|N\}\rangle_{\mathbb{Q}}$.

Corollary: $Z(\mathbb{E}) = \mathbb{T}'$.

Thus: $\mathbb{T}'$ has an intrinsic interpretation.

Remark: The above results also apply to other modular curves such as the principal modular curve

$$X(N) = X_{\Gamma(N),\mathbb{Q}},$$

where $\Gamma(N) = \mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$.

[Indeed, $\Gamma(N)$ is conjugate to a group $\Gamma[N]$ with

$$\Gamma_1(N^2) \le \Gamma[N] \le \Gamma_0(N),$$

and we have $\mathbb{Q}$-isomorphisms

$$X(N) \simeq X_{\Gamma[N],\mathbb{Q}} \quad \text{and} \quad J(N) \simeq J_{X_{\Gamma[N],\mathbb{Q}}}$$

which are compatible which the action of the Hecke algebras.]

Problem 2: For each $\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times$, determine $\dim_{\mathbb{Q}} \mathbb{T}_\varepsilon$, where

$$\mathbb{T}_\varepsilon = \sum_{a^2 n \equiv \varepsilon (N)} \mathbb{Q} T_{a,n}.$$

Here $T_{a,n} = T(a,a)T_n$, where $T(a,a) = \langle a \rangle$ denotes the diamond operator. Note that by definition we have

$$\sum_\varepsilon \mathbb{T}_\varepsilon = \mathbb{T}'.$$

Theorem 2: If $X = X(N)$, then

$$\mathbb{T}' = \bigoplus_\varepsilon \mathbb{T}_\varepsilon.$$

Remarks: 1) Thus, we might expect that

$$\dim \mathbb{T}_\varepsilon \stackrel{?}{=} \frac{1}{\phi(N)} \dim \mathbb{T}' = \frac{1}{\phi(N)} \# \mathcal{N}(\Gamma(N)).$$

This is almost true, but the presence of CM elliptic curves in $J(N)$ makes the actual result a bit more complicated. (See Theorem 5 below.)

2) As we shall see, $\mathbb{T}_\varepsilon$ also has an intrinsic interpretation in terms of the algebra $\mathbb{M}$ of all modular correspondences.

3) The group $\mathbb{T}_\varepsilon$ is closely related to the Neron-Severi group $NS(Z_{N,\varepsilon})$ of the modular diagonal quotient surface (MDQS)

$$Z_{N,\varepsilon} = (X(N) \times X(N))/\Delta_\varepsilon,$$

where $\Delta_\varepsilon \leq G_N \times G_N$ is a certain (twisted) diagonal subgroup of the group $G_N = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\pm 1$.

2. Ingredients of Theorem 1

(a) The Degeneracy Algebra:

Recall: The algebra $\mathbb{E}$ acts faithfully on the $\mathbb{Q}$-vector spaces

$$H^0(J,\Omega^1_J) \simeq H^0(X,\Omega^1_X) \simeq S_{\mathbb{Q}} := S_2(\Gamma,\mathbb{Q}),$$

where $S_{\mathbb{Q}} = S_2(\Gamma,\mathbb{Q})$ = space of all weight 2 cusp forms on Γ with $\mathbb{Q}$-rational Fourier expansions. Thus:

$$\mathbb{E}_{\mathbb{C}} = \mathbb{E} \otimes \mathbb{C} \quad \text{acts faithfully on} \quad S := S_2(\Gamma) = S_{\mathbb{Q}} \otimes \mathbb{C}.$$

Basic Fact (Atkin-Lehner Theory): The isotypic decomposition of S as a $\mathbb{T}'_{\mathbb{C}}$-module is given by

$$S = \bigoplus_{f \in \mathcal{N}(\Gamma)} S_f, \quad \text{where } S_f = \sum_{d|(N/N_f)} \mathbb{C} f|\beta_d.$$

Here $\beta_d = \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)$, so $f|\beta_d(z) = f(dz)$ and hence

$$n_f := \dim S_f = \sigma_0(N/N_f).$$

Definition: The degeneracy algebra is

$$\mathbb{D} = \langle \mathbb{T}', \{D_{M,d}, {}^tD_{M,d} : Md|N\}\rangle \subset \mathbb{E}.$$

Theorem 3: Each S_f is an irreducible $\mathbb{D}_{\mathbb{C}}$-module, and every irreducible $\mathbb{D}_{\mathbb{C}}$-module is isomorphic to a unique S_f. Thus $Z(\mathbb{D}_{\mathbb{C}}) = \mathbb{T}'_{\mathbb{C}}$ and $\mathbb{D}_{\mathbb{C}} = C_S(\mathbb{T}'_{\mathbb{C}})$, the centralizer of $\mathbb{T}'$ in $\mathrm{End}_{\mathbb{C}}(S)$. In particular, S has multiplicity 1 as a $\mathbb{D}_{\mathbb{C}}$-module.

