MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Pages 000–000
S 0025-5718(XX)0000-0

VISIBLE EVIDENCE FOR THE BIRCH AND SWINNERTON-DYER CONJECTURE FOR MODULAR ABELIAN VARIETIES OF ANALYTIC RANK ZERO (WITH AN APPENDIX BY J. CREMONA AND B. MAZUR)

AMOD AGASHE AND WILLIAM STEIN

Abstract. This paper provides evidence for the Birch and Swinnerton-Dyer conjecture for analytic rank 0 abelian varieties A_f that are optimal quotients of $J_0(N)$ attached to newforms. We prove theorems about the ratio $L(A_f,1)/\Omega_{A_f}$, develop tools for computing with A_f, and gather data about certain arithmetic invariants of the nearly 20000 abelian varieties A_f of level ≤ 2333. Over half of these A_f have analytic rank 0, and for these we compute upper and lower bounds on the conjectural order of $Ш(A_f)$. We find that there are at least 168 such that the Birch and Swinnerton-Dyer Conjecture implies that $Ш(A_f)$ is divisible by an odd prime, and we prove for 37 of these that the odd part of the conjectural order of $Ш(A_f)$ really divides $\#Ш(A_f)$ by constructing nontrivial elements of $Ш(A_f)$ using visibility theory. We also give other evidence for the conjecture. The appendix, by Cremona and Mazur, fills in some gaps in the theoretical discussion in their paper on visibility of Shafarevich-Tate groups of elliptic curves.

Contents

Received by the editor June 10, 2003.
1991 *Mathematics Subject Classification.* Primary 11G40; Secondary 11F11, 11G10, 14K15, 14H25, 14H40.
Key words and phrases. Birch and Swinnerton-Dyer conjecture, modular abelian variety, visibility, Shafarevich-Tate groups.

1. Introduction

Let N be a positive integer, and f be a newform of weight 2 on $\Gamma_0(N)$. A construction due to Shimura associates to f an abelian variety quotient A_f of $J_0(N)$. We say that A_f has *analytic rank zero* if its L-function $L(A_f, s)$ is nonzero at $s = 1$. In this paper we give evidence for the Birch and Swinnerton-Dyer conjecture for analytic rank 0 abelian varieties A_f of arbitrary dimension. For such abelian varieties, the conjecture asserts that $A_f(\mathbf{Q})$ is finite, and gives a formula for the order of the Shafarevich-Tate group Ш(A_f).

Kolyvagin and Logachev proved in [KL89, KL92] that if $L(A_f, 1) \neq 0$, then $A_f(\mathbf{Q})$ and Ш(A_f) are both finite. To the best of our knowledge, Birch and Swinnerton-Dyer's formula for #Ш(A_f) has not been completely verified for a single abelian variety A_f of dimension greater than one. In [KL92, §1.6] Kolyvagin and Logachev remark that if one were able to compute the height of a certain Heegner point, their methods could be used to find an upper bound on #Ш(A_f), but we have not done this. Instead, in this paper we focus on computing *nonzero subgroups* of Ш(A_f) when the conjecture predicts that Ш(A_f) is nonzero.

Inspired by work of Cremona and Mazur (see [CM]), we had the idea to reverse their methods and prove, in some cases, that #Ш(A_f) is at least as big as predicted by the Birch and Swinnerton-Dyer conjecture. Instead of assuming that Ш(A_f) is as predicted by the conjecture and trying to understand whether or not it is visible in $J_0(N)$, we prove a theorem (see [AS02b]) that allows us to sometimes construct the odd part of Ш(A_f) without assuming any conjectures. After developing algorithms that allow us to compute the conjectural order of Ш(A_f) in most cases, we analyzed the 19608 abelian varieties A_f of level ≤ 2333, and constructed the tables of Section 5. This resulted in the first systematic experimental evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of dimension greater than 2 (see [FpS$^+$01] for dimension 2).

This paper is organized as follows. In Section 2 we review background about modular abelian varieties and state the Birch and Swinnerton-Dyer conjecture. Section 3 explains the basic facts about quotients A_f of $J_0(N)$ that one needs to know in order to compute with them. In Section 4 we discuss a generalization of the Manin constant, derive a formula for the ratio $L(A_f, 1)/\Omega_{A_f}$, and bound the denominator of this ratio, thus giving some theoretical evidence towards the Birch and Swinnerton-Dyer conjecture. Section 5 reports on our construction of a table of 168 rank 0 abelian varieties A_f of level ≤ 2333 such that the Birch and

Swinnerton-Dyer conjecture predicts that $\#Ш(A_f)$ is divisible by an odd prime, and discusses what we computed to show that for 37 of the A_f there are *at least* as many elements of the odd part of $\#Ш(A_f)$ as predicted. The part of $\#Ш(A_f)$ that is coprime to the modular degree of A_f (which we define below) is a perfect square, and in the several cases where we could compute the odd part of the conjectured value of $\#Ш(A_f)$, we found the odd part to be a perfect square, which gives computational evidence for the conjecture. The appendix, written by Cremona and Mazur, fills in some gaps in the theoretical discussion in [CM].

