Explicitly Computing With Modular Abelian Varieties

William Stein
Harvard University

February 6, 2004
Center for Communications Research in Princeton

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

Connection with Cryptographhy

Modular abelian varieties over finite fields provide a large source of groups that can be used for cryptography (e.g., Elliptic Curve Cryptography). I will focus on modular abelian varieties over infinite fields today, but the results are relevant for understanding the reductions of those varieties modulo primes.

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. $X_1(N)$ has natural structure of 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 (of weight 2):
$$S_2(N) = \mathrm{H}^0\left(X_1(N), \Omega^1_{X_1(N)}\right)$$
2. $f \in S_2(N)$ has Fourer expansion in terms of $q(z) = e^{2\pi iz}$
$$f = \sum_{n=1}^{\infty} a_n q^n$$
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 divisor classes on $X_1(N)$ of degree 0.

Modular Abelian Varieties

Shimura

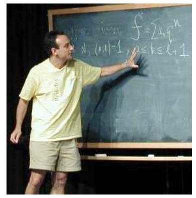
A **modular abelian variety** A over a number field K is any abelian variety A (over K) such that there is a homomorphism
$$A \to J_1(N)$$
with finite kernel.

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 **Q-curve** if for each Galois conjugate A^σ of A there is an isogeny $A \to A^\sigma$ (an isogeny is a map with finite kernel).
  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 simple abelian variety $A/\mathbf{Q}$ is of GL_2-**type** if

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

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

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

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

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

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

Conjecture. (Ribet)

The simple modular abelian varieties A over $\mathbf{Q}$ are exactly the simple abelian varieties over $\mathbf{Q}$ of GL_2-type.

Ribet proved that his conjecture follows from Serre's unproven conjectures on modularity of odd mod p Galois representations.

2. Computing With Abelian Varieties

Goal: Develop a systematic theory for computing with modular abelian varieties.

Basic Problems: Presentation, isogeny testing, isomorphism testing, endomorphism ring, enumeration.

Arithmetic Problems: Special values of L-functions, computing Shafarevich-Tate groups, Tamagawa numbers, enumerating elements of isogeny class.

Presentation

Modular abelian varieties can be specified in many ways:

- Equations
- Built from newform abelian varieties A_f
- Arise theoretically (e.g., Jacobians of Shimura curves).

For all our questions today we will view a modular abelian variety as being defined in the following way. Any modular abelian variety B can be obtained by quotienting an abelian subvariety $A \subset J_1(N)$ by a finite subgroup G. Thus we represent B by giving a pair (A, G), where $G \subset A \subset J_1(N)$.

Specifing A

An inclusion $\varphi : A \hookrightarrow J_1(N)$ induces an inclusion on homology

$$\mathrm{H}_1(A, \mathbf{Q}) \hookrightarrow \mathrm{H}_1(J_1(N), \mathbf{Q}),$$

and A is completely determined by the image of $\mathrm{H}_1(A, \mathbf{Q})$ in the vector space $\mathrm{H}_1(J_1(N), \mathbf{Q})$.

We give A by giving a subspace $V = V_{\mathbf{Q}} \subset \mathrm{H}_1(J_1(N), \mathbf{Q})$.

Specifing G

By the Abel-Jacobi theory there is a canonical isomorphism

$$J_1(N)(\mathbf{C}) \cong \mathrm{H}_1(J_1(N), \mathbf{R}) / \mathrm{H}_1(J_1(N), \mathbf{Z}).$$

Likewise $A(\mathbf{C}) \cong V_{\mathbf{R}}/V_{\mathbf{Z}}$, where $V_{\mathbf{Z}} = V \bigcap \mathrm{H}_1(J_1(N), \mathbf{Z})$, so

$$A(\mathbf{C})_{\mathrm{tor}} \cong V_{\mathbf{Q}}/V_{\mathbf{Z}}.$$

We give G by giving finitely many elements of $V_{\mathbf{Q}}/V_{\mathbf{Z}}$.

Recognition Problem

Problem: When does a subspace $V \subset \mathrm{H}_1(J_1(N), \mathbf{Q})$ correspond to an abelian subvariety A of $J_1(N)$ over K?