Remark: There is an analogous statement for the space $S_k(\Gamma)$ of cusp forms of arbitrary weight k.

(b) Ribet's work:

Notation: $K_f := \mathbb{Q}(\{a_n(f)\})$, if $f = \sum a_n(f)q^n \in \mathcal{N}(\Gamma)$.

Theorem 4 (Ribet)

$$\mathbb{E} := \mathrm{End}^0_{\mathbb{Q}}(J) \simeq \prod_{f \in \mathcal{N}(\Gamma)/G_{\mathbb{Q}}} M_{n_f}(K_f).$$

Remark: Although the above result is not mentioned explicitly in Ribet's work, it can be deduced from his results (with some difficulty).

Proof of Theorem 1: Since $\mathbb{D} \subset \mathbb{E}$, we have $Z(\mathbb{E}) \subset C_{S_{\mathbb{Q}}}(\mathbb{E}) \subset C_{S_{\mathbb{Q}}}(\mathbb{D}) = \mathbb{T}'$ (Theorem 3). But by Theorem 4 we have $\dim \mathbb{Z}(\mathbb{E}) = \#\mathcal{N}(\Gamma) = \dim \mathbb{T}'$, and so $Z(\mathbb{E}) = C_{S_{\mathbb{Q}}}(\mathbb{E}) = \mathbb{T}'$. Thus $\mathbb{D} = \mathbb{E}$ by the double centralizer theorem.

Example: $X = X(p)$, p a prime.

Let $\eta : X(p) \to X^1(p)$ and $\eta' : X(p) \to X_1(p)$ be the usual covering maps, and put $\tau = \eta^* \circ \eta_*$, $\tau' = (\eta')^* \circ \eta'_*$. Then Theorem 1 (+ a refinement) gives

$$\mathbb{E} = \langle \mathbb{T}', \tau, T_p, {}^tT_p \rangle_{\mathbb{Q}} = \langle \mathbb{T}', \tau, \tau' \rangle_{\mathbb{Q}}. \tag{1}$$

[Indeed, $\tau = D_{p,1}$, $T_p = {}^tD_{p,p}$, and ${}^tT_p = D_{p,p}$.] Moreover,

$$\begin{aligned} \dim \mathbb{T}' &= g(p) - g_1(p) \\ \dim \mathbb{T} &= g(p) \\ \dim \mathbb{E} &= g(p) + 2g_1(p) \end{aligned}$$

where $g(p) = g_{X(p)}$ and $g_1(p) = g_{X_1(p)}$.

3. CM-forms and the Dimension of $\mathbb{T}_\varepsilon$

Notation: Let $f, g \in \mathcal{N}(\Gamma)$. If χ is a Dirichlet character with conductor $\mathrm{cond}(\chi)|N$, then we write

$$f_\chi \sim g \;\Leftrightarrow\; \chi(n)a_n(f) = a_n(g),\ \forall n \geq 1, (n, N) = 1.$$

Definition: $f \in \mathcal{N}(\Gamma)$ is called a CM-form if $f_\theta \sim f$, for some Dirichlet character $\theta \neq 1$.

Let $\mathcal{N}(\Gamma)^{CM} \subset \mathcal{N}(\Gamma)$ denote set of all CM-forms on Γ.

Remarks: 1) If $f_\theta \sim f$, $\theta \neq 1$, then $\theta^2 = 1$ and $\theta = \theta_f$ is uniquely determined by f.

