Some Abelian Varieties with Visible Shafarevich-Tate Groups

William Stein*

May 28, 1999

Abstract

We give examples of abelian variety quotients of the modular jacobian $J_0(N)$ with nontrivial visible Shafarevich-Tate groups. In computing these examples we developed formulas for invariants of higher dimensional modular abelian varieties.

Introduction

In [4] Cremona and Mazur studied visibility of Shafarevich-Tate groups of elliptic curves $E \subset J_0(N)$. This paper extends some of these computations to higher dimensional $A \subset J_0(N)$. For each $N \leq 1001$ and $N = 1028, 1061$, we compute the analytic rank 0 new optimal A in $J_0(N)$ having nontrivial odd visible Shafarevich-Tate group, visible in the new part of $J_0(N)$. A total of 19 such A were found having Ш of order the squares of: $3, 5, 7, 3^2, 11, 13, 151$. Our computations say little about invisible elements of Ш, however see [1]. The algorithms developed for computing invariants of modular abelian varieties are also of some interest.

Acknowledgment: It is a pleasure to thank Barry Mazur for his brilliant lectures on visibility, Ken Ribet and Robert Coleman for explaining monodromy, and John Cremona for explaining modular symbols. The author would also like to thank Richard Taylor and Loic Merel for comments, and Amod Agashe for many useful discussions and proving Theorem 2.7.

Notation

Let $S_2(N) = S_2(\Gamma_0(N), \mathbf{C})$ be the space of cusp forms of weight 2 for the subgroup $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbf{Z})$. Thus $S_2(N)$ can be identified with the differentials on the modular curve $X_0(N)$. Let $J_0(N)$ denote the jacobian of $X_0(N)$. Denote by $H_1(X_0(N), \mathbf{Z})$ the integral homology of $X_0(N)$. The Hecke algebra $\mathbf{T}$ acts in a compatible manner on $S_2(N)$, $H_1(X_0(N), \mathbf{Z})$ and $J_0(N)$. The letters f and g

*Amod Agashe will be a joint author of this paper as soon as he has had a chance to agree with what it says.

are reserved for newforms, i.e., normalized eigenforms for $\mathbf{T}$ in the complement of the old subspace of $S_2(N)$. Let $f_1, \dots, f_d$ denote the Galois conjugates of f, and $I_f = \mathrm{Ann}(f)$ the annihilator of f in $\mathbf{T}$.

1 Optimal abelian varieties and newforms

An abelian variety quotient of $J_0(N)$ is called **optimal** if the kernel is connected. We associate to f an optimal quotient A_f of $J_0(N)$:

$$0 \to I_f J_0(N) \to J_0(N) \to A_f \to 0.$$

Let $H = H_1(X_0(N), \mathbf{Z})$, $S_2 = S_2(N)$, and recall that integration defines a non-degenerate pairing $S_2 \times H \to \mathbf{C}$, hence a map $H \to \mathrm{Hom}_{\mathbf{C}}(S_2, \mathbf{C})$. Composing with restriction to $S_2[I_f]$ defines a map $\Phi_f : H \to \mathrm{Hom}(S_2[I_f], \mathbf{C})$.

Theorem 1.1. *A_f is an abelian variety of dimension d with canonical L-series*

$$L(A_f, s) = \prod_{i=1}^{d} L(f_i, s).$$

The complex uniformization of the tori $A_f(\mathbf{C})$ and $A_f^\vee(\mathbf{C})$ is described by the following diagram

$$\begin{array}{ccccc}
0 & & 0 & & 0 \\
\downarrow & & \downarrow & & \downarrow \\
H[I_f] & \longrightarrow & H & \longrightarrow & \Phi_f(H) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Hom}(S_2, \mathbf{C})[I_f] & \longrightarrow & \mathrm{Hom}(S_2, \mathbf{C}) & \longrightarrow & \mathrm{Hom}(S_2[I_f], \mathbf{C}) \\
\downarrow & & \downarrow & & \downarrow \\
A^\vee(\mathbf{C}) & \longrightarrow & J_0(N)(\mathbf{C}) & \longrightarrow & A(\mathbf{C}) \\
\downarrow & & \downarrow & & \downarrow \\
0 & & 0 & & 0
\end{array}$$

in which the vertical columns are exact but the rows are not.

Proof. [16] and section 1.7 of [5]. □

1.1 The Birch and Swinnerton-Dyer Conjecture

Let $\mathcal{A}/\mathbf{Z}$ be the Neron model of $A = A_f$. The **Tamagawa number** c_p is the number of $\mathbf{F}_p$-rational components of the special fiber $\mathcal{A}_{\mathbf{F}_p}$. A basis $h_1, \dots, h_d$ for the Neron differentials defines a measure μ on $A(\mathbf{R})$ and we let $\Omega_{\mathcal{A}} = \mu(A(\mathbf{R}))$. Let $w : H^1(\mathbf{Q}, A) \to \prod_v H^1(\mathbf{Q}_v, A)$ and set $\text{Ш} = \mathrm{Ker}(w)$. If $L(A, 1) \neq 0$ it is known [9] that $A(\mathbf{Q})$ and $\text{Ш}(A)$ are both finite. One then has the following fundamental and still open

Conjecture 1.2 (Birch, Swinnerton-Dyer, Tate).

$$L(A, 1) = \Omega_{\mathcal{A}} \cdot \frac{|\text{Ш}| \cdot \prod_{p|N} c_p}{|A(\mathbf{Q})| \cdot |A^\vee(\mathbf{Q})|}.$$

1.2 The Manin Constant

Let $S_f(\mathbf{C}) \subset S_2(N, \mathbf{C})$ denote the subspace of cusp forms spanned by the conjugates of f. There are two lattices in $S_f(\mathbf{C})$. One is the lattice $S_f(\mathbf{Z})$ of cusp forms with integer Fourier expansion at infinity. The other $S_f(\mathcal{A}/\mathbf{Z})$ is got by pulling back the Neron differentials defined above. The **Manin constant** is

$$c_f = [S_f(\mathbf{Z}) : S_f(\mathcal{A}/\mathbf{Z})].$$

We are aware of no examples of *newforms* f for which $c_f \neq 1$. It is reasonable to expect that one can extend methods known for elliptic curves (e.g., [11]) to show that c_f is at least coprime to $2N$.

