Explicitly Computing With Modular Abelian Varieties

William Stein
Harvard University

June 18, 2003
Computational Arithmetic Geometry Workshop in Sydney

Overview of Talk

1. Modular Abelian Varieties

2. Computerizing Modular Abelian Varieties

3. Computing Endomorphism Rings of Modular Abelian Varieties of Level N

Modular Abelian Varieties

Abel

Abelian variety: A complete group variety

Examples:

1. Elliptic curves, e.g., $y^2 = x^3 + ax + b$

2. Jacobians of curves

3. Quotients of Jacobians of curves

The Modular curve $X_1(N)$

Hecke

Let $\mathfrak{h}^* = \{z \in \mathbf{C} : \Im(z) > 0\} \cup \mathbf{P}^1(\mathbf{Q})$.

1. $X_1(N)_{\mathbf{C}} = \Gamma_1(N)\backslash\mathfrak{h}^*$ (compact Riemann surface)

2. In fact, $X_1(N)$ is an algebraic curve over $\mathbf{Q}$

3. $X_1(N)(\mathbf{C}) = \{(E,P) : \mathrm{ord}(P) = N\}/\sim$ (moduli space)

N	≤ 10	11	13	37	169	512	2003
genus$(X_1(N))$	0	1	2	40	1070	7809	166167

Modular forms

Hecke

1. Cuspidal modular forms

$$S_2(N) = H^0\left(X_1(N), \Omega^1_{X_1(N)}\right)$$

2. $f \in S_2(N)$ has $q(z) = e^{2\pi i z}$-expansion:

$$f = \sum_{n=1}^{\infty} a_n q^n$$

3. Hecke algebra (commutative ring):

$$\mathbf{T} = \mathbf{Z}[T_1, T_2, \ldots] \hookrightarrow \mathrm{End}(S_2(N))$$

The Modular Jacobian $J_1(N)$

Jacobi

1. Jacobian of $X_1(N)$:

$$J_1(N) = \mathrm{Jac}(X_1(N))$$

2. $J_1(N)$ is an abelian variety over $\mathbf{Q}$ of dimension $g(X_1(N))$.

3. The elements of $J_1(N)$ parameterize degree 0 divisor classes on $X_1(N)$.


Shimura

Modular Abelian Varieties

A **modular abelian variety** A over a number field K is any abelian variety quotient (over K)

$$J_1(N) \twoheadrightarrow A.$$

In other words, an abelian variety is **modular** if there exists a surjective morphism $J_1(N) \twoheadrightarrow A$.

Examples and Conjectures

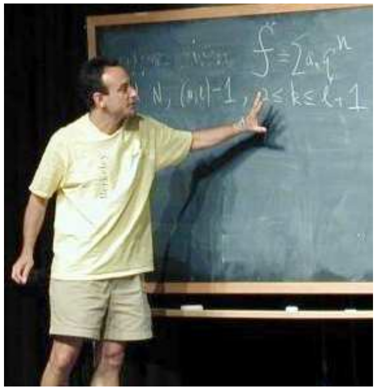
Suppose $\dim A = 1$.

- **Theorem (Wiles, Breuil, Conrad, Diamond, Taylor).** If $K = \mathbf{Q}$ then A is modular.

- **Theorem (Shimura).** If A has CM then A is modular.

- **Definition:** A over $\overline{\mathbf{Q}}$ is a **$\mathbf{Q}$-curve** if for each Galois conjugate A^σ of A there is an isogeny $A \to A^\sigma$.
  Conjecture (Ribet, Serre). Over $\overline{\mathbf{Q}}$ the non-CM modular elliptic curves are exactly the $\mathbf{Q}$-curves.

GL_2-type



Ken Ribet

Defn. $A/\mathbf{Q}$ is of (primitive) GL_2-**type** if

$$\text{End}_0(A/\mathbf{Q}) = \text{End}(A/\mathbf{Q}) \otimes \mathbf{Q}$$

is a number field of degree $\dim(A)$.

Shimura associated GL_2-type modular abelian varieties to $\mathbf{T}$-eigenforms:

$$f = q + \sum_{n \geq 2} a_n q^n \in S_2(N)$$

$$I_f = \text{Ker}(\mathbf{T} \to \mathbf{Q}(a_1, a_2, a_3, \ldots)), \; T_n \mapsto a_n$$

Abelian variety A_f over $\mathbf{Q}$ of dim $= [\mathbf{Q}(a_1, a_2, \ldots) : \mathbf{Q}]$:

$$A_f := J_1(N)/I_f J_1(N)$$

Theorem (Ribet). Shimura's A_f is $\mathbf{Q}$-isogeny simple since

$$\mathrm{End}_0(A_f/\mathbf{Q}) = \mathbf{Q}(a_2, a_3, \ldots).$$

Also $J_1(N) \sim \prod_f A_f$, where the product is over Galois-conjugacy classes of f.

