On Shimura Curve Invariants

David R. Kohel
Mathematical Sciences Research Institute
and
University of Sydney
Computational Algebra Group

Shimura Curve Invariants

1. Shimura Curve Definition.
2. Quaternion Method of Graphs.
3. Character Groups of $J_0^D(m)$.
4. Examples and Computations.
5. Further Directions and Vistas.

Terminology

Definition. A *quaternion algebra* $\mathbf{H}$ over a field K is a central simple K-algebra of dimension 4. An *Eichler order* $\mathcal{O}$ of $\mathbf{H}$ is a $\mathbf{Z}_K$-order of $\mathbf{H}$ which is the intersection of two maximal $\mathbf{Z}_K$-orders.

Example. $\mathbf{H} = \mathbf{M}_2(\mathbf{Q})$ is a quaternion algebra over $\mathbf{Q}$ and $\mathcal{O} = \mathbf{M}_r(\mathbf{Z})$ is a maximal order of $\mathbf{H}$.

Definition. Let $\mathbf{H}$ be a quaternion algebra over K. A place v of K is said to *split* (respectively *ramify*) in $\mathbf{H}$ if the quaternion algebra $\mathbf{H} \otimes_K K_v$ is isomorphic to $\mathbf{M}_2(K_v)$ (respectively to a division algebra over K_v).

Shimura Curve Definition

Let $\mathcal{O}$ be an order in an indefinite quaternion algebra $\mathbf{H}$ over $\mathbf{Q}$, and fix an isomorphism $\mathbf{H} \otimes_{\mathbf{Q}} \mathbf{R} \cong \mathbf{M}_2(\mathbf{R})$. Under this isomorphism, the group

$$U^1(\mathcal{O}) = \{x \in O^* \mid \mathrm{N}(x) = 1\} \subset \mathrm{SL}_2(\mathbf{R})$$

acts discretely on the upper half plane $\mathfrak{H}$. If $\mathbf{H}$ is a division algebra, then the quotient $U^1(O)\backslash\mathfrak{H}$ is a compact Riemann surface.

If the discriminant of $\mathbf{H}$ is D and $\mathcal{O}$ is an Eichler order of index m in a maximal order, then the resulting algebraic curve is the *Shimura curve* $X_0^D(m)$.

N.B. The curve $X_0^D(m)$ is a moduli space for abelian surfaces $A/\mathbf{C}$ with an embedding $\mathcal{O} \to \mathrm{End}(A)$, where $\mathcal{O}$ is an Eichler order of index m in a maximal order in the indefinite $\mathbf{Q}$-quaternion algebra of discriminant D.

Example. Consider the indefinite quaternion algebra over $\mathbf{Q}$ defined by

$$\mathbf{H} = \frac{\mathbf{Q}\langle i, j\rangle}{(i^2 - 2, j^2 + 13, ij + ji)}.$$

We can embed $\mathbf{H}$ in the matrix algebra $\mathbf{M}_2(\mathbf{R})$ by means of the homomorphism:

$$i \longmapsto \begin{pmatrix} \sqrt{2} & 0 \\ 0 & -\sqrt{2} \end{pmatrix} \quad j \longmapsto \begin{pmatrix} 0 & -1 \\ 13 & 0 \end{pmatrix}$$

The algebra $\mathbf{H}$ is ramified at 2 and 13. If we set $t = (1+i+j)/2$ and $u = (1 + j + k)/2$, then $\{1, i, t, u\}$ is a basis for a maximal order $\mathcal{O}$ of $\mathbf{H}$. We can easily write down units of $\mathcal{O}$,

$$1 + i,\ 5 + k = 5 + i - 2t + 2u,\ 1 + u,\ 8 + 3(t - u),$$

each of which is a fundamental unit of the corresponding real quadratic subring of $\mathcal{O}$ which it generates.

Question. How do we compute a fundamental domain, or generators and relations for $U^1(\mathcal{O})$? *N.B. The approach to Shimura curve invariants taken here bypasses the action on $\mathfrak{H}$.*

Quaternion Method of Graphs

Let R be an Eichler order in a definite quaternion algebra $\mathbf{H}$ ramified at Dp and of index m in a maximal order of $\mathbf{H}$. Let $I_1, \dots, I_h$ be representatives for the left ideal classes of R, and define

$$\begin{aligned} \mathcal{X}(Dp, m) &= \langle\, [I_i] - [I_{i+1}] \mid 1 \le i < h \,\rangle \\ &\subset M(Dp, m) = \textstyle\bigoplus_i \mathbf{Z}[I_i]. \end{aligned}$$

For a prime ℓ we define I_j to be ℓ-isogenous to I_i if there exists a homomorphism $\varphi : I_i \to I_j$ such that $I_j/\varphi(I_i) \cong \mathbf{Z}/\ell\mathbf{Z} \times \mathbf{Z}/\ell\mathbf{Z}$.