Later in this paper we give a formula for $L(A_f, 1)/\Omega_f$ where Ω_f is computed using the lattice $S_f(\mathbf{Z})$. Thus our BSD special value is off by the Manin constant. For the remainder of this paper we officially assume

Conjecture 1.3. $c_f = 1$

1.3 Connecting Mordell-Weil and Shafarevich-Tate

Let $f, g \in S_2(N)$ be nonconjugate newforms and A_f, A_g the corresponding optimal quotients of $J_0(N)$. Let $\mathfrak{m} \subset \mathbf{T}$ be a maximal ideal such that $A_f^\vee[\mathfrak{m}] = A_g^\vee[\mathfrak{m}] \subset J_0(N)$. Let p be the residue characteristic of $\mathfrak{m}$. Assume that $p \nmid 2N \cdot \prod_{p|N} c_p c'_p$ where c'_p are the Tamagawa numbers of A_g.

Under hypothesis such as these we expect there to be a commutative diagram

$$\begin{array}{ccccccccc}
0 & \to & A_f(\mathbf{Q})/\mathfrak{m}A_f(\mathbf{Q}) & \to & X & \to & Ш(A_f)[\mathfrak{m}] & \to & 0 \\
 & & & & || & & & & \\
0 & \to & A_g(\mathbf{Q})/\mathfrak{m}A_g(\mathbf{Q}) & \to & X & \to & Ш(A_g)[\mathfrak{m}] & \to & 0
\end{array}$$

with exact rows. Here X is an abelian group, $H^1(\operatorname{Spec}\mathbf{Z}, A_f[\mathfrak{m}])$. A precise statement will not be given here as the purpose of this paper is merely to present a few algorithms and computational results.

2 Algorithms

2.1 Modular Symbols

Modular symbols give a presentation of the homology of the modular curve $X_0(N)$. Here we briefly review modular symbols for $\Gamma_0(N)$. More information on how to actually compute with them can be found in [3], [7], and [12].

Define the space of **modular symbols** $\underline{\mathcal{M}}(N, \mathbf{Z})$ to be the *free* abelian group generated by symbols $\{\alpha, \beta\}$ such that $\alpha, \beta \in \mathbf{P}^1(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\}$ subject to the relations

$$\begin{aligned}
0 &= \{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\}, \\
\{\alpha, \beta\} &= \{g(\alpha), g(\beta)\}, \quad \text{all } g \in \Gamma_0(N).
\end{aligned}$$

The space of **boundary symbols** $\underline{\mathcal{B}}(N, \mathbf{Z})$ is the free abelian group generated by symbols $\{\alpha\}$, $\alpha \in \mathbf{P}^1(\mathbf{Q})$, modulo the relations

$$\{\alpha\} = \{g(\alpha)\}, \quad \text{all } g \in \Gamma_0(N).$$

The **cuspidal symbols** $\underline{\mathcal{S}}(N, \mathbf{Z})$ are the kernel of the boundary map $\partial(\{\alpha, \beta\}) = \{\beta\} - \{\alpha\}$:

$$0 \to \underline{\mathcal{S}}(N, \mathbf{Z}) \to \underline{\mathcal{M}}(N, \mathbf{Z}) \xrightarrow{\partial} \underline{\mathcal{B}}(N, \mathbf{Z}).$$

The Hecke algebra act on $\underline{\mathcal{M}}(N, \mathbf{Z})$ and there is an involution $*\{\alpha, \beta\} = \{-\alpha, -\beta\}$. Integration defines a pairing

$$S_2(N) \times \underline{\mathcal{M}}(N, \mathbf{Z}) \to \mathbf{C}.$$

The Manin-Drinfeld theorem asserts that the image of $\underline{\mathcal{M}}(N, \mathbf{Z})$ in $\mathrm{Hom}(S_2(N), \mathbf{C})$ is a lattice. There is a natural isomorphism between $\underline{\mathcal{S}}(N, \mathbf{Z})$ and $H_1(X_0(N), \mathbf{Z})$.

2.2 The Method of Graphs

We briefly review the method of graphs, see [13] and [15] for more details. Let M be a positive integer, p a prime not dividing M, and put $N = pM$. Let D be the finitely generated free abelian group on the superingular points of $X_0(M)(\overline{\mathbf{F}}_p)$, i.e., the enhanced elliptic curves $\mathbf{E} = (E, C)$ where E is a supersingular elliptic curve defined over $\overline{\mathbf{F}}_p$ and C is a cyclic subgroup of order M, and enhanced curves are identified if they are isomorphic in the evident way. Let $w_{\mathbf{E}} = \frac{|\mathrm{Aut}(\mathbf{E})|}{2}$ where $\mathrm{Aut}(\mathbf{E})$ is the group of $\overline{\mathbf{F}}_p$-automorphisms of $\mathbf{E}$. We have $w_{\mathbf{E}} \leq 12$ and if $p \geq 5$ then $w_{\mathbf{E}} \leq 3$. The **monodromy pairing** on D is

$$\langle \mathbf{E}, \mathbf{E}' \rangle = \begin{cases} w_{\mathbf{E}} & \text{if } \mathbf{E} = \mathbf{E}' \\ 0 & \text{if } \mathbf{E} \neq \mathbf{E}' \end{cases}$$

The Hecke operators act on D in a way compatible with this pairing. Define

$$X_{N,p} = \{\sum a_{\mathbf{E}} \mathbf{E} : \sum a_{\mathbf{E}} = 0\}$$

It is known that $X_{N,p} \otimes \mathbf{C}$ is isomorphic as a Hecke module to the subspace of $S_2(N, \mathbf{C})$ generated by newforms and oldforms of level pd for $d|M$.

