Explicit Modular Abelian Varieties

William Stein and Tseno Tselkov

July 27, 2004

Contents

1 Introduction **2**
1.1 Modular Abelian Varieties 2

2 Explicit Computations with Modular Abelian Varieties **2**
2.1 Enumeration 2
2.2 Isogenies 2
2.3 The Endomorphism Ring 4
2.4 Determining Isomorphism 6
2.5 Determining Minimal Degree of an Isogeny 8

3 Examples **9**
3.1 Level 35 9
3.2 Level 69: The first A_f that is not isomorphic to $A_f^\vee$ 9
3.3 Level 195: An A_f not isomorphic to its dual, though there are solutions to norm equation 10

4 Future Directions **10**
4.1 Enumerating Elements of the Isogeny Class 10
4.2 Frank Calegari - Hope? 12

5 Tables **12**

6 Diary (omit from final paper) **13**
6.1 06-21-2004 13
6.2 06-23-2004 13
6.3 06-23-2004 14
6.4 06-30-2004 15
6.5 07-24-2004 16

7 Polarization **17**

1 Introduction

A *modular abelian variety* A over $\mathbf{Q}$ is an abelian variety that admits a finite map to $J_1(N)$, for some positive integer N.

Definition 1.1 (GL_2**-type).** Suppose A is a simple abelian variety over $\mathbf{Q}$. Then A is of GL_2-type if and only if $\mathrm{End}(A) \otimes \mathbf{Q}$ is a number field of dimension equal to $\dim(A)$.

Conjecture 1.2 (Ribet). *The simple abelian varieties over* $\mathbf{Q}$ *of* GL_2*-type are exactly the simple modular abelian varieties.*

Ribet proves in [Rib92, Thm. 4.4] Conjecture 1.2 is implied by Serre's conjectures [Ser87] on modularity of two-dimensional odd mod p Galois representations. Also, Wiles et al. have proven Conjecture 1.2 for all abelian varieties of dimension 1.

1.1 Modular Abelian Varieties

What are they? Standard conjectures? How we represent in computer. Jacobian of Shimura curves...

Acknowledgement: Allan Steel for mentioning Algorithm [[...]] for saturation.

2 Explicit Computations with Modular Abelian Varieties

2.1 Enumeration

Algorithm 2.1 (Enumerate Modular Abelian Varieties). Given a positive integer N this algorithm returns one explicit modular abelian variety in each isogeny class of simple new modular abelian varieties of level N.

Algorithm 2.2 (Decompose as Product). Given an explicit modular abelian variety A, this algorithm finds simples abelian varieties B_i and an isogeny $A \to \prod B_i$.

Proof. □

Complexity?

2.2 Isogenies

Algorithm 2.3 (Test if Isogenous). Given two explicit modular abelian varieties A and B, this algorithm decides whether or not A and B are isogenous, and if so returns an explicit isogeny.

1. [A, B both simple] When A and B are both simple they are isogenous if and only if the associated newforms are Galois conjugate. In this case, a natural isogeny is induced by the map on modular forms.

2. [Pair off factors] When A and B are not simple we pair off factors, i.e. for any C in a factorization of A we try to find an isogenous D in a factorization of B. If such D exists and the multiplicities of C in A and D in B are the same we remove D and continue with another C. Otherwise, A and B cannot be isogenous.

Proof. When A and B are simple, by Proposition 3.2. in "Finiteness Results for ..." A and B are isogenous if and only if the corresponding newforms are Galois conjugate.

[[logic is obscure]] Suppose now that A and B are not simple but there is an isogeny $\varphi : A \to B$. Let $\prod_{i \in I} A_i^{e_i}$ and $\prod_{j \in J} B_j^{f_j}$ be the factorizations of A and B into products of non-isogenous simple abelian varieties. Fix some i. Combining φ with the projections of B to each of its factors we obtain morphisms from A_i to each B_j for all possible j. Since the $B_j's$ are simple each of those morphisms, which is not zero must be an isogeny. Hence exactly one of them is an isogeny and the others are zero, or otherwise φ is the zero map. Thus, for each A_i we find an isogenous copy in the decomposition of B. Repeating this argument we see that A and B are isogenous if and only if there is an isomorphism between I and J, such thatA_i is isogenous to B_i for all i, and $e_i = f_i$. $\square$

Complexity?

2.3 The Endomorphism Ring

We will use the following saturation algorithm later in order to compute $\mathrm{End}(A)$ or $\mathrm{Hom}(A, B)$ given $\mathrm{End}(A) \otimes \mathbf{Q}$ or $\mathrm{Hom}(A, B) \otimes \mathbf{Q}$. The Hermite and Smith normal forms of an integer matrix and their properties are discussed at length in [[Cohen's book]].