We define a collection of commuting *Hecke operators* T_ℓ as the linear operator defined on ideals classes by

$$T_\ell([I]) = \sum_{\varphi: I \to J} [J],$$

where the sum is over ℓ-isogenies of I, up to isomorphism of J, and define an inner product by $\langle [I], [J] \rangle = |\mathrm{Isom}(I, J)|/2$.

N.B. This construction generalizes the method of graphs of Mestre and Oesterlé, defined in terms of supersingular elliptic curves.

Character Groups of $J_0^D(m)$

Let A be an abelian variety A over $\mathbf{Q}$ with semistable reduction at a prime p. Let $\mathcal{T}/\mathbf{F}_p$ be the toric part of the reduction of a Néron model for A, and set

$$\mathcal{X}(A,p) = \mathrm{Hom}_{\overline{\mathbf{F}}_p}(\mathcal{T}, \mathbf{G}_m).$$

There exists a canonical nondegenerate monodromy pairing

$$\langle\ ,\ \rangle : \mathcal{X}(A,p) \times \mathcal{X}(A^\vee,p) \longrightarrow \mathbf{Z},$$

where $A^\vee$ is the dual of A. If A is principally polarized ($A \cong A^\vee$), and in particular if A is a Jacobian, then we obtain a positive definite inner product on $\mathcal{X}(A,p)$.

Theorem 1 *With the notation as above, there exists a canonical isomorphism $\mathcal{X}(Dp, m) \cong \mathcal{X}(J_0^D(mp), p)$, which is compatible with the action of Hecke operators and the monodromy pairing.*

Corollary 2 *We can effectively compute $\mathcal{X}(J_0^D(m), p)$ for $p|m$.*

Theorem 3 *Let D be a product of an even number of primes, and let p and q be distinct primes coprime to D. Then there exists a canonical exact sequence*

$$0 \longrightarrow \mathcal{X}(A', p) \xrightarrow{\iota} \mathcal{X}(A, q) \longrightarrow \mathcal{X}(A'', q) \times \mathcal{X}(A'', q) \longrightarrow 0$$

where $A' = J_0^{Dpq}(m)$, $A = J_0^D(mpq)$, and $A'' = J_0^D(mq)$. The sequence is compatible with the Hecke operators T_ℓ for all primes ℓ relatively prime to $Dpqm$, and the map ι defines an isometry with its image, with respect to the monodromy pairings on $\mathcal{X}(A', p)$ and $\mathcal{X}(A, q)$.

Corollary 4 *We can effectively compute $\mathcal{X}(J_0^D(m), p)$ for $p|D$.*

Notation. For an abelian variety $A/\mathbf{Q}$ we denote the component group of a Néron model at p by $\Phi(A, p)$.

Theorem 5 *Let $A/\mathbf{Q}$ be an abelian variety with semistable reduction at p with a principle polarization $\xi : A \to A^\vee$. There exists a natural exact sequence*

$$0 \longrightarrow \mathcal{X}(A, p) \longrightarrow \mathrm{Hom}(\mathcal{X}(A, p), \mathbf{Z}) \longrightarrow \Phi(A, p) \longrightarrow 0,$$

taking $x \in \mathcal{X}(A, p)$ to $\langle -, \xi(x) \rangle$.

Corollary 6 *We can effectively compute $\Phi(J_0^D(m), p)$.*

Examples and Computations

1. L-functions of simple factors $J_0^D(m) \to A$.
2. Homomorphisms $\mathcal{X}(J_0^D(m), p) \to S_2(\Gamma_0(Dm))$.
3. Comparison of isogeny factors of $J_0^D(m)$ and $J_0^1(Dm)$.
4. Component groups $\Phi(A, p)$ and modular degrees m_A of optimal quotients.

Example. We have canonically that $\mathcal{X}(13, 2) \cong \mathcal{X}(J_0(26), 13)$, and that $\mathcal{X}(J_0^{26}(1), 2)$ is the kernel of the homomorphism

$$\mathcal{X}(J_0(26), 13) \to \mathcal{X}(J_0(13), 13) \times \mathcal{X}(J_0(13), 13) = 0.$$

Therefore also $\mathcal{X}(13, 2) \cong \mathcal{X}(J_0^{26}(1), 2)$.

```
> M := BrandtModule(2,13);
> M;
Brandt module of level (2,13), dimension 3, and degree 3 over Integer..
> [ qExpansionBasis(N,20) : N in Decomposition(M,13) ];
[
[
7 + 12*q + 12*q^2 + 48*q^3 + 12*q^4 + 72*q^5 + 48*q^6 + 96*q^7
 + 12*q^8 + 156*q^9 + 72*q^10 + 144*q^11 + 48*q^12 + 324*q^13
 + 96*q^14 + 288*q^15 + 12*q^16 + 216*q^17 + 156*q^18 + 240*q^19
 + 72*q^20 + O(q^21)
],
[
q - q^2 + q^3 + q^4 - 3*q^5 - q^6 - q^7 - q^8 - 2*q^9 + 3*q^10
 + 6*q^11 + q^12 + q^13 + q^14 - 3*q^15 + q^16 - 3*q^17 + 2*q^18
 + 2*q^19 - 3*q^20 + O(q^21)
],
[
q + q^2 - 3*q^3 + q^4 - q^5 - 3*q^6 + q^7 + q^8 + 6*q^9 - q^10
 - 2*q^11 - 3*q^12 - q^13 + q^14 + 3*q^15 + q^16 - 3*q^17 + 6*q^18
 + 6*q^19 - q^20 + O(q^21)
]
]
```

Component groups...