David Kohel [8] has implimented an algorithm which computes the action of the Hecke operators on $X_{N,p}$ using the arithmetic of quaternion algebras.

2.3 Enumerating quotients of $J_0(N)$

It is necessary to list all newforms of a given level N. This can be done by decomposing the new subspace of the modular symbols $\underline{\mathcal{S}}(N, \mathbf{Q})$ using the Hecke operators. The characteristic polynomial of T_2 is computed, and then T_2 is used to break up the space. The process is applied recursively with $T_3, T_5, \ldots$ until it terminates. After computing the decomposition we order the newforms as suggested by Cremona: First by dimension. Within each dimension, in binary by the signs of the Atkin-Lehner involutions, e.g., $+++$, $++-$, $+-+$, $+--$, $-++$, etc. When two forms have the same involutions, order by $|\operatorname{Tr}(a_p)|$ with ties broken by taking the positive trace first. For historical reasons this does not always agree with the ordering in Cremona's tables (page 5 of [3]). There is only one case in our table in which the two ordering schemes disagree, our **446B** is Cremona's **446D**.

2.4 The Modular Polarization

A polarization of an abelian variety A is an isogeny between A and its dual arising from a very amply invertible sheaf (see [14]). $J_0(N)$ is a Jacobian so it possesses a canonical polarization arising from the θ-divisor and this induces the **modular polarization** $\theta_f : A_f^\vee \to A_f$.

$$\begin{tikzcd}
A_f^\vee \arrow[r] \arrow[dr, "\theta_f"] & J_0(N) \arrow[d] \\
& A_f
\end{tikzcd}$$

By ([14], Theorem 13.3) $\deg(\theta_f)$ is a perfect square so we may define the **modular degree** $\delta_f = \sqrt{\deg(\theta_f)}$. The kernel of θ_f is the intersection of $A_f^\vee$ with $I_f J_0(N)$ so it measure intersections between $A_f^\vee$ and other factors of $J_0(N)$.

Proposition 2.1. *With notation as in Theorem 1.1,*

$$\operatorname{Ker}(\theta_f) \cong \operatorname{Coker}(H[I_f] \to \Phi_f(H))$$

Proof. Delete the middle column of the diagram in Theorem 1.1 and apply the snake lemma. □

Using Lemma 2.5, to be proved later, we see that the modular degree can be computed as follows: Let $\varphi_1, \ldots, \varphi_{2d}$ be a basis for $\operatorname{Hom}(H, \mathbf{Z})[I_f]$ and $a_1, \ldots, a_{2d}$ a basis for $H[I_f]$. Then δ_f is the square root of the absolute value of the determinant of the matrix $(\varphi_i(a_j))$.

2.5 Torsion

We can obtain both upper and lower bounds on $A_f(\mathbf{Q})_{\mathrm{tor}}$ and $A_f^\vee(\mathbf{Q})_{\mathrm{tor}}$. For the examples considered in our table these bounds were sufficient to determine the odd parts of these groups. Let $\chi_p(X) \in \mathbf{Z}[X]$ denote the characteristic polynomial of T_p acting on A_f. It is a polynomial having integer coefficients and degree equal to $\dim A_f$.

Proposition 2.2. *Both* $|A_f(\mathbf{Q})_{\mathrm{tor}}|$ *and* $|A_f^\vee(\mathbf{Q})_{\mathrm{tor}}|$ *divide*

$$\gcd\{\chi_p(p+1) : (p, 2N) = 1,\ p \text{ prime}\}.$$

Proof. Use the Eichler-Shimura relation and injectivity of rational torsion under reduction modulo an odd prime p (since $1 = e < p - 1$). □

The difference of cusps $\alpha, \beta \in X_0(N)$ define a point $(\alpha) - (\beta) \in J_0(N)(\mathbf{C})$.

Proposition 2.3. *The order of the image of* $(\alpha) - (\beta)$ *in* $A_f(\mathbf{C})$ *equals the order of the image of the modular symbol* $\{\alpha, \beta\}$ *in*

$$\frac{\Phi_f(\underline{\mathcal{M}}(N, \mathbf{Z}))}{\Phi_f(\underline{\mathcal{S}}(N, \mathbf{Z}))}.$$

Proof. By the classical Abel-Jacobi theorem ([10], ch IV, Theorem 2.2), the modular symbol $\{\alpha, \beta\}$ maps, via the period map, to the point $(\alpha) - (\beta) \in J_0(N)(\mathbf{C})$. Now use Theorem 1.1. □

In particular, the point $(0) - (\infty) \in J_0(N)(\mathbf{Q})$ generates a cyclic subgroup of $A_f(\mathbf{Q})$ and this gives a lower bound on $A_f(\mathbf{Q})_{\mathrm{tor}}$.

2.6 Component Groups

Let p be a prime exactly dividing N and $\Phi_{A,p}$ the component group of $A = A_f$. Thus we have the exact sequence

$$0 \to \mathcal{A}^0_{\mathbf{F}_p} \to \mathcal{A}_{\mathbf{F}_p} \to \Phi_{A,p} \to 0$$

with $\mathcal{A}$ the Neron model of A and $\mathcal{A}^0_{\mathbf{F}_p}$ connected. Let $X[I_f]$ be the submodule of $X = X_{N,p}$ cut out by the annihilator of f. The monodromy pairing defines a map $X \to \mathrm{Hom}(X[I_f], \mathbf{Z})$. Let δ_f be the modular degree and w_p the sign of the Atkin-Lehner involution W_p on f. The following will be proved in [18].