Algorithm 2.4 (Saturate). Given a subgroup L of $\mathbf{Z}^n$, this algorithm computes the saturation $\mathbf{Q}L \cap \mathbf{Z}^n$ of L in $\mathbf{Z}^n$. Let B be a basis for L.

1. [Hermite Normal Form] Find the Hermite Normal Form H of B.
2. [Smith Normal Form] Compute the Smith Normal Form $S = PHQ$ of H for some P and Q.
3. [Remove content] If S has only ones on the diagonal return H. Otherwise, set $H = PH$, divide each row of H by its content (the gcd of the entries), and go to step 2.

Proof. In order to prove that the algorithm terminates, we must show that if some diagonal entry of S is not 1, then some row of PH has content bigger than 1. □

[[william–finish this. include modular method for small prime divisors of det... See photo from 07/24. Also look at NTL.]] Complexity?

Lemma 2.5. *Let K be a number field. If an element $x \in \mathbf{C}$ is fixed by every element of $\mathrm{Aut}(\mathbf{C}/K)$, then $x \in K$.*

Proof. If $x \in \overline{K}$, this is standard Galois theory. If $x \notin \overline{K}$, then x is transcendental. Since $x + 1$ is also transcendental, the fields $\overline{K}(x)$ and $\overline{K}(x+1)$ are isomorphic via a map σ sending x to $x + 1$. Every automorphism of a subfield of $\mathbf{C}$ extends to $\mathbf{C}$, so σ extends to an automorphism of $\mathbf{C}$ that does not fix x. [[I'm not completely convinced.]] □

Proposition 2.6. *Let A be a simple abelian variety over a number field K.*

$$\mathrm{End}(A/K) = (\mathrm{End}(A/K) \otimes \mathbf{Q}) \cap \mathrm{End}(\Lambda_A),$$

where $\Lambda_A = \mathrm{H}_1(A, \mathbf{Z})$ and we implicitly embed $\mathrm{End}(A/K)$ in $\mathrm{End}(\Lambda_A)$, so the intersection takes place in $\mathrm{End}(\Lambda_A) \otimes \mathbf{Q}$.

Proof. The inclusion of $\mathrm{End}(A/K)$ in the right hand side is obvious, so suppose $\varphi \in (\mathrm{End}(A/K) \otimes \mathbf{Q}) \cap \mathrm{End}(\Lambda_A)$. Then there is a positive integer n such that $n\varphi \in \mathrm{End}(A/K)$. Thus $n\varphi$ induces a complex-linear endomorphism of $\mathrm{Tan}(A_{\mathbf{C}})$. Thus φ induces a complex-linear endomorphism of $\mathrm{Tan}(A_{\mathbf{C}})$, and by hypothesis φ preserves Λ_A. An element of $\mathrm{End}(A/\mathbf{C})$ is a complex linear map on $\mathrm{Tan}(A_{\mathbf{C}})$ that preserves Λ_A, so $\varphi \in \mathrm{End}(A/\mathbf{C})$.

There is an n such that $n\varphi$ is defined over K, so for any $\sigma \in \mathrm{Gal}(\mathbf{C}/K)$, we have $\sigma([n]\varphi) - [n]\varphi = 0$. But

$$\sigma([n]\varphi) = \sigma([n])\sigma(\varphi) = [n]\sigma(\varphi),$$

so

$$[n](\sigma(\varphi) - \varphi) = 0,$$

which implies $\sigma(\varphi) = \varphi$, since the kernel of $[n]$ is finite and image of $\sigma(\varphi) - \varphi$ is either infinite or 0. By Lemma 2.5, $\varphi \in \mathrm{End}(A/K)$. ☐

Complexity?

[[This must be after Alg 2.9 to compute the $\mathrm{End}(A)$ in the first place.]]

Algorithm 2.7 (Endomorphism Algebra as Field). Given a simple explicit modular abelian variety A over $\mathbf{Q}$, this (randomized) algorithm returns a number field K and an isomorphism $\mathrm{End}(A) \otimes \mathbf{Q} \to K$.

1. [Choose random endomorphism] Randomly pick an endomorphism φ and compute its minimal polynomial f.
2. [Does endomorphism generate?] If $\deg f = \dim(A)$, then let K be the number field generated by a root α of f. Otherwise, go to step 1.
3. [Define an explicit isomorphism] Let Ψ be the unique field homomorphism $\mathrm{End}(A) \otimes \mathbf{Q} \to K$ that sends φ to α. Then Ψ is the desired isomorphism.

