Explicitly Computing With Modular Abel

William Stein
Harvard University

February 6, 2004
Center for Communications Research in P

Overview of Talk

1. Modular Abelian Varieties

2. Computing With Modular Abelian Varieties

Modular Abelian Varieties

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 Cryptograp

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

The Modular Curve $X_1(N)$

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 sur

2. $X_1(N)$ has natural structure of algebraic curv

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

N	≤ 10	11	13	37	169	51
genus($X_1(N)$)	0	1	2	40	1070	78

Modular Forms

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

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

3. Hecke algebra (*commutative* ring):

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

The Modular Jacobian $J_1(N)$

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 dimensi

3. The elements of $J_1(N)$ parameterize divisor cl
of degree 0.

Modular Abelian Varieties

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.

Suppose $\dim A = 1$.

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

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

- **Definition:** A over $\overline{\mathbf{Q}}$ is a **Q-curve** if for ea jugate A^σ of A there is an isogeny $A \to A^\sigma$ (map with finite kernel).
  Conjecture (Ribet, Serre). Over $\overline{\mathbf{Q}}$ the no elliptic curves are exactly the $\mathbf{Q}$-curves.

GL_2-type

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 eigenforms:

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

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

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

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

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

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

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

Conjecture. (Ribet)

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

Ribet proved that his conjecture follows from Se conjectures on modularity of odd mod p Galois r

2. Computing With Abelian Variet

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

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

Arithmetic Problems: Special values of L-f
puting Shafarevich-Tate groups, Tamagawa nur
ating elements of isogeny class.

Presentation

Modular abelian varieties can be specified in mar

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

For all our questions today we will view a modul ety as being defined in the following way. Any r variety B can be obtained by quotienting an abe $A \subset J_1(N)$ by a finite subgroup G. Thus we repres 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

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

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

We give A by giving a subspace $V = V_{\mathbf{Q}} \subset$

Specifing G

By the Abel-Jacobi theory there is a canonical is

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

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

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

We give G by giving finitely many element

Recognition Problem

Problem: When does a subspace $V \subset \mathrm{H}_1(J$
spond to an abelian subvariety A of $J_1(N)$ over K

Solution: Given an isogeny decomposition of
as a direct sum of simple abelian varieties, I hav
to solve this problem. (It is straightforward to c
decomposition when $K = \mathbf{Q}$.)

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

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

Modular Symbols

Modular symbols provide a presentation of

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

on which one can give formulas for Hecke and o
They have been intensively studied by Birch, Ma
Mazur, Merel, Cremona, and others.

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

Enumeration Problem Over

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

The isogeny classes of simple modular abelian v
are in bijection with *newforms*, which are eigenve
operators in the space $S_2(\Gamma_1(N))$ of modular fo
Atkin-Lehner-Li theory of newforms, modular sym
algebra, we can thus enumerate the isogeny clas

I **do not know** how to find all abelian varieties
class, except when A has dimension 1, where it is
at least find several by intersecting $A \subset J_1(N)$ wit
varieties over $\mathbf{Q}$, quotienting out by intersectio
quotient is not isomorphic to A.

Example

```
> Factorization(J1(17));
[*
<Modular abelian variety 17A of dimension 1, le
 and conductor 17 over Q, [
    Homomorphism from 17A to J1(17) given on in
    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,
 and conductor 17^4 over Q, [
    Homomorphism from 17A[2] to J1(17) (not pri
    8x10 matrix)
]>
*]
```

Enumeration Problem Over

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

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

Obstructions:

- Difficulty of constructing End$(A_f/\overline{\mathbf{Q}})$ explicitly (
rithm, but it is *way too slow* to be useful)
- Difficulty of decomposing $A_f/\overline{\mathbf{Q}}$ as a product c
given End$(A_f/\overline{\mathbf{Q}})$. Need a good "Meataxe" over

Computing Endomorphism Ri

Problem: Given a modular abelian variety A ov
End(A) explicitly, i.e., give matrices in End(V)
End(A) as an abelian group.

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

We can also explicitly compute Hom(A, B) for any
varieties A and B, by writing A and B as simp
endomorphism algebras, and finding the $\mathbf{Z}$-modul
phisms that induce a map that fixes integral hon

Example

```
> A := J0(33); A;
Modular abelian variety J0(33) of dimension 3 and level 3
> End(A);
Group of homomorphisms from J0(33) to J0(33)
> Basis(End(A));
[
    Homomorphism from J0(33) to J0(33) (not printing 6x6
    Homomorphism from J0(33) to J0(33) (not printing 6x6
    Homomorphism from J0(33) to J0(33) (not printing 6x6
    Homomorphism from J0(33) to J0(33) (not printing 6x6
    Homomorphism from J0(33) to J0(33) (not printing 6x6
]
> 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 an
whether or not A is isogenous to B.

Determine whether A is isogenous to B is easy
assume A and B are attached to newforms $\sum a_n$
and then A is isogenous to B if and only if the
Galois conjugate.

Isomorphism Testing

Problem: Suppose A is isogenous to B. Decid
isomorphic to B.

I **do not know how to do this** in general. As
computed End(A), End(B), and Hom(A, B) exp
basis for Hom(A, B), how do we know if some line
of that basis has determinant 1? It's not clear (t

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

Algorithm for Testing Isomorp

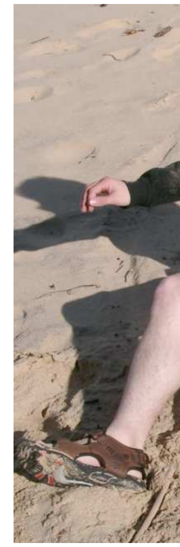
Suppose A and B are explicitly defined modular a
over $\mathbf{Q}$ that are both isogenous to an abelian va
following algorithm determine whether A is isomo

Let $H = \mathrm{Hom}(A, B)$. Both A and B are given ex
(V, G_1) and (V, G_2), so we can compute an isog
Let $H_f = \{\phi \circ f : \phi \in H\} \subset \mathrm{End}(B)$. Note that
to B if and only if H_f contains an element of
Also note that H_f has finite index in $\mathrm{End}(B)$.

By hypothesis $K = \mathrm{End}(B) \otimes \mathbf{Q}$ is the field ge
Fourier coefficients of f. The norm of an eleme
positive square root of the degree of the corres
morphism (see Milne in Cornell-Silverman, pg 126

Thus if deg(f) is not a perfect square, then there
ment of B of degree deg(f), so A is not isomorp
suppose deg(f) $= d^2$.

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



Thank you for inviting me!

Acknowledgements:

Papers of Ken Ribet, Goro Shimura, and Joan L
Conversations with John Cannon, Enrique Gonza
hel, Barry Mazur, Allan Steel