Theorem 2.4.

$$\begin{aligned} |\Phi_{A,p}(\overline{\mathbf{F}}_p)| &= \delta_f \cdot \frac{|\operatorname{Coker}(X \to \mathrm{Hom}(X[I_f], \mathbf{Z}))|^2}{\operatorname{Disc}(X[I_f] \times X[I_f] \to \mathbf{Z})}, \\ |\Phi_{A,p}(\mathbf{F}_p)| &= \begin{cases} |\Phi_{A,p}(\overline{\mathbf{F}}_p)| & w_q = -1 \\ |\Phi_{A,p}(\overline{\mathbf{F}}_p)[2]| & w_q = +1 \end{cases} \end{aligned}$$

2.7 Rational part of the special value

Let $\underline{\mathcal{M}}(\mathbf{Q}) = \underline{\mathcal{M}}(N, \mathbf{Q})$ and extend Φ_f to a map $\underline{\mathcal{M}}(\mathbf{Q}) \to \mathbf{C}$. Then Φ_f has a rational structure in the following sense.

Lemma 2.5. *Let* $\varphi_1, \ldots, \varphi_n$ *be a* $\mathbf{Q}$*-basis for* $\mathrm{Hom}(\underline{\mathcal{M}}(\mathbf{Q}), \mathbf{Q})[I_f]$ *and set*

$$\Psi = \varphi_1 \times \cdots \times \varphi_n : \underline{\mathcal{M}}(\mathbf{Q}) \to \mathbf{Q}^n.$$

Then $n = 2d$ *and* $\mathrm{Ker}(\Psi) = \mathrm{Ker}(\Phi_f)$.

Proof. This result is due to Shimura ([17]), but we sketch a proof. To compute $\dim \mathrm{Hom}(\underline{\mathcal{M}}(\mathbf{Q}), \mathbf{Q})[I_f]$ we may first tensor with $\mathbf{C}$. Let $\overline{S}_2$ denote the weight 2 anti-holomorphic cusp forms and E_2 the weight 2 Eisenstein series for $\Gamma_0(N)$. Then $\underline{\mathcal{M}}(\mathbf{C})$ is isomorphic as a $\mathbf{T}$-module to $S_2 \oplus \overline{S}_2 \oplus E_2$ (prop. 9 of [12] and the Eichler-Shimura embedding). Because of the Peterson inner product, the dual $\mathrm{Hom}(\underline{\mathcal{M}}(\mathbf{C}), \mathbf{C})$ is also isomorphic as a $\mathbf{T}$-module to $S_2 \oplus \overline{S}_2 \oplus E_2$. Since f is new, by the Atkin-Lehner multiplicity one theory,

$$(S_2 \oplus \overline{S}_2 \oplus E_2)[I_f] = S_2[I_f] \oplus \overline{S}_2[I_f]$$

has complex dimension $2d$, which gives the first assertion.

Next note that $\mathrm{Ker}(\Phi_f) \otimes \mathbf{C} \subset \mathrm{Ker}(\Psi) \otimes \mathbf{C}$ because each map $x \mapsto \langle f_i, x\rangle$ lies in $\mathrm{Hom}(\underline{\mathcal{M}}(\mathbf{Q}), \mathbf{C})[I_f]$ and $\mathrm{Ker}(\Psi) \otimes \mathbf{C}$ is the intersection of the kernels of *all* maps in $\mathrm{Hom}(\underline{\mathcal{M}}(\mathbf{Q}), \mathbf{C})[I_f]$. By Theorem 1.1 the image of Φ_f is a lattice, so $\dim_{\mathbf{Q}} \mathrm{Ker}(\Phi_f) = \dim_{\mathbf{Q}} \underline{\mathcal{M}}(\mathbf{Q}) - 2d$. Since Ψ is the intersection of the kernels of $n = 2d$ independent linear functionals $\varphi_1, \dots, \varphi_n$, $\mathrm{Ker}(\Psi)$ also has dimension $\dim \underline{\mathcal{M}}(\mathbf{Q}) - 2d$. Since the dimensions are the same and there is an inclusion, we have an equality $\mathrm{Ker}(\Phi_f) \otimes \mathbf{C} = \mathrm{Ker}(\Psi) \otimes \mathbf{C}$ which forces $\mathrm{Ker}(\Phi_f) = \mathrm{Ker}(\Psi)$. □

Let V be a finite dimensional vector space over $\mathbf{R}$. A **lattice** $L \subset V$ is a free abelian group of rank $= \dim V$ such that $\mathbf{R}L = V$. If $L, M \subset V$ are lattices, the **lattice index** $[L : M]$ is the absolute value of the determinant of an automorphism of V taking L isomorphically onto M. Extend the definition to the case when M has rank strictly smaller than $\dim V$ by defining $[L : M] = 0$.

Lemma 2.6. *Suppose $\tau_i : V \to W_i$, $i = 1, 2$ are surjective linear maps such that $\mathrm{Ker}(\tau_1) = \mathrm{Ker}(\tau_2)$. Then*

$$[\tau_1(L) : \tau_1(M)] = [\tau_2(L) : \tau_2(M)].$$

Proof. Surjectivety and equality of kernels insures that there is a unique isomorphism $\iota : W_1 \to W_2$ such that $\iota\tau_1 = \tau_2$. Let σ be an automorphism of W_1 such that $\sigma(\tau_1(L)) = \tau_1(M)$. Then

$$\iota\sigma\iota^{-1}(\tau_2(L)) = \iota\sigma\tau_1(L) = \iota\tau_1(M) = \tau_2(M).$$

Since conjugation doesn't change the determinant,

$$[\tau_2(L) : \tau_2(M)] = |\det(\iota\sigma\iota^{-1})| = |\det(\sigma)| = [\tau_1(L) : \tau_1(M)].$$

□

Let $S_2(N, \mathbf{Z})$ be the space of cusp forms whose q-expansion at infinity hass integer coefficients. Let Ω_f^0 be the measure of the identity component of $A_f(\mathbf{R})$ with respect to an integral basis for $S_f(\mathbf{Z}) = S_2(N, \mathbf{Z})[I_f]$. Let $\mathbf{e} = \{0, \infty\} \in \underline{\mathcal{M}}(N, \mathbf{Z})$ denote the **winding element**.