Proof. By Ribet [...], because A is simple, modular, and defined over $\mathbf{Q}$, we know that $\mathrm{End}(A) \otimes \mathbf{Q}$ is a number field of degree equal to $\dim(A)$. (If A were not defined over, then $\mathrm{End}(A) \otimes \mathbf{Q}$ could be a non-commutative division algebra.)

By the primitive element theorem, there exists a φ such that $\deg(f) = \dim(A)$, where f is the minimal polynomial of φ. Then since $\deg(f) = \dim(A)$ it follows that the map Ψ is an isomorphism (a nonzero homomorphism between number fields of the same dimension is an isomorphism). ☐

Complexity? This is where probability of choosing a primitive element at random comes in... This is CERTAINLY already already analyzed somewhere in the literature. "ON DENSITY OF PRIMITIVE ELEMENTS FOR FIELD EXTENSIONS JOEL V. BRAWLEY AND SHUHONG GAO"
(`http://www.math.clemson.edu/faculty/Gao/papers/prim-ele.pdf`)

Algorithm 2.8 (Compute $\mathrm{Hom}(A, B)$). Given explicit modular abelian varieties A and B, this algorithm computes $\mathrm{Hom}(A, B)$.

1. [Factorizations] Compute using Algorithm [[...blah...]] factorizations $\prod_{i \in I} C_i^{e_i}$ and $\prod_{i \in I} C_i^{f_i}$ of A and B respectively, where I is some index set, the $C_i's$ are non-isogenous simple abelian varieties, and $e_i, f_i \geq 0$.
2. [Simple case] When $A \sim C^e$ and $B \sim D^f$, where C, D are simple abelian varieties we compute $\mathrm{Hom}(A, B)$ in the following way. If C and D are not isogenous $\mathrm{Hom}(A, B) = 0$. If C and D are isogenous, $\mathrm{Hom}(A, B) = \mathrm{Hom}(C^e, D^f) \otimes \mathbf{Q} = M_{e \times f}(\mathrm{End}(C) \otimes \mathbf{Q})$. Then we compute $\mathrm{Hom}(A, B) \subset \mathrm{Hom}(A, B) \otimes \mathbf{Q}$ using algorithm [...].

3. [General case] We compute each $\mathrm{Hom}(C_i^{e_i}, C_j^{f_j})$ as in step [...] and obtain $\mathrm{Hom}(A, B)$ as a block matrix with blocks $\mathrm{Hom}(C_i^{e_i}, C_j^{f_j})$.

[[Remark: A and B need not be isomorphic to those products of C_i. So you have to precompose with the isogeny $A \to \prod C_i^{e_i}$, etc.]]

Proof. Suppose first that $A \sim C^e$, $B \sim D^f$ with C, D simple abelian varieties. When C and D are not isogenous there is no morphism $A \to B$, so $\mathrm{Hom}(A, B) = 0$. When C and D are isogenous, a morphism $C^e \to D^f$ over $\mathbf{Q}$ is given by an $e \times f$ matrix with entries from $\mathrm{End}(A) \otimes \mathbf{Q}$, where the $(i, j)^{th}$ entry represents the morphism between the i^{th} component of A and j^{th} component of B. We get $\mathrm{End}(A) \otimes \mathbf{Q}$ using algorithm [...]. Once we have $\mathrm{Hom}(A, B) \otimes \mathbf{Q}$ to get $\mathrm{Hom}(A, B)$ we only need to apply algorithm [...].

In general, when $A = \prod_{i \in I} C_i^{e_i}$ and $B = \prod_{i \in I} C_i^{f_i}$ we get $\mathrm{Hom}(C_i^{e_i}, C_j^{f_j})$ as before and combining these blocks we obtain $\mathrm{Hom}(A, B)$. □

Complexity?

Algorithm 2.9 (Compute $\mathrm{End}(A)$). Given an explicit modular abelian variety A, this algorithm computes $\mathrm{End}(A)$.

1. [Initialize] Let $d = \dim(A_f)$, let $n = 1$, and let V be the zero subspace of $\mathrm{End}(A_f/\mathbf{Q}) \otimes \mathbf{Q}$.
2. [Compute Hecke operator] Using ... compute the restriction of the Hecke operator T_n to A_f, as an element of $\mathrm{End}(A_f/\mathbf{Q}) \otimes \mathbf{Q}$.
3. [Increase V] Replace V by $V + \mathbf{Q} \cdot T_n$.
4. [Finished?] If $\dim(V) < d$, go to step 2.
5. [Saturate] Compute $\mathrm{End}(A_f/\mathbf{Q}) = V \cap \mathrm{End}(\Lambda_{A_f})$ using algorithm ....