Notation. Let p be a fixed prime. We denote by $\mathcal{X} = \mathcal{X}_J$ the character group of a Jacobian $J/\mathbf{Q}$ at p, and associated to any $A/\mathbf{Q}$ we define Φ_A to be the component group at p. Suppose that $\mathcal{L}$ be a primitive, Hecke irreducible sublattice of $\mathcal{X}$ and hereafter let A be the associated optimal quotient of J.

Define $\Phi_{\mathcal{L}} = \mathrm{Hom}(\mathcal{L}, \mathbf{Z})/\mathcal{L}$ and let α be the map of the commuting diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{X}_J \arrow[r] \arrow[dr, "\alpha"] & \mathrm{Hom}(\mathcal{X}, \mathbf{Z}) \arrow[r] \arrow[d] & \Phi_J \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathcal{L} \arrow[r] \arrow[u, hook] & \mathrm{Hom}(\mathcal{L}, \mathbf{Z}) \arrow[r] & \Phi_{\mathcal{L}} \arrow[r] & 0
\end{tikzcd}$$

from which we define

$$\Psi_{\mathcal{X},\mathcal{L}} = \alpha(\mathcal{X})/\alpha(\mathcal{L})$$
$$\Phi_{\mathcal{X},\mathcal{L}} = \mathrm{Hom}(\mathcal{L}, \mathbf{Z})/\alpha(\mathcal{X}) = \mathrm{coker}(\alpha).$$

Therefore we have an exact sequence of abelian groups

$$0 \to \Psi_{\mathcal{X},\mathcal{L}} \to \Phi_{\mathcal{L}} \to \Phi_{\mathcal{X},\mathcal{L}} \to 0$$

each of whose terms we can effectively compute.

...and modular degrees

For any optimal quotient $\pi : J \to A$, we define the *modular degree* $m_A = \sqrt{\deg(\phi_A)}$, where ϕ_A is defined by the following commutative diagram

$$\begin{tikzcd} A^\vee \arrow[r, "\pi^*"] \arrow[dr, "\phi_A"'] & J \arrow[d, "\pi"] \\ & A. \end{tikzcd}$$

and define the *congruence modulus* $m_{\mathcal{X},\mathcal{L}} = |\Psi_{\mathcal{X},\mathcal{L}}|$.

Theorem 7 (Stein) *The component group Φ_A at p and the modular degree m_A are related to the above quantities by*

$$\Phi_{\mathcal{X},\mathcal{L}} \subseteq \Phi_A, \quad m_{\mathcal{X},\mathcal{L}} \mid m_A,$$

and

$$|\Phi_A| = \frac{m_A}{m_{\mathcal{X},\mathcal{L}}} |\Phi_{\mathcal{X},\mathcal{L}}|.$$

Experimental Results

$J_0^D(m)$	A	g	p	$\|\Phi_{\mathcal{X},\mathcal{L}}\|$	$m_{\mathcal{X},\mathcal{L}}$
$J_0^{26}(1)$	J	2	2	21	1
	$A1$	1	”	1	2
	$A2$	1	”	3	2
$J_0^{26}(1)$	J	2	13	21	1
	$A1$	1	”	7	2
	$A2$	1	”	3	2
$J_0^{26}(31)$	J	29	31	30	1
		1	”	1	16
		1	”	1	16
		1	”	1	8
		1	”	3	56
		1	”	5	104
		1	”	1	8
		2	”	1	64
		2	”	1	64
		3	”	1	5824
		5	”	1	4096
		5	”	1	4096
		6	”	2	4096

Further Directions and Vistas

1. Higher weight Brandt modules $M_k(Dp, m) \supset \mathcal{X}_k(Dp, m)$.
2. Models for Shimura curves?

   Does there exist a natural ring structure
   $$\bigoplus_{r=0}^{\infty} \mathcal{X}_{2r}(Dp, m) \to \bigoplus_{r=0}^{\infty} S_{2r}(\Gamma(Dpm)),$$
   giving $X_0^D(m)$ by projective embedding?

   Analytic coverings
   $$U^1(\mathcal{O})\backslash\mathfrak{H} \cong X_0^D(m),$$
   or analysis of ramification (see Elkies in ANTS III).