Theorem 2.7. *Let Ψ be as in Lemma 2.5. Then*

$$\pm\frac{L(A_f, 1)}{\Omega_f^0} = [\Psi(\underline{\mathcal{S}}(N, \mathbf{Z})^+) : \Psi(\mathbf{Te})]$$

Proof. Let $\Phi = \Phi_f$ be the period map defined by a basis $f_1, \dots, f_d$ of conjugate newforms. The image of Φ, which we identify with $\mathbf{C}^d$, is an algebra with unit element $\mathbf{1} = (1, \dots, 1)$ equipped with an action of the Hecke operators: T_p acts as $(a_p^{(1)}, \dots, a_p^{(d)})$ where the components are the Galois conjugates of a_p. Let $\mathbf{Z}^d \subset \mathbf{R}^d \subset \mathbf{C}^d$ be the usual submodules. Let $\mathrm{Vol}(\underline{\mathcal{S}}^+)$ be the volume of the image of $\underline{\mathcal{S}}^+ = \underline{\mathcal{S}}(N, \mathbf{Z})^+$ under Φ. Observe that $\mathrm{Vol}(\underline{\mathcal{S}}^+) = [\mathbf{Z}^d : \Phi(\underline{\mathcal{S}}^+)]$ and $|L(A_f, 1)| = [\mathbf{Z}^d : \Phi(\mathbf{e})\mathbf{Z}^d]$. Let $W \subset \mathbf{C}^d$ be the $\mathbf{Z}$-module spanned by the columns of a basis for $S_f(\mathbf{Z})$. Because Ω_f^0 is computed with respect to a basis for $S_f(\mathbf{Z})$,

$$\mathrm{Vol}(\underline{\mathcal{S}}^+) = [W : \mathbf{T1}] \cdot \Omega_f^0.$$

Because $S_2(N, \mathbf{Z})$ is saturated, $[\mathbf{Z}^d : W] = 1$ so $[\mathbf{Z}^d : \mathbf{T1}] = [W : \mathbf{T1}]$. The following calculation involves lattices in $\mathbf{R}^d$:

$$\begin{aligned}
[\Phi(\underline{\mathcal{S}}^+) : \Phi(\mathbf{Te})] &= [\Phi(\underline{\mathcal{S}}^+) : \mathbf{Z}^d] \cdot [\mathbf{Z}^d : \Phi(\mathbf{Te})] \\
&= \frac{1}{[\mathbf{Z}^d : \Phi(\underline{\mathcal{S}}^+)]} \cdot [\mathbf{Z}^d : \Phi(\mathbf{Te})] \\
&= \frac{1}{\mathrm{Vol}(\underline{\mathcal{S}}^+)} \cdot [\mathbf{Z}^d : \Phi(\mathbf{e})\mathbf{Z}^d] \cdot [\Phi(\mathbf{e})\mathbf{Z}^d : \Phi(\mathbf{Te})] \\
&= \frac{|L(A_f, 1)|}{\mathrm{Vol}(\underline{\mathcal{S}}^+)} \cdot [\Phi(\mathbf{e})\mathbf{Z}^d : \Phi(\mathbf{Te})] \\
&= \frac{|L(A_f, 1)|}{\mathrm{Vol}(\underline{\mathcal{S}}^+)} \cdot [\Phi(\mathbf{e})\mathbf{Z}^d : \Phi(\mathbf{e})\mathbf{T1}] \\
&= \frac{|L(A_f, 1)|}{\Omega_f^0 \cdot [W : \mathbf{T1}]} \cdot [\mathbf{Z}^d : \mathbf{T1}] \\
&= \frac{|L(A_f, 1)|}{\Omega_f^0}.
\end{aligned}$$

The theorem now follows from lemmas 2.5, 2.6, and the fact that f has real Fourier coefficients so $L(A_f, 1) \in \mathbf{R}$ hence $|L(A_f, 1)| = \pm L(A_f, 1)$.

$\square$

Corollary 2.8. *Let n_f be the order of the image in $A_f(\mathbf{Q})$ of the point $(0) - (\infty) \in J_0(N)(\mathbf{Q})$. Then*

$$\frac{L(A_f, 1)}{\Omega_f^0} \in \frac{1}{n_f}\mathbf{Z}.$$

Proof. Let x denote the image of $(0) - (\infty) \in A_f(\mathbf{Q})$ and set $I = \mathrm{Ann}(x) \subset \mathbf{T}$. Since f is a *newform* the Hecke operators T_p for $p|N$ act as 0 or ± 1 on $A_f(\mathbf{Q})$ (end of section 6 of [6]). If $p \nmid N$ a standard calculation (section 2.8 of [3]) combined with the Abel-Jacobi theorem shows that $T_p(x) = (p+1)x$. Let $C = \mathbf{Z}x$ denote the (finite, by Manin-Drinfeld) cyclic subgroup of $A_f(\mathbf{Q})$ generated by x, so n_f is the order of C. There is an injection $\mathbf{T}/I \hookrightarrow C$ sending T_p to

$T_p(x)$. By the theorem, we have

$$\begin{aligned}\pm L(A_f,1)/\Omega_f^0 &= [\Psi(\underline{\mathcal{S}}^+):\Psi(\mathbf{T}e)]\\ &= [\Psi(\underline{\mathcal{S}}^+):\Psi(I\mathbf{e})]\cdot[\Psi(I\mathbf{e}):\Psi(\mathbf{T}\mathbf{e})]\\ &= [\Psi(\underline{\mathcal{S}}^+):I\Psi(\mathbf{e})]\cdot[I\Psi(\mathbf{e}):\mathbf{T}\Psi(\mathbf{e})]\\ &= \frac{[\Psi(\underline{\mathcal{S}}^+):I\Psi(\mathbf{e})]}{[\mathbf{T}\Psi(\mathbf{e}):I\Psi(\mathbf{e})]}\in\frac{1}{n_f}\mathbf{Z}.\end{aligned}$$