Proof. We need to show that the algorithm terminates, i.e. that the Hecke algebra generates $\mathrm{End}(A_f/\mathbf{Q}) \otimes \mathbf{Q}$. But by Theorem 1 of Shimura's "On the factors..." the image of $T \otimes \mathbf{Q}$ in $\mathrm{End}(A_f/\mathbf{Q}) \otimes \mathbf{Q}$ is a subfield of degree $\dim A_f$. But A_f is simple by Corollary 4.2 of Ribet's "Twists of Modular Forms and ...", so Theorem 2.1 from Ribet's "Abvars over $\mathbf{Q}$ and modular forms" implies that $\mathrm{End}(A_f/\mathbf{Q}) \otimes \mathbf{Q}$ also has dimension $\dim(A_f)$. Thus the Hecke algebra generates $\mathrm{End}(A_f/\mathbf{Q}) \otimes \mathbf{Q}$. By Proposition 2.6 once we have $\mathrm{End}(A_f/\mathbf{Q}) \otimes \mathbf{Q}$ we apply algorithm [...] to get $\mathrm{End}(A_f/\mathbf{Q})$. □

Complexity?

2.4 Determining Isomorphism

Algorithm 2.10 (Norm Equation). Given an order $\mathcal{O}$ in a number field K and an element $a \in \mathbf{Q}$, this algorithm finds all solutions in $\mathcal{O}$ to the norm equation $\mathrm{Norm}(x) = a$, up to units of $\mathcal{O}$.

Claus Fieker suggests the following algorithm (we should expand on that)

1. [Class Group] Find the class group of K.
2. [Ideals of bounded norm] Use linear programming to find all ideals of norm up to some bound.
3. [Solve] Deduce all solutions to the norm equation up to units.

Proof. □

Complexity: need bound on number of Hecke operators needed to generate. Will come from Sturm's paper.

Algorithm 2.11 (Test if Isomorphic). Given explicit simple modular abelian varieties A and B, this algorithm either proves that A and B are not isomorphic, or returns an explicit isomorphism between them.

1. [Equal?] If $A = B$, return "yes" and the identity map.
2. [Isogenous?] Determine whether A and B are isogenous using [..]. If A and B are not isogenous then return "no", and if A and B are isogenous, let $f : B \to A$ be an isogeny.
3. [Degree of isogeny] Compute $\deg(f)$ using [..]. If $\deg(f)$ is not a square, return "no". Let d be the positive square root of $\deg(f)$.
4. [Endomorphism algebra] Compute the number field $K = \mathrm{End}(A) \otimes \mathbf{Q}$, and an explicit embedding of $\mathrm{End}(A)$ into K using [...].
5. [Hom space] Explicitly compute $\mathrm{Hom}(A, B)$ using ...
6. [Image of Hom space] Compute the image H_f of $\mathrm{Hom}(A, B)$ in $\mathrm{End}(A)$ got by composing with f...
7. [Endomorphism ring] Compute the order $\mathcal{O}$ in K generated by $\mathrm{End}(A)$ [...].
8. [Solve norm equation] Find solutions (up to units of $\mathcal{O}$) of the norm equations $\mathrm{Norm}(x) = \pm d$ in $\mathcal{O}$. If there are no solutions, return "no".
9. [Lift to H_f?] For each solution (up to units), check whether it lies in H_f.
10. [Isomorphic?] If a solution x lies in H_f, then return "yes" and $x \circ f^{-1}$.
11. [Not isomorphic?] If none of the solutions lies in H_f, return "no".

Proof. Let $f : B \to A$ be an isogeny and denote its degree by d. Define $H_f = \{f \circ \phi : \phi \in \mathrm{Hom}(A, B)\} \subset \mathrm{End}(A)$. Since degree is multiplicative, A and B are isomorphic if and only if H_f contains an element of degree d. Embed $\mathrm{End}(A)$ into $K = \mathrm{End}(A) \otimes \mathbf{Q}$ and let $\mathcal{O}$ be the order in K generated by $\mathrm{End}(A)$. By Proposition 12.12. in Milne's "Abelian Varieties" for $x \in K$ we have $\mathrm{Norm}(x)^2 = \deg(x)$. Thus, finding an element of degree d in H_f is equivalent to finding $x \in \mathcal{O}$ with $\mathrm{Norm}(x) = \pm\sqrt{d}$, such that x actually comes from H_f. □

[[There are infinitely many units, so why does looking at finitely many units suffice?!]]

[[Fix inconsistency with d's..]]

Complexity analysis. (Often solving the norm equation probably denominates...)