Solution: Given an isogeny decomposition of $J_1(N)$ over K as a direct sum of simple abelian varieties, I have an algorithm to solve this problem. (It is straightforward to compute such a decomposition when $K = \mathbf{Q}$.)

Problem: Given a group G defined by a finite list of elements of $V_{\mathbf{Q}}/V_{\mathbf{Z}}$, find the smallest number field over which G is defined. This is important because if G is defined over K, then $B = A/G$ is defined over K.

Solution??: I have not solved this problem, which is likely very difficult.

Modular Symbols

Manin

Modular symbols provide a presentation of

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

on which one can give formulas for Hecke and other operators. They have been intensively studied by Birch, Manin, Shokurov, Mazur, Merel, Cremona, and others.

```
> M := CuspidalSubspace(ModularSymbols(Gamma1(11)));
> Basis(M);
[
 -1/5*{-1/2, 0} + -2/5*{-1/4, 0} + 3/5*{-1/7, 0} + -1/5*{7/15,1/2},
 -2/5*{-1/2, 0} + 1/5*{-1/4, 0} + 1/5*{-1/7, 0} + -2/5*{7/15,1/2}
]
```


Enumeration Problem Over Q

Problem: Give an algorithm to systematically enumerate every modular abelian variety over $\mathbf{Q}$.

The isogeny classes of simple modular abelian varieties over $\mathbf{Q}$ are in bijection with *newforms*, which are eigenvectors for Hecke operators in the space $S_2(\Gamma_1(N))$ of modular forms. Using the Atkin-Lehner-Li theory of newforms, modular symbols, and linear algebra, we can thus enumerate the isogeny classes over $\mathbf{Q}$.

I **do not know** how to find all abelian varieties in an isogeny class, except when A has dimension 1, where it is solved. Maybe at least find several by intersecting $A \subset J_1(N)$ with other abelian varieties over $\mathbf{Q}$, quotienting out by intersection, and proving quotient is not isomorphic to A.

Example

```
> Factorization(J1(17));
[*
<Modular abelian variety 17A of dimension 1, level 17
 and conductor 17 over Q, [
    Homomorphism from 17A to J1(17) given on integral
    homology by:
    [-3  1  2 -2  0 -2  2 -1  2  4]
    [-2 -2  0  0  0  0  0  2  4  0]
]>,
<Modular abelian variety 17A[2] of dimension 4, level 17
 and conductor 17^4 over Q, [
    Homomorphism from 17A[2] to J1(17) (not printing
    8x10 matrix)
]>
*]
```


Enumeration Problem Over $\overline{\mathbf{Q}}$

Problem: Give an algorithm to systematically enumerate every modular abelian variety over $\overline{\mathbf{Q}}$.

There is a huge amount of work by Shimura, Ribet, González, Lario, and others, but still nobody has given an algorithm to enumerate all isogeny classes of modular abelian varieties over $\overline{\mathbf{Q}}$ explicitly. By explicit, I mean in the sense of giving defining data, i.e., a pair $(V,\ G \subset V_{\mathbf{Q}}/V_{\mathbf{Z}})$.

Obstructions:
- Difficulty of constructing $\mathrm{End}(A_f/\overline{\mathbf{Q}})$ explicitly (I have an algorithm, but it is *way too slow* to be useful)
- Difficulty of decomposing $A_f/\overline{\mathbf{Q}}$ as a product of simples, even given $\mathrm{End}(A_f/\overline{\mathbf{Q}})$. Need a good "Meataxe" over $\mathbf{Q}$.

Computing Endomorphism Rings

Problem: Given a modular abelian variety A over K, compute $\mathrm{End}(A)$ explicitly, i.e., give matrices in $\mathrm{End}(V)$ that generate $\mathrm{End}(A)$ as an abelian group.

Solution: When $A \subset J_1(N)$ is simple, $\mathrm{End}(A) \otimes \mathbf{Q}$ is a skew field, which can be computed. For example, if $K = \mathbf{Q}$, then $A = A_f$ is attached to a newform and $\mathrm{End}(A) \otimes \mathbf{Q}$ is generated by the image of the Hecke algebra. We can then find $\mathrm{End}(A)$ in $\mathrm{End}(A) \otimes \mathbf{Q}$ as the $\mathbf{Z}$-submodule of elements that preserve the lattice $V_{\mathbf{Z}}$.