The final inclusion follows from two observations. By Abel-Jacobi, I is exactly those elements of $\mathbf{T}$ which send $\Psi(\mathbf{e})$ into $\Psi(\underline{\mathcal{S}}^+)$, so $[\Psi(\underline{\mathcal{S}}^+) : I\Psi(\mathbf{e})] \in \mathbf{Z}$. Second, there is a surjective map

$$\mathbf{T}/I \to \frac{\mathbf{T}\Psi(\mathbf{e})}{I\Psi(\mathbf{e})}$$

sending t to $t\Psi(\mathbf{e})$, so $[\mathbf{T}\Psi(\mathbf{e}) : I\Psi(\mathbf{e})]$ divides $n_f = |C| = |\mathbf{T}/I|$. □

2.8 Intersections

Let f, g be nonconjugate newforms and $H = H_1(X_0(N), \mathbf{Z})$.

Proposition 2.9. $(A_f^\vee \cap A_g^\vee)[p] \neq 0$ *iff the mod p rank of $H[I_f] + H[I_g]$ is strictly less than* $\operatorname{rank} H[I_f] + \operatorname{rank} H[I_g]$.

Proof. By (1.1) $\Lambda_f = H[I_f]$ (resp., $\Lambda_g = H[I_g]$) is the submodule of H which defines A_f (resp., A_g). By reduction mod p we mean the map $H \to H \otimes \mathbf{F}_p$. Suppose

$$\operatorname{rank}(\Lambda_f + \Lambda_g) \bmod p < \operatorname{rank}\Lambda_f + \operatorname{rank}\Lambda_g.$$

Since Λ_f (resp., Λ_g) is a kernel, it is saturated, so $\operatorname{rank}\Lambda_f \bmod p = \operatorname{rank}\Lambda_f$ (resp., for Λ_g). We conclude that the mod p linear dependence must involve vectors from both Λ_f and Λ_g; there is $v \in \Lambda_f$ and $w \in \Lambda_g$ so that $v, w \not\equiv 0 \bmod p$ but $v + w \equiv 0 \bmod p$. Thus $\frac{v+w}{p} \in H$ is integral, i.e., in $J_0(N)(\mathbf{C})$ we have $\frac{1}{p}v - (-\frac{1}{p}w) = 0$. But $\frac{1}{p}v \notin \Lambda_f$ and $\frac{1}{p}w \notin \Lambda_g$ (otherwise v and w would be $0 \bmod p$), so $\frac{1}{p}v$ and $-\frac{1}{p}w$ are both nontrivial p-torsion in $A_f^\vee$, $A_g^\vee$, resp. Conclusion: $0 \neq \frac{1}{p}v = -\frac{1}{p}w \in (A_f^\vee \cap A_g^\vee)[p]$.

Conversely, suppose $0 \neq x \in (A_f^\vee \cap A_g^\vee)[p]$. Choose lifts modulo H to $x_f \in \frac{1}{p}\Lambda_f$ and $x_g \in \frac{1}{p}\Lambda_g$. Then $px_f \in \Lambda_f$ (resp., $px_g \in \Lambda_g$), but $px_f \notin pH$ (resp., $px_g \notin pH$) because $x \neq 0$. Since $x_f - x_g \in H$, $px_f - px_g = p(x_f - x_g) \equiv 0 \bmod p$. This is a nontrivial linear relation between Λ_f and Λ_g. □

Corollary 2.10. *If $p > 2$ and the sign of some Atkin-Lehner involution for f is different than that for g then $(A_f^\vee \cap A_g^\vee)[p] = 0$.*

Proof. Suppose $w_q(f) \neq w_q(g)$ and let $G = (A_f^\vee \cap A_g^\vee)[p]$. Observe that W_q acts as $w_q(f) \bmod p$ on $A_f^\vee[p]$ and as $w_q(g) \bmod p$ on $A_g^\vee[p]$. Hence W_q acts as both $w_q(f) \bmod p$ and $w_q(g) \bmod p$ on G. Since $p > 2$, this is not possible when $G \neq 0$. □

3 Results

This section contains tables computed using the above algorithms as implimented in the author's program `HECKE` (a `C++` program using `LiDIA` and `NTL`), David Kohel's `Magma` software, and `PARI`. Each factor A_f of $J_0(N)$ is denoted as follows:

N isogeny-class dimension

The dimension frequently determines the factor, so it is included in the notation. We consider only the odd part of Ш so we only computed the odd parts of the arithmetic invariants of A_f. Thus at this point we make the

WARNING: ONLY ODD PARTS OF INVARIANTS ARE GIVEN!

Tables 1-3: New Visible Ш
Let n_f be the largest odd square dividing the numerator of $L(A_f,1)/\Omega_f$. Table 1 lists those A_f such that, for $p|n_f$ there exists a *new* factor B_g of $J_0(N)$, of positive analytic rank, and such that $(A_f^\vee \cap B_g^\vee)[p] \neq 0$. This is necessary (and usually sufficient) for the p-torsion in the new visible part of Ш to be nonzero. In many cases it could be seen that there were no other appropriate new factors by looking at the signs of the Atkin-Lehner involutions. Up to level 1001 our search was systematic. The two examples after level 1001 were not found by systematic search (i.e., there may be a gap). In those cases for which $4|N$, we put $c_2 = a$, as we don't know how to compute c_2 exactly when the reduction is additive. Table 2 contains further arithmetic information about each explanatory factor.

The explanatory factors of level ≤ 1028 are *exactly* the set of rank 2 elliptic curves of level ≤ 1028. By [2], the explanatory factor at level 1061 is the first surface of rank 4 (and prime level).