[[Discuss how non-simple case appears very difficult.]]

2.5 Determining Minimal Degree of an Isogeny

A small extension of algorithm [...] gives us the minimal degree of an isogeny between two explicit isogenous modular abelian varieties. [[add labels]]

Algorithm 2.12 (Minimal Isogeny). Given explicit simple modular abelian varieties A and B, this algorithm checks if A and B are isogenous and if so returns the minimal degree of an isogeny $A \to B$ together with an explicit isogeny of that degree..

1. If $A = B$, return 1 and the identity map.
2. Determine whether A and B are isogenous using [..]. If A and B are not isogenous then return "not isogenous", and if A and B are isogenous, let $f : B \to A$ be some isogeny.
3. Compute $\deg(f)$ using [..]. Write $\deg(f)$ as ab^2, where a is squarefree.
4. Compute the number field $K = \mathrm{End}(A) \otimes \mathbf{Q}$, and an explicit embedding of $\mathrm{End}(A)$ into K using [...].
5. Explicitly compute $\mathrm{Hom}(A, B)$ using ...
6. Compute the image H_f of $\mathrm{Hom}(A, B)$ in $\mathrm{End}(A)$ got by composing with f...
7. Compute the order $\mathcal{O}$ in K generated by $\mathrm{End}(A)$ [...].
8. Let $i = 0$.
9. Increase i by one and find the solutions (up to units of $\mathcal{O}$) of the norm equations $\mathrm{Norm}(x) = \pm abi$ in $\mathcal{O}$. If there are no solutions, repeat this step.
10. For each solution (up to units), check whether it lies in H_f.
11. If a solution x lies in H_f, then return ai^2 and $x \circ f^{-1}$.
12. If none of the solutions lies in H_f, return to step [...].

Proof. Let $f : A \to B$ be an isogeny and denote its degree by $d = ab^2$, where a is squarefree. Define $H_f = \{\phi \circ f : \phi \in \mathrm{Hom}(B, A)\} \subset \mathrm{End}(A)$. Since degree is multiplicative, B and A are siogenous with isogeny of degree d' if and only if H_f contains an element of degree dd'. Embed $\mathrm{End}(A)$ into $K = \mathrm{End}(A) \otimes \mathbf{Q}$ and let $\mathcal{O}$ be the order in K generated by $\mathrm{End}(A)$. By Proposition 12.12. in Milne's "Abelian Varieties" for $x \in K$ we have $\mathrm{Norm}^2(x) = \deg(x)$. Thus, finding an element of degree dd' in H_f is equivalent to finding $x \in \mathcal{O}$ with $\mathrm{Norm}(x) = \pm\sqrt{dd'}$, such that x actually comes from H_f. Hence, the possible values for d' are ai^2 for $i \in \mathcal{N}$, so the algorithm indeed finds the minimal degree of an isogeny $B \to A$. $\square$

3 Examples

A few examples with lots of detail that illustrate key aspects of the algorithm. Imagine somebody implementing the algorithm; they would compare what they get to what we give here.

3.1 Level 35

It's not obvious that A_f is iso. to its dual.

```
[35, 2, 2, 1, 6, x^4 + 2*x^3 - 7*x^2 - 8*x + 16],
```

Mention 6-author paper and Hasegawa, but that kernel of modular polarization is NOT kernel of multiplication by an integer, so Wang excludes.

Kernel is $(\mathbf{Z}/2\mathbf{Z})^2$, which is not $\ker([2]) = (\mathbf{Z}/2\mathbf{Z})^4$.

```
> J := JZero(35);
> A := J(2);
> Dual(A);
Modular abelian variety of dimension 2 and level 5*7 over Q
> Kernel(ModularPolarization(A));
Finitely generated subgroup of abelian variety with
invariants [ 2, 2 ]
```

There is a solution, and it gives an iso.

3.2 Level 69: The first A_f that is not isomorphic to $A_f^\vee$

Let A be the second factor in the decomposition of $J_0(69)$. [[Say $\dim(A) = 2$, etc., which determines A.]] Then A is not isomorphic to its dual $A^\vee$ because there are no solutions to the norm equation

$$\mathit{this} = \mathit{that}.$$

(Pell equation???) A minimal isogeny between A and $A^\vee$ is of degree 4 and is given on the integral homology by

$$\begin{pmatrix} 1 & 0 & 2 & -2 \\ 0 & 1 & 0 & 0 \\ -2 & 1 & 0 & 2 \\ 4 & -2 & 2 & -4 \end{pmatrix}$$

3.3 Level 195: An A_f not isomorphic to its dual, though there are solutions to norm equation

$[195, 5, 3, [4, 4, 4, 4, 176, 176], 0, 6, x^6 - 14 * x^4 - 4 * x^3 + 49 * x^2 + 28 * x + 4]$

There are solutions to the norm equation, but none of them works.