2) $\#\mathcal{N}(\Gamma)^{CM}$ can be calculated explicitly in terms of class numbers of imaginary quadratic fields. (Shimura)

3) $f \in \mathcal{N}(\Gamma)^{CM} \;\Leftrightarrow\; A_f \otimes \mathbb{C} \sim E^m$, where E is a CM elliptic curve. (Here A_f = abelian quotient of J.) (Shimura, Ribet)

Notation: If $f, g \in \mathcal{N}(\Gamma)$, then we write

$$f \approx g \quad \Leftrightarrow \quad f_\chi \sim g, \text{ for some } \chi \text{ with } \mathrm{cond}(\chi)|N.$$

Moreover, for $\varepsilon \in (\mathbb{Z}/N\mathbb{Z})^\times$ put

$$\mathcal{N}_\varepsilon(\Gamma) \;=\; \{f \in \mathcal{N}(\Gamma) : f \notin \mathcal{N}(\Gamma)^{CM} \text{ or } f \in \mathcal{N}(\Gamma)^{CM} \text{ and } \theta_f(\varepsilon) = 1\}.$$

Theorem 5: We have

$$\dim \mathbb{T}_\varepsilon \;=\; \#\mathcal{N}_\varepsilon(\Gamma)/\approx.$$

4. The Algebra $\mathbb{M}$ of Modular Correspondences

Fact (Klein, Gierster, Hurwitz, ...) Each $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ defines a modular correspondence

$$T_\Gamma(\alpha) \subset X_\Gamma \times X_\Gamma$$

and hence induces an endomorphism $f_\alpha \in \mathrm{End}_{\mathbb{C}}(X_\Gamma)$. We call the $\mathbb{Q}$-algebra $\mathbb{M} \subset \mathrm{End}^0_{\mathbb{C}}(X_\Gamma)$ generated by the f_α's the algebra of modular correspondences.

Remarks: 1) The Hecke correspondence T_p (p any prime) is given by $T_p = f_{\alpha_p}$, where $\alpha_p = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$.

2) It follows from the example below that

$$\mathbb{M} \subset \mathbb{E}' := \mathrm{End}^0_{K_N}(X_\Gamma), \quad \text{where } K_N = \mathbb{Q}(\zeta_N).$$

Thus, the group $(\mathbb{Z}/N\mathbb{Z})^\times \simeq \mathrm{Gal}(K_N/\mathbb{Q})$ induces a natural Galois action on $\mathbb{E}'$ and on $\mathbb{M}$ via

$$\tau_a(f) = \tilde{\tau}_a \circ f \circ \tilde{\tau}_a^{-1}, \quad a \in (\mathbb{Z}/N\mathbb{Z})^\times,$$

where $\tilde{\tau}_a$ is the lift of $\tau_a \in \mathrm{Gal}(K_N/\mathbb{Q})$ to $J \otimes K_N$.

Example: Let $\Gamma = \Gamma(N)$. Then

$$(2) \qquad \mathbb{M} = \langle \mathbb{T}, G_N \rangle_{\mathbb{Q}}, \quad \text{where } G_N = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\},$$

viewed as acting as a group of automorphims on $X(N)$ and hence on $J(N)$. Moreover, the Galois action on $\mathbb{M}$ is given by

$$\begin{aligned} \tau_a(T) &= T, && \text{if } T \in \mathbb{T}, \\ \tau_a(g) &= \overline{\beta}_a^{-1} g \overline{\beta}_a, && \text{if } g \in G_N, \end{aligned}$$

where $\overline{\beta}_a = \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Observation: In the above situation ($\Gamma = \Gamma(N)$) we have

(3) $$Tg = \tau_\varepsilon(g)T, \quad \text{for all } T \in \mathbb{T}_\varepsilon, g \in G_N.$$

Theorem 6: If $\Gamma = \Gamma(p)$, where p is prime, then

$$\mathbb{M} = \langle \mathbb{T}, G_p \rangle_{\mathbb{Q}} \stackrel{!}{=} \langle \mathbb{T}', G_p \rangle_{\mathbb{Q}}.$$

Proof. Combine equations (1) and (2) of the two examples.

Notation: Let

$$\rho : \mathbb{M}_{\mathbb{C}} := \mathbb{M} \otimes \mathbb{C} \longrightarrow \mathrm{End}_{\mathbb{C}}(S)^{op}$$

be the representation afforded by $S = S_2(\Gamma)$ (viewed as a right $\mathbb{M}_{\mathbb{C}}$-module), and put

$$\begin{aligned}&\mathrm{End}_{\mathbb{M},\varepsilon}(S)\\ &\quad = \{f \in \mathrm{End}(S) : \rho(x) \circ f = f \circ \rho(\tau_\varepsilon(x)), \forall x \in \mathbb{M}\}.\end{aligned}$$

Theorem 7: $\rho(\mathbb{T}_\varepsilon \otimes \mathbb{C}) = \mathrm{End}_{\mathbb{M},\varepsilon}(S)$.

Remark: This gives an intrinsic interpretation of the space $\mathbb{T}_\varepsilon$.