Table 4: Component groups
Table 4 gives the quantities involved in the formula for Tamagawa numbers, for each of the A_f from table 1.

Table 5: Odd square numerator
In order to find the A_f, we first enumerated those A_f for which the numerator of $L(A_f,1)/\Omega_f$ is divisible by an odd square n_f. For $N < 1000$, these are given in table 5. Any odd visible Ш coprime to primes dividing torsion and c_p must show up as a divisor of the numerator, and given BSD, it must show up as a square divisor because the Mordell-Weil rank of the explanatory factor is even. It would be interesting to compute the conjectural order of Ш for each abelian variety in this table, but not in table 1, and show (when possible) that the visible Ш is old.

$\mathbf{A_f}$	n_f	w_q	c_p	T	$TL(1)/\Omega_f$	δ_A	$\mathbf{B_g}$
389E20	5^2	$-$	97	97	5^2	5	**389A1**
433D16	7^2	$-$	3^2	3^2	7^2	$3 \cdot 7 \cdot 37$	**433A1**
446F8	11^2	$+-$	$1, 3$	3	11^2	$11 \cdot 359353$	**446B1**
563E31	13^2	$-$	281	281	13^2	13	**563A1**
571D2	3^2	$-$	1	1	3^2	$3^2 \cdot 127$	**571B1**
655D13	3^4	$+-$	$1, 1$	1	3^4	$3^2 \cdot 19 \cdot 515741$	**655A1**
664F8	5^2	$-+$	$a, 1$	1	5^2	5	**664A1**
681B1	3^2	$+-$	$1, 1$	1	3^2	$3 \cdot 5^3$	**681C1**
707G15	13^2	$+-$	$1, 1$	1	13^2	$13 \cdot 800077$	**707A1**
709C30	11^2	$-$	59	59	11^2	11	**709A1**
718F7	7^2	$+-$	$1, 1$	1	7^2	$7 \cdot 151 \cdot 35573$	**718B1**
794G14	11^2	$+-$	$3, 1$	3	11^2	$3 \cdot 7 \cdot 11 \cdot 47 \cdot 35447$	**794A1**
817E15	7^2	$+-$	$1, 5$	5	7^2	$7 \cdot 79$	**817A1**
916G9	11^2	$-+$	$a, 1$	1	11^2	$3^9 \cdot 11 \cdot 17 \cdot 239$	**916C1**
944O6	7^2	$+-$	$a, 1$	1	7^2	7	**944E1**
997H42	3^4	$-$	83	83	3^4	3^2	**997B1, C1**
1001L7	7^2	$+-+$	$1, 1, 1$	1	7^2	$7 \cdot 19 \cdot 47 \cdot 2273$	**1001C1**
1028E14	$3^2 \cdot 11^2$	$-+$	$a, 1$	3	$3^4 \cdot 11^2$	$3^{13} \cdot 11$	**1028A1**
1061D46	151^2	$-$	$5 \cdot 53$	$5 \cdot 53$	151^2	$61 \cdot 151 \cdot 179$	**1061B1**

Table 1: New visible III

$\mathbf{B_g}$	rank	w_q	c_p	T	δ_B	Comments
389A1	2	$-$	1	1	5	first curve of rank 2
433A1	2	$-$	1	1	7	
446B1	2	$+-$	$1, 1$	1	11	this is **446D** in [3]
563A1	2	$-$	1	1	13	
571B1	2	$-$	1	1	3	
655A1	2	$+-$	$1, 1$	1	3^2	
664A1	2	$-+$	$1, 1$	1	5	
681C1	2	$+-$	$1, 1$	1	3	
707A1	2	$+-$	$1, 1$	1	13	
709A1	2	$-$	1	1	11	
718B1	2	$+-$	$1, 1$	1	7	
794A1	2	$+-$	$1, 1$	1	11	
817A1	2	$+-$	$1, 1$	1	7	
916C1	2	$-+$	$3, 1$	1	$3 \cdot 11$	
944E1	2	$+-$	$1, 1$	1	7	
997B1	2	$-$	1	1	3	
997C1	2	$-$	1	1	3	
1001C1	2	$+-+$	$1, 3, 1$	1	$3^2 \cdot 7$	
1028A1	2	$-+$	$3, 1$	1	$3 \cdot 11$	intersects **1028E** mod 11
1061B2	4	$-$	1	1	151	first surface of rank 4 [2]

Table 2: Explanatory factors

$\mathbf{446} = 2 \cdot 223$	$\mathbf{655} = 5 \cdot 131$	$\mathbf{664} = 2^3 \cdot 83$	$\mathbf{681} = 3 \cdot 227$
$\mathbf{707} = 7 \cdot 101$	$\mathbf{718} = 2 \cdot 359$	$\mathbf{794} = 2 \cdot 397$	$\mathbf{817} = 19 \cdot 43$
$\mathbf{916} = 2^2 \cdot 229$	$\mathbf{944} = 2^4 \cdot 59$	$\mathbf{1001} = 7 \cdot 11 \cdot 13$	$\mathbf{1028} = 2^2 \cdot 257$