Conjecture. (Serre, Ribet)

If $A/\mathbf{Q}$ is of GL_2-type, then A is modular.

2. Computerizing Abelian Varieties

Motivating Problem: Given N, "list" the modular abelian varieties $A/\overline{\mathbf{Q}}$, that are quotients of $J_1(N)$. Much work towards this by the Barcelonians Josep and Enrique González and Joan-C. Lario, building on work of Shimura, Ribet, and others. See Lario and Gonzalez, $\mathbf{Q}$-*curves and their Manin Ideals*.

Representation: $J_1(N)(\mathbf{C}) \cong V/\Lambda$,
where

$$V = \text{ complex vector space of dim } d = \dim J_1(N)$$
$$\Lambda = \text{ lattice, so } \Lambda \cong \mathbf{Z}^{2d} \text{ and } \mathbf{R}\Lambda = V$$

Quotients of $J_1(N)$

If $A(\mathbf{C}) = V_A/\Lambda_A$ then surjective morphism $\pi : J_1(N) \to A$ induces

$$\pi_V : V \to V_A \text{ and } \pi_\Lambda : \Lambda \to \Lambda_A$$

with $\mathrm{Coker}(\pi_\Lambda)$ finite.

Notice that π and $A = J_1(N)/\mathrm{Ker}(\pi)$ are determined by π_Λ. So if we had an explicit map $J_1(N)(\mathbf{C}) \cong V/\Lambda$, we could specify A by giving a map $\Lambda \to \Lambda_A \cong \mathbf{Z}^n$ with finite cokernel.

Modular Symbols

Manin

Modular symbols are a model for

$$\Lambda \cong H_1(X_1(N), \mathbf{Z})$$

on which one can give formulas for Hecke and other operators.

Intensively studied by Birch, Manin, Shokurov, Mazur, Merel, Cremona, and others.

Let $\boldsymbol{\mathcal{S}}_2(N)$ denote the space of modular symbols for $\Gamma_1(N)$. There is an explicit finite Manin symbols presentation for $\boldsymbol{\mathcal{S}}_2(N)$ and map from pairs $\alpha, \beta \in \mathbf{P}^1(\mathbf{Q})$ to $\{\alpha, \beta\} \in \boldsymbol{\mathcal{S}}_2(N)_{\mathbf{Q}}$; here $\{\alpha, \beta\}$ corresponds to the homology class in $H_1(X_1(N), \mathbf{Q})$ defined by path in $\mathfrak{h}^*$ from α to β. We have $\boldsymbol{\mathcal{S}}_2(N) \cong H_1(X_1(N), \mathbf{Z})$.

Specifying a Modular Abelian Variety (I)

DATA: A homomorphism $\boldsymbol{\mathcal{S}}_2(N) \to \mathbf{Z}^n$ for some N and n.

This data completely specifies a modular abelian variety A.

Note that **not** just any homomorphisms defines a modular abelian variety, but any modular abelian variety can be "recorded" by giving such a homomorphism. I do not know an algebraic way to decide whether such data in fact defines a modular abelian variety.

Dirichlet Character Decomposition

There is an action of $(\mathbf{Z}/N)^*$ on $\boldsymbol{\mathcal{S}}_2(N)$ by "diamond bracket operators".

Let $\varepsilon : (\mathbf{Z}/N)^* \to \mathbf{C}^*$ be a Dirichlet character and set $K = \mathbf{Q}(\varepsilon)$. The space $\boldsymbol{\mathcal{S}}_2(N,\varepsilon)_{\mathbf{Q}}$ is the biggest quotient of $\boldsymbol{\mathcal{S}}_2(N)_K$ on which $(\mathbf{Z}/N)^*$ acts through ε. We view $\boldsymbol{\mathcal{S}}_2(N,\varepsilon)_{\mathbf{Q}}$ as a $\mathbf{Q}$-vector space by restriction of scalars.

Lattice Structure on $\mathcal{S}_2(N,\varepsilon)_{\mathbf{Q}}$

There is a decomposition

$$\boldsymbol{\mathcal{S}}_2(N)_{\mathbf{Q}} = \bigoplus_{\{\varepsilon\}} \boldsymbol{\mathcal{S}}_2(N,\varepsilon)_{\mathbf{Q}},$$

where the sum is over all Galois-conjugacy classes of mod N Dirichlet characters.

The image of $\boldsymbol{\mathcal{S}}_2(N)$ in $\boldsymbol{\mathcal{S}}_2(N,\varepsilon)_{\mathbf{Q}}$ defines a lattice $\boldsymbol{\mathcal{S}}_2(N,\varepsilon)$.