4 Future Directions

Polarization, enumerating the isogeny class, working over number fields, isomorphism testing in the non-simple case.

4.1 Enumerating Elements of the Isogeny Class

Discuss problem of finding lots of non-isomorphic A in the isogeny class of A_f.

Various ways to compute finite $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-stable subgroups of A. (I.e., kernel of maps to higher level Np. Intersection with other A_g's. Intersection with (or image of) cuspidal subgroup.)

Example 4.1. We show that the $\mathbf{Q}$-isogeny class of **43B** contains at least three non-isomorphic abelian varieties.

```
> J := JZero(43);
> A := J(2);
> A;
Modular abelian variety 43B of dimension 2, level 43 and
conductor 43^2 over Q
> G := RationalCuspidalSubgroup(A);
> G;
Finitely generated subgroup of abelian variety with invariants [
7 ]
> B := A/G;
> B;
Modular abelian variety of dimension 2 and level 43 over Q
> IsIsomorphic(A,B);
false
> Adual := Dual(A);
> IsIsomorphic(Adual,A);
true Homomorphism from modular abelian variety of dimension 2 to
43B given on integral homology by:
[ 1  0 -2 -1]
[ 1  0 -3 -1]
[ 0  2 -2 -1]
[ 0  1 -1 -1]
> Bdual := Dual(B);

>> Bdual := Dual(B);
```

```
                 ^
Runtime error in 'Dual': The modular embedding of argument 1 must
be injective.
> J2 := JZero(43*2);
> phi := NaturalMap(J,J2,1);
> phi2 := NaturalMap(J,J2,2);
> H := Kernel(phi-phi2);
> H := Kernel(phi-phi2);
> H;
Finitely generated subgroup of abelian variety with invariants [
7 ]
> A;
Modular abelian variety 43B of dimension 2, level 43 and
conductor 43^2 over Q
> A/H;
Modular abelian variety of dimension 2 and level 43 over Q
Homomorphism from 43B to modular abelian variety of dimension 2
given on integral homology by:
[ 1  0  1  0]
[ 1 -1  0 -1]
[ 1 -1 -1  1]
[ 1  1 -1  0]
Homomorphism from modular abelian variety of dimension 2 to 43B
given on integral homology by:
[ 3  1  1  2]
[ 1 -2 -2  3]
[ 4 -1 -1 -2]
[ 2 -4  3 -1]
> C := A/H;
> IsIsomorphic(A,C);
false
> IsIsomorphic(B,C);
false
> G;
Finitely generated subgroup of abelian variety with invariants [
7 ]
> H;
Finitely generated subgroup of abelian variety with invariants [
7 ]
> G eq H;
false
> G +H;
Finitely generated subgroup of abelian variety with invariants [
7, 7 ]
```

Ways to get abelian varieties isogenous to A:

1. Quotient out by any subgroup of the cuspidal subgroup.
2. Quotient out by any subgroup of the Shimura subgroup Σ. The Shimura subgroup is by definition the kernel of the natural map $J_0(N) \to J_1(N)$ induced by $X_1(N) \to X_0(N)$. Paper Ling and Oesterlé that explicitly describes Σ in computable terms directly at level N.
3. Suppose $A, B \subset J_0(M)$ are simple and non-isogenous, for some M. Then $A/(A \cap B)$ is isogenous to A.

Question 4.2. Do the three operations above suffice to enumerate all elements of *any* isogeny class?

4.2 Frank Calegari - Hope?

Frank Calegari's ideas describe the simple abelian varieties that can be isogenous to A with an isogeny whose kernel has support outside certain set of primes..

Here we make this more precise. Suppose that N is prime. Let A be a simple modular abelian variety and let f be the associated normalized newform. Denote by $\mathcal{O}$ the finite $\mathbf{Z}$-algebra generated by the coefficients of f and consider $H = \mathrm{Pic}(\mathcal{O})$. Let $S = \{\mathfrak{q}_i\}$ be a set of representatives for H such that $\mathfrak{q}_i$ has odd residual characteristic and is non-Eisenstein. Then the following proposition describes all possible simple abelian varieties that are isogenous to A with an isogeny whose kernel has support outside the Eisenstein primes and primes of residual characteristic 2.