We can also explicitly compute $\mathrm{Hom}(A, B)$ for any modular abelian varieties A and B, by writing A and B as simples, computing endomorphism algebras, and finding the $\mathbf{Z}$-module of homomorphisms that induce a map that fixes integral homology.

Example

```
> A := J0(33); A;
Modular abelian variety J0(33) of dimension 3 and level 3*11 over Q
> End(A);
Group of homomorphisms from J0(33) to J0(33)
> Basis(End(A));
[
    Homomorphism from J0(33) to J0(33) (not printing 6x6 matrix),
    Homomorphism from J0(33) to J0(33) (not printing 6x6 matrix),
    Homomorphism from J0(33) to J0(33) (not printing 6x6 matrix),
    Homomorphism from J0(33) to J0(33) (not printing 6x6 matrix),
    Homomorphism from J0(33) to J0(33) (not printing 6x6 matrix)
]
> Matrix(Basis(End(A))[2]);
[ 0  1  0  0  0 -1]
[ 0  1  0  0  0  0]
[ 0  1  0  0 -1  0]
[ 0  1 -1  1 -1  0]
[ 0  1 -1  0  0  0]
[-1  1  0  0  0  0]
```

Isogeny Testing

Problem: Given modular abelian varieties A and B, determine whether or not A is isogenous to B.

Determine whether A is isogenous to B is easy, since we may assume A and B are attached to newforms $\sum a_n q^n$ and $\sum b_n q^n$, and then A is isogenous to B if and only if the newforms are Galois conjugate.

Isomorphism Testing

Problem: Suppose A is isogenous to B. Decide whether A is isomorphic to B.

I **do not know how to do this** in general. Assume we have computed End(A), End(B), and Hom(A, B) explicitly. Given a basis for Hom(A, B), how do we know if some linear combination of that basis has determinant 1? It's not clear (to me).

If A and B are both simple and have commutative endomorphism ring, then I found an algorithm to decide whether A is isomorphic to B. This algorithm can be extended to abelian varieties that are products of such A, assuming the factors occur with multiplicity 1 (up to isogeny). However, I do not know in general how to decide whether $A \oplus A$ is isomorphic to $B \oplus B$, though I have a vague strategy that I think might work.

Algorithm for Testing Isomorphism

Suppose A and B are explicitly defined modular abelian varieties over $\mathbf{Q}$ that are both isogenous to an abelian variety A_f. The following algorithm determine whether A is isomorphic to B.

Let $H = \text{Hom}(A, B)$. Both A and B are given explicitly by pairs (V, G_1) and (V, G_2), so we can compute an isogeny $f : B \to A$. Let $H_f = \{\phi \circ f : \phi \in H\} \subset \text{End}(B)$. Note that A is isomorphic to B if and only if H_f contains an element of degree deg(f). Also note that H_f has finite index in End(B).

By hypothesis $K = \text{End}(B) \otimes \mathbf{Q}$ is the field generated by the Fourier coefficients of f. The norm of an element of K is the positive square root of the degree of the corresponding homomorphism (see Milne in Cornell-Silverman, pg 126, Prop. 12.12).

Thus if deg(f) is not a perfect square, then there can be no element of B of degree deg(f), so A is not isomorphic to B. Thus suppose deg$(f) = d^2$.

Typically there will be infinitely many element in $\mathcal{O}_K$ of norm d, but there are only finitely many up to units. There is an algorithm, which involves computing the class group of $\mathcal{O}_K$, which enumerates representive elements of $\mathcal{O}_K$ of norm d, up to units (e.g., the `NormEquation` command in MAGMA). Thus suppose we have computed representative elements $z_1, \ldots, z_n$ of the elements of $\mathcal{O}_K$ with norm d. Then A is isomorphic to B if and only if there is a unit u and a z_i such that $u^{-1} z_i \in H_f \subset K$. Equivalently, such that $z_i \in uH_f$. There are only finitely many possibilities for uH_f, since H_f has finite index in $\mathcal{O}_K$ and $[\mathcal{O}_K : uH_f] = [\mathcal{O}_K : H_f]$, since $\mathcal{O}_K = u\mathcal{O}_K$. We can thus list all subgroups uH_f (since we can compute generaturs for $\mathcal{O}_K^*$) and hence determine whether H_f contains an element of norm d, as required.