Computing with $\boldsymbol{\mathcal{S}}_2(N,\varepsilon)$ is typically much more practical than computing with $\boldsymbol{\mathcal{S}}_2(N)$. For example, $\dim \boldsymbol{\mathcal{S}}_2(N,1) = 334$, whereas $\dim \boldsymbol{\mathcal{S}}_2(N) = 332334$.

Specifying a Modular Abelian Variety (II)

DATA: A homomorphism $\boldsymbol{\mathcal{S}}_2(N, \varepsilon) \to \mathbf{Z}^n$ for some N, n, and ε.

Since there is a natural homomorphism $\boldsymbol{\mathcal{S}}_2(N) \to \boldsymbol{\mathcal{S}}_2(N, \varepsilon)$, the above data completely specifies a modular abelian variety A.

3. Endomorphism Rings

A Motivating Problem. Compute

$$\mathrm{End}(J_1(N)/\overline{\mathbf{Q}}) \subset \mathrm{End}(\Lambda) \cong \mathrm{Mat}_{2d\times 2d}(\mathbf{Z})$$

with action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Solving this problem would facilitate computation of $\mathrm{End}(A/\overline{\mathbf{Q}})$ for any modular abelian variety A, and listing all modular A.

$\mathsf{End}(A)$ **versus** $\mathsf{End}_0(A)$

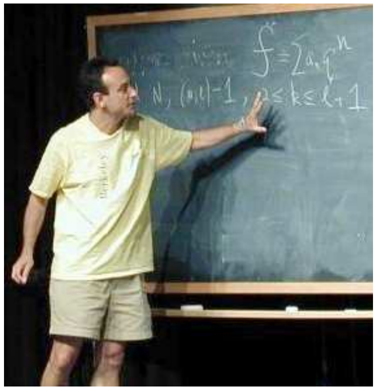
Suppose $A(\mathbf{C}) = V/\Lambda$. Given

$$\mathsf{End}_0(A) = \mathsf{End}(A) \otimes \mathbf{Q} \subset \mathsf{End}(\Lambda \otimes \mathbf{Q}),$$

it **is easy to compute** $\mathsf{End}(A)$, since

$$\begin{aligned} \mathsf{End}(A) &= \{\varphi \in \mathsf{End}_0(A) : \varphi(\Lambda) \subset \Lambda\} \\ &= \mathsf{End}_0(A) \cap \mathsf{Mat}_{2d \times 2d}(\mathbf{Z}). \end{aligned}$$

Inner Twists



Ribet

Theorem (Ribet, Math. Ann. 1980):
Description of generators for $\mathrm{End}_0(A/\overline{\mathbf{Q}})$.

Let $f = \sum a_n q^n \in S_2(N)$ be $\mathbf{T}$-eigenform, and $E = \mathbf{Q}(a_1, a_2, \ldots)$. Let T be the set of inner twists, i.e., Dirichlet characters χ such that there exists $\gamma_\chi : E \to \mathbf{C}$ such that for all $p \nmid N$ we have $\chi(p)a_p = \gamma_\chi(a_p)$. (The γ form an abelian group and $\gamma_\chi \mapsto \chi$ is a 1-cocycle.) Then

$$\mathrm{End}_0(A_f/\overline{\mathbf{Q}}) = \bigoplus_{\chi \in T} E \cdot \eta_\chi,$$

where η_χ is as defined by Shimura (and $\eta_\chi^2 = \chi(-1)r$). Also $\mathrm{End}_0(A_f/\overline{\mathbf{Q}})$ is a matrix ring over F=fixed field of all γ_χ or a matrix algebra over a quaternion division algebra with center F.

(Perhaps) Open Problem ????

Suppose $f \in S_2(N)$ is an eigenform with an inner twist by $\chi \neq 1$. Let $V \subset \boldsymbol{\mathcal{S}}_2(N,\varepsilon)_{\mathbf{Q}}$ be the subspace corresponding to f and its Galois conjugates. **Efficiently compute η_χ on V.**

Motivation: Needed to find $\boldsymbol{\mathcal{S}}_2(N,\varepsilon) \to \Lambda_A$ purely algebraically.

Shimura and Ribet: A formula for η_γ on modular forms. Let $r = \mathrm{cond}(\chi)$. Then η_γ on $S_2(\mathrm{lcm}(N, r^2, Nr))$ is given by

$$g \mapsto \sum_{u=1}^{r} \chi^{-1}(u) g|_{\left(\begin{smallmatrix} 1 & u/r \\ 0 & 1 \end{smallmatrix}\right)}.$$

By duality, the formula

$$x \mapsto \sum_{u=1}^{r} \chi^{-1}(u) \begin{pmatrix} 1 & u/r \\ 0 & 1 \end{pmatrix} (x)$$

defines η_χ on $\boldsymbol{\mathcal{S}}_2(\mathrm{lcm}(N, r^2, Nr)) \otimes \mathbf{Z}[\chi]$.