Proposition 4.3. *Let $\varphi : A \to A'$ be an isogeny whose kernel has support outside the Eisenstein primes and primes of residual characteristic 2. Then $A' \simeq A/A[\mathfrak{q}]$ for some $\mathfrak{q} \in H$.*

How useful is that? I don't understand Eisenstein primes, so I don't know how computable this set of primes is. However, Frank's method gives us at least part of the isogeny class. We should probably run computaions to see how many non-isomorphic elements we get among $A/A[\mathfrak{q}]$ for various $q \in H$. Note that at the end of his notes Frank mentions a relation between the Eisenstein primes and non-trivial isogenies. If we can understand this, it would certainly be very useful.

5 Tables

For every factor A_f of $J_0(N)$ for $N < 1000$ and such that the computation takes at most n minutes, we used the first author's MAGMA package ... to compute the minimal degree of an isogeny from $A_f^\vee$ to A_f (and structure of kernel).

Discuss the standard magma v2.11 was distributed with some functionality but not enough... All code used to this computation using standard MAGMA 2.11 is available [[WEB SITE]].

[[Table summarizing results of the first table.]]

Also something for quotients of $J_1(N)$, for $N < 50$.

Connections with BSD. Away from 2 and minimal degree of isogeny, the order of Ш (mod maximal divisible subgroup) is a perfect square (reference [[william will find]]). Our data is consistent with [[william will find]].

Connections with computing curves X whose Jacobian is an A_f. [[Papers of people about this, and they care about whether A_f is isomorphic to its dual.]]

6 Diary (omit from final paper)

6.1 06-21-2004

done Modify MAGMA code to utilize norm equation in orders, so it will always answer "yes" or "no".

done Make sure Tseno has easy access to this new code.

done Try, using Tseno's account, to do some IsIsomorphic computations.

done Set up computation of a table.

done First draft of precise description of algorithm (high level).

6.2 06-23-2004

ok Show me result of trying to compute a table.

done List what other algorithms the main algorithm depends on. Modify modabvar.m to output log info about how it makes its decision.

Here is a list of various functions CanDetermineIsomorphism depends on (only in the case of two simple modular abelian varieties):

- IsIsogenous,
- IsSimple,
- NaturalMap,
- IsField,
- Hom,
- End,
- Generators,
- Degree,
- Dimension,
- NormEquation.
- Order
- Saturation of a submodule of $\mathbf{Z}^n$, which is basically how to compute the kernel of a matrix over Z.

I also modified modabvar.m to show us how it makes its decision. Here are the possible outcomes:

- 1 - not isogenous
- 2 - same variety
- 3 - endomorphism ring is not a field
- 4 - the degree is not a perfect square
- 5 - no solution to the norm equation
- 6 - alright, we got to the very end

done Precisely define "explicit modular abelian variety".

A **modular abelian variety** A is an abelian variety such that there is a homomorphism $A \to J_1(N)$ with finite kernel. Thus, we can give any modular abelian variety B by quotienting an abelian subvariety A of $J_1(N)$ by a finite subgroup G. In other words we represent B by giving a pair (A, G), where $G \subset A \subset J_1(N)$.

Let us now discuss how we can specify such A and G. An inclusion $A \hookrightarrow J_1(N)$ induces an inclusion on homology $H_1(A, \mathbf{Q}) \hookrightarrow H_1(J_1(N), \mathbf{Q})$ and A is completely determined by the image of $H_1(A, \mathbf{Q})$ in the vector space $H_1(J_1(N), \mathbf{Q})$. Thus we give A by defining a subspace $V = V_{\mathbf{Q}} \subset H_1(J_1(N), \mathbf{Q})$. We give G by giving finitely many elements of $V_{\mathbf{Q}}/V_{\mathbf{Z}}$, where $V_{\mathbf{Z}} = V \cap H_1(J_1(N), \mathbf{Z})$. This is because we have canonical isomorphisms $J_1(N)(\mathbf{C}) \cong H_1(J_1(N), \mathbf{R})/H_1(J_1(N), \mathbf{Z})$ and $A(\mathbf{C}) \cong V_{\mathbf{R}}/V_{\mathbf{Z}}$, so $A(\mathbf{C})_{tor} \cong V_{\mathbf{Q}}/V_{\mathbf{Z}}$.

ok Discuss examples in which interesting things happen.

Today @ 1pm.

6.3 06-23-2004

1. Write more about the algorithm for computing $\mathrm{End}(A_f)$.

done Figure out precisely why computation is getting stuck at level 173, etc.

I put various markers and it turned out that the computation is getting stuck exactly where we expected - in solving the norm equation for $[173, 2, 10]$ - probably the dimension is too big.

ok Look at Ribet's paper.

done Investigate the examples in more detail.