5. Application to $NS(Z_{N,\varepsilon})$

Definition: The modular diagonal quotient surface of type (N,ε) is the quotient surface

$$Z_{N,\varepsilon/\mathbb{C}} = (X(N)_{/\mathbb{C}} \times X(N)_{/\mathbb{C}})/\Delta_{N,\varepsilon}$$

where $\Delta_{N,\varepsilon} = \{(g, \tau_\varepsilon(g)) : g \in \Gamma_N\} \leq G_N \times G_N$.

Note: $Z_{N,\varepsilon/\mathbb{C}}$ has a canonical model $Z_{N,\varepsilon}$ over $\mathbb{Q}$, even though the automorphism group is only defined over $K_N = \mathbb{Q}(\zeta_N)$. In addition, the quotient map

$$\Psi : X(N) \times X(N) \ \to \ Z_{N,\varepsilon}$$

is defined over $\mathbb{Q}$.

Remark: The MDQS $Z_{N,\varepsilon}$ has a natural modular interpretation: the open subset

$$Z'_{N,\varepsilon} \ = \ Z_{N,\varepsilon} \setminus \cup\{\text{cuspidal divisors}\}$$

classifies isomorphisms (of determinant ε) of mod N Galois representations of elliptic curves.

Note: $\varepsilon = -1 \rightsquigarrow$ Hurwitz spaces and Humbert surfaces.

Key Open Question: If $N = p > 19$, is every curve $C \subset Z_{N,\varepsilon}$ of genus ≤ 1 a modular curve, i.e. of the form $C = T_{a,n}$?

- via Lang's Conjecture, this would have interesting Diophantine consequences.

Simpler Question: Up to (algebraic) equivalence, are all the ($\mathbb{Q}$-rational) curves/divisors on $Z_{N,\varepsilon}$ modular?

Notation: Let $NS^0(Z_{N,\varepsilon}) = NS(Z_{N,\varepsilon}) \otimes \mathbb{Q}$, where $NS(Z_{N,\varepsilon})$ denotes the Neron-Severi group of $Z_{N,\varepsilon}$, i.e.

$$NS(Z_{N,\varepsilon}) = \mathrm{Div}(Z_{N,\varepsilon})/(\text{algebraic equivalence}).$$

In addition, we write

$$\overline{NS}^0(Z_{N,\varepsilon}) = NS^0(Z_{N,\varepsilon})/\langle cl(\Psi(P \times X)), cl(\Psi(X \times P))\rangle,$$

where $X = X(N)$ and $P \in X(\mathbb{Q})$, and, as above, Ψ denotes the quotient map $\Psi : X \times X \to Z_{N,\varepsilon}$.

Proposition: We have a canonical identification

$$\overline{NS}^0(Z_{N,\varepsilon}) \simeq \mathrm{End}^0_{G_{N,\varepsilon}}(J(N)),$$

where

$$\mathrm{End}_{G_{N,\varepsilon}}(J(N)) = \{f \in \mathrm{End}^0_{\mathbb{Q}}(J(N)) : gf = f\tau_\varepsilon(g), \forall g \in G_N\}.$$

Corollary: For any (N, ε) we have a natural embedding

$$\mathbb{T}_{\varepsilon^{-1}} \subset \overline{NS}^0(Z_{N,\varepsilon})$$

Theorem 8: If $N = p$ is prime, then

$$\overline{NS}^0(Z_{p,\varepsilon}) \simeq \mathbb{T}_{\varepsilon^{-1}}.$$

Proof (Sketch) Use Theorem 6 and Theorem 7.

Conclusion: Thus, up to algebraic equivalence, all divisors in $Z_{p,\varepsilon}$ are modular, i.e. they are $\mathbb{Q}$-linear combinations of the divisors $\Psi(T_{a,n})$ with $a^2n \equiv \varepsilon(N)$, together with the two curves $\Psi(P \times X)$ and $\Psi(X \times P)$.

Corollary: We have

$$\operatorname{rk} NS(Z_{p,\varepsilon}) = 2 + \frac{1}{24}(p-1)(p-5) + \frac{1}{2}\left(\frac{\varepsilon}{p}\right) h(p),$$

where $\left(\frac{\varepsilon}{p}\right)$ denotes the Legendre symbol and

$$h(p) = \begin{cases} h(\mathbb{Q}(\sqrt{-p}) & \text{if } p \equiv 3(4) \\ 0 & \text{if } p \equiv 1(4) \end{cases}$$

Proof. Use Theorem 5 (and Theorem 8).