Table 3: Factorizations

$\mathbf{A_f}$	p	w_p	$\lvert\text{Coker}\rvert$	$\lvert\text{Disc}(X[I_f])\rvert$	$\lvert\Phi(\overline{\mathbf{F}}_p)\rvert$
389E20	389	$-$	97	$5 \cdot 97$	97
433D16	433	$-$	3^2	$3^3 \cdot 7 \cdot 37$	3^2
446F8	223	$-$	3	$3 \cdot 11 \cdot 359353$	3
	2	$+$	3	$3 \cdot 11$	$3 \cdot 359353$
563E31	563	$-$	281	$13 \cdot 281$	281
571D2	571	$-$	1	$3^2 \cdot 127$	1
655D13	131	$-$	1	$3^2 \cdot 19 \cdot 515741$	1
	5	$+$	1	3^2	$19 \cdot 515741$
664F8	83	$+$	1	5	1
681B1	227	$-$	1	$3 \cdot 5^3$	1
	3	$+$	1	$3 \cdot 5^2$	5
707G15	101	$-$	1	$13 \cdot 800077$	1
	7	$+$	1	13	800077
709C30	709	$-$	59	$11 \cdot 59$	59
718F7	359	$-$	1	$7 \cdot 151 \cdot 35573$	1
	2	$+$	1	7	$151 \cdot 35573$
794G14	397	$-$	3	$3^2 \cdot 7 \cdot 11 \cdot 47 \cdot 35447$	3
	2	$+$	3	$3 \cdot 11$	$3^2 \cdot 7 \cdot 47 \cdot 35447$
817E15	43	$-$	5	$5 \cdot 7 \cdot 79$	5
	19	$+$	1	7	79
916G9	229	$+$	1	$3^9 \cdot 11 \cdot 17 \cdot 239$	1
944O6	59	$-$	1	7	1
997H42	997	$-$	83	$3^2 \cdot 83$	83
1001L7	13	$+$	1	$7 \cdot 19 \cdot 47 \cdot 2273$	1
	11	$-$	1	$7 \cdot 19 \cdot 47 \cdot 2273$	1
	7	$+$	1	$7 \cdot 19 \cdot 47$	2273
1028E14	257	$+$	1	$3^{13} \cdot 11$	1
1061D46	1061	$-$	$5 \cdot 53$	$5 \cdot 53 \cdot 61 \cdot 151 \cdot 179$	$5 \cdot 53$

Table 4: Component groups

305D7 : 3	**309D8** : 5	**335E11** : 3^2	**389E20** : 5	**394A2** : 5	**399G5** : 3^4
433D16 : 7	**435G2** : 3	**436C4** : 3	**446E7** : 3	**446F8** : 11	**455D4** : 3
473F9 : 3	**500C4** : 3	**502E6** : 11	**506I4** : 5	**524D4** : 3	**530G4** : 7
538E7 : 3	**551H18** : 3	**553D13** : 3	**555E2** : 3	**556C7** : 3	**563E31** : 13
564C3 : 3	**571D2** : 3	**579G13** : $3 \cdot 5$	**597E14** : 19	**602G3** : 3	**604C6** : 3
615F6 : 5	**615G8** : 7	**620D3** : 3	**620E4** : 3	**626F12** : 5	**629G15** : 3
642D2 : 3	**644C5** : 3	**644D5** : 3	**655D13** : 3^2	**660F2** : 3	**662E10** : 43
664F8 : 5	**668B5** : 3	**678I2** : 3	**681B1** : 3	**681I10** : 3	**682I6** : 11
707G15 : 13	**709C30** : 11	**718F7** : 7	**721F14** : 3^2	**724C8** : 3	**756G2** : 3
764A8 : 3	**765M4** : 3	**766B4** : 3	**772C9** : 3	**790H6** : 3	**794G12** : 11
794H14 : 5^2	**796C8** : 3	**817E15** : 7	**820C4** : 3	**825E2** : 3	**844C10** : 3^2
855M4 : 3	**860D4** : 3	**868E5** : 3	**876E5** : 3	**878C2** : 3	**884D6** : 3
885L9 : 3^2	**894H2** : 3	**902I5** : 3	**913G17** : 3	**916G9** : 11	**918O2** : 5
918P2 : 3	**925K7** : 3	**932B13** : 3^2	**933E14** : 19	**934I12** : 7	**944O6** : 7
946K7 : 3	**949B2** : 3	**951D19** : 3	**959D24** : 3	**964C12** : 3^2	**966J1** : 3
970I5 : 3	**980F1** : 3	**980J2** : 3	**986J7** : 5	**989E22** : 5	**993B3** : 3^2
996E4 : 3	**997H42** : 3^2	**998A2** : 3	**998H9** : 3	**999J10** : 3	

Table 5: Odd square numerator

References

[1] A. Agashé, *On invisible elements of the Tate-Shafarevich group*, Théorie des nombres **328** (1999), 369–374.

[2] A. Brumer, *The rank of* $J_0(N)$, Astérisque (1995), no. 228, 3, 41–68, Columbia University Number Theory Seminar (New York, 1992).

[3] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[4] J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Proceedings of the Arizona Winter School (1998).

[5] H. Darmon, F. Diamond, and R. Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Internat. Press, Cambridge, MA, 1994, pp. 1–154.

[6] F. Diamond and J. Im, *Modular forms and modular curves*, (1995).

[7] G. Frey and M. Müller, *Arithmetic of modular curves and applications*, Algorithmic algebra and number theory (Heidelberg, 1997), Springer, Berlin, 1999, pp. 11–48.

[8] D. Kohel, *Hecke module structure of quaternions*, (1998).

[9] V. A. Kolyvagin and D. Yu. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Algebra i Analiz **1** (1989), no. 5, 171–196.

[10] S. Lang, *Introduction to modular forms*, Springer-Verlag, Berlin, 1995, With appendixes by D. Zagier and Walter Feit, Corrected reprint of the 1976 original.

[11] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[12] L. Merel, *Universal Fourier expansions of modular forms*, On Artin's conjecture for odd 2-dimensional representations (Berlin), Springer, 1994, pp. 59–94.

[13] J.-F. Mestre, *La méthode des graphes. Exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata) (1986), 217–242.

[14] J.S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

[15] K. A. Ribet, *On modular representations of* $\mathrm{gal}(\overline{\mathbf{q}}/\mathbf{q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.

[16] G. Shimura, *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan **25** (1973), no. 3, 523–544.

[17] ———, *On the periods of modular forms*, Math. Ann. **229** (1977), 211–221.

[18] W. Stein, *Component groups of optimal factors of* $J_0(N)$, Preprint (1999).