However, dim $\boldsymbol{\mathcal{S}}_2(\mathrm{lcm}(N, r^2, Nr))$ can be **huge!**
First example: $N = 13$, $\varepsilon : (\mathbf{Z}/13)^* \to \mu_6$, $\chi = \varepsilon^{-1}$, $r = 13$,

$$\mathrm{lcm}(N, r^2, Nr) = 169$$

$$\dim \boldsymbol{\mathcal{S}}_2(169) = 2140.$$

Conjecture (W. Stein). ???

Let $\gamma \in \mathrm{Gal}(\mathbf{Q}(\varepsilon)/\mathbf{Q})$ be such that $\chi^2\varepsilon = \gamma(\varepsilon)$.
Let $N' = \mathrm{lcm}(N, r^2, sr)$ where $r = \mathrm{cond}(\chi)$ and $s = \mathrm{cond}(\varepsilon)$.
Conjectural formula for η_χ on $V \subset \boldsymbol{\mathcal{S}}_2(N,\varepsilon)_{\mathbf{Q}}$:

$$\eta_\chi(x) = * \sum_{u=1}^{r} \chi(u)^{-1} \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)} \gamma(\varepsilon)(a) \cdot \left(\begin{pmatrix} 1 & u/r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) \gamma(x),$$

where the inner sum is over $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N')\backslash\Gamma_0(N)$. (Here $*$ is a nonzero scalar that does not depend on x and is easy to identify in practice from the fact that $\eta_\chi^2 = \chi(-1)r$. Guess: $* = \varphi(N'/N)$?)

Evidence

1. I've computed formula for every $f \in S_2(N)$ for $N \leq 49$ and it satisfies some consistency checks.

2. Formula motivated by formally composing

$$\begin{tikzcd}
\boldsymbol{\mathcal{S}}_2(N,\varepsilon)_{\mathbf{Q}} \arrow[r] & \boldsymbol{\mathcal{S}}_2(N',\varepsilon) \arrow[d, "\eta"] \\
\boldsymbol{\mathcal{S}}_2(N,\gamma(\varepsilon))_{\mathbf{Q}} \arrow[u] & \boldsymbol{\mathcal{S}}_2(N',\gamma(\varepsilon)) \arrow[l]
\end{tikzcd}$$

Example: $J_1(13)$

$f = q + (-\omega - 1)q^2 + (2\omega - 2)q^3 + \omega q^4 + (-2\omega + 1)q^5 + \cdots$
where $\omega^3 = 1$.

Character ε of f of order 6 and $\chi = \varepsilon^{-1}$ is inner twist.

Using above formula, get

$$\eta_\chi = \begin{pmatrix} 0 & 3 & 0 & -4 \\ 3 & 0 & -4 & 0 \\ 0 & -1 & 0 & -3 \\ -1 & 0 & -3 & 0 \end{pmatrix}$$

in terms of basis

$$b_1 = \{-1/8, 0\} - 2\{-1/6, 0\} - 2\omega\{-1/6, 0\}$$
$$b_2 = \{-1/4, 0\} - \{-1/6, 0\} - 2\omega\{-1/6, 0\}$$
$$b_3 = -2\{-1/6, 0\} - \omega\{-1/8, 0\}$$
$$b_4 = -2\{-1/6, 0\} - \omega\{-1/4, 0\} - \omega\{-1/6, 0\}$$

Note that $\eta_\chi^2 = \chi(-1)13 = 13$.

With respect to this basis, we also have

$$T_2 = \begin{pmatrix} -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & -1 \\ 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & -2 \end{pmatrix}$$

We have $\mathrm{End}(J_1(13)/\overline{\mathbf{Q}}) = \mathrm{Mat}_2(\mathbf{Q})$ generated as a $\mathbf{Q}$-vector space explicitly by 1, η_χ, T_2 and $T_2\eta_\chi$.

Using η_χ and a formula in Gonzalez-Lario, we can algebraically find a map from $\boldsymbol{\mathcal{S}}_2(13) \to \Lambda_A$ for an elliptic curve factor A of $J_1(13)/\overline{\mathbf{Q}}$.

Thank you for coming!

Acknowledgements:

Papers of Ken Ribet, Goro Shimura, etc.

Conversations with David Kohel, Enrique Gonzalez

Kite photos by Allan Steel