Look at the file examples_details.txt

ok Run computation of table for levels up to 500 and dimension at most 5.

Almost done but it is starting to look strange after some point.

6.4 06-30-2004

1. Saturation: 1. See if MAGMA says how they do it (NO). 2. Look in Cohen to see how to find integer kernels. Answer: Here's algorithm.

   (a) Find echelon form of basis of lattice.

   (b) Write down matrix over $\mathbf{Z}$ that has saturation of lattice as kernel.

   (c) Find the kernel using algorithm 2.7.2 of Cohen's book (Kernel over $\mathbf{Z}$ using LLL).

   Complexity? Probably dominated by LLL step... ??

2. Investigate in detail what PARI can do regarding solving norm equations. 1. Start pari and type '?6'. 2. Looks in users.dvi and see what PARI can do. Does it solve norm equations at all? Yes. 3. Does it solve diophantine norm equation, i.e., solutions in $\mathcal{O}_K$? 4. Does it solve diophantine norm equation, i.e., solutions in order $\mathcal{O}$? 5. Does it give ALL solutions or just one? 6. What algorithm?

3. Decide on a computational goal for the project. (REMEMBER to use new version!!)
   (a) Determine what degree gets too difficult.
   (b) Determine whether A is isomorphic to $A^\vee$ for factors $A = A_f$ of $J_0(N)$, for $N \leq 500$ and $\dim(A_f) < 10$.
   (c) Determine piece of isogeny class of A for factors $A = A_f$ of $J_0(N)$, for $N \leq 100$.
   (d) Determine whether A is isomorphic to $A^\vee$ for factors $A = A_f$ of $J_1(N)$, for $N \leq 50$ and $\dim(A_f) < 10$.

4. Generating up isogeny class systematically.

   (a) How to compute the Shimura subgroup Σ?!: Definition: $\Sigma = \mathrm{Ker}(J_0(N) \to J_1(N))$.

      i. kernel to higher level

      ii. ling-oesterle (****)

      iii. Compute kernel directly?

   (b) Suppose G is a subgroup of $J_0(N)$ defined over $\mathbf{Q}$. Then we get abelian varieties isogenous to A from $A/(A[n] \cap G)$ for any integer n. For example $A^\perp$ is got from $G = A \cap B$, where B is the Hecke-stable complement of A in $J_0(N)$.

   (c) Sources of G:

      i. Quotient by subgroups of cuspidal subgroup

      ii. Shimura subgroup,

      iii. intersecting with other abvars

      iv. dual.

v. Map to higher level then intersection with other abelian varieties of higher level.

(d) Specifying each element of the isogeny class. Need notation. $A = A_f$ is the subvariety of $J_0(N)$. Examples: $B = A/C[3]$, where C is cuspidal subgroup. $B = A/\langle(3) - (1/7)\rangle$, or $B = A/(A \cap A_g)$, where g is another newform. $B = A/\Sigma[2]$.

5. Write up something about finding minimal degree of isogeny. square free part business....

6.5 07-24-2004

1. Look over new proofs.

2. Figure out how to compute saturations. (1) prove Allan Steel's simple algorithm (why HNF?) Try (1) in MAGMA. (2) Look at what NTL does to compute kernels.

3. Decide on and set up a systematic computation, write it and start it running. Everything up to level 1000, but time out computations after 10 minutes. (William.)

4. Talk about your short talk on Monday (when? what?)

   - solved the "minimal degree problem"

   - discuss some examples at length illustrating what's going on

   - briefly explain future directions.

   - more motivation (?) e.g., enumerating isogeny classes to get a higher dimensional cremona; bsd sha order,...

5. Norm equation – how much to write up. References. Search MSN. Look in book... ???

6. Figure out *exactly* what else we need to do to completely finish this paper. Assign tasks:

   (a) (Stein) Write introduction.

   (b) (Stein) Write enumerating section.

   (c) (Stein) Say something about complexity somewhere???

   (d) (Tseno) Rewrite proof of isogeny testing algorithm.

7. Make a list of problems for future investigation: polarization, enumerating the isogeny class, working over other number fields, isomorphism testing in the non-simple case.

7 Polarization

We can decide whether A is isomorphic to $A^\vee$. Can we decide if A is principally polarized!? The point is that a principal polarization is an isomorphism that arises from a divisor class...

References

[Rib92] K. A. Ribet, *Abelian varieties over* $\mathbf{Q}$ *and modular forms*, Algebra and topology 1992 (Taejŏn), Korea Adv. Inst. Sci. Tech., Taejŏn, 1992, pp. 53–79. MR 94g:11042

[Ser87] J-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.