Acknowledgment. It is a pleasure to thank Bryan Birch, Robert Coleman, Benedict Gross, Hednrik Lenstra, Dino Lorenzini, Loïc Merel, Bjorn Poonen, Ken Ribet, and John Tate for many helpful comments and discussions. Special thanks go to Barry Mazur for guiding our ideas on visibility and purchasing the second author a powerful computer, and to Allan Steel and David Kohel at MAGMA for their crucial computational support.

2. Background and Definitions

2.1. Modular Forms.

Fix a positive integer N. The group

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : N \mid c \right\}$$

acts by linear fractional transformations on the extended complex upper halfplane $\mathfrak{h}^*$. As a Riemann surface, $X_0(N)(\mathbf{C})$ is the quotient $\Gamma_0(N)\backslash\mathfrak{h}^*$. There is a standard model for $X_0(N)$ over $\mathbf{Q}$ (see [Shi94, Ch. 6]), and the Jacobian $J_0(N)$ of $X_0(N)$ is an abelian variety over $\mathbf{Q}$ of dimension equal to the genus g of $X_0(N)$, which is equipped with an action of the Hecke algebra $\mathbf{T} = \mathbf{Z}[\ldots T_n \ldots]$. The space $S_2(\Gamma_0(N))$ of cuspforms of weight 2 on $\Gamma_0(N)$ is a module over $\mathbf{T}$ and $S_2(\Gamma_0(N)) \cong H^0(X_0(N), \Omega_{X_0(N)})$ as $\mathbf{T}$-modules.

2.2. Abelian Varieties Attached to Newforms.

A *newform*

$$f = \sum_{n\geq 1} a_n q^n \in S_2(\Gamma_0(N))$$

is an eigenvector for $\mathbf{T}$ that is normalized so that $a_1 = 1$ and which lies in the orthogonal complement of the old subspace of $S_2(\Gamma_0(N))$. Let I_f denote the annihilator $\mathrm{Ann}_{\mathbf{T}}(f)$ of f in $\mathbf{T}$. Following Shimura [Shi73], attach to I_f the quotient

$$A_f = J_0(N)/I_f J_0(N),$$

which is an abelian variety over $\mathbf{Q}$ of dimension $[\mathbf{Q}(\ldots, a_n, \ldots) : \mathbf{Q}]$, which is equipped with a faithful action of $\mathbf{T}/I_f$. Moreover, A_f is an *optimal quotient* of $J_0(N)$, in the sense that $A_f^\vee \to J_0(N)$ is a closed immersion, or equivalently that the kernel of $J_0(N) \to A_f$ is connected (see [CS02, Prop. 3.3]).

Also, the complex torus $A_f(\mathbf{C})$ fits into the exact sequence

$$H_1(X_0(N), \mathbf{Z}) \to \mathrm{Hom}(S_2(\Gamma_0(N))[I_f], \mathbf{C}) \to A_f(\mathbf{C}) \to 0.$$

2.3. The Birch and Swinnerton-Dyer Conjecture.

The conjecture of Birch and Swinnerton-Dyer makes sense for abelian varieties over fairly general global fields, but we only state a special case. This conjecture involves the L-function attached to $A = A_f$:

$$L(A,s) = \prod_{i=1}^{d} L(f^{(i)},s) = \prod_{i=1}^{d} \left(\sum_{n\geq 1} \frac{a_n^{(i)}}{n^s} \right),$$

where $f^{(i)}$ is the ith Galois conjugate of f and $a_n^{(i)}$ is the ith Galois conjugate of a_n. It follows from work of Hecke that $L(A,s)$ has an analytic continuation to the whole complex plane and satisfies a functional equation. Birch and Swinnerton-Dyer made the following conjecture, which relates the rank of A to the order of vanishing of $L(A,s)$ at $s = 1$.

Conjecture 2.1 (Birch and Swinnerton-Dyer)**.** *The Mordell-Weil rank of A is equal to the order of vanishing of $L(A,s)$ at $s = 1$, i.e.,*

$$\dim(A(\mathbf{Q}) \otimes \mathbf{Q}) = \mathrm{ord}_{s=1} L(A,s).$$

Birch and Swinnerton-Dyer also furnished a conjectural formula for the order of the Shafarevich-Tate group

$$Ш(A) := \ker \left(H^1(\mathbf{Q},A) \longrightarrow \prod_{\text{all places } v} H^1(\mathbf{Q}_v, A) \right).$$

(They only made their conjecture for elliptic curves, but Tate [Tat66] reformulated it a functorial way which makes sense for abelian varieties. See also [Lan91, §III.5] for another formulation.) We now state their conjecture in the special case when $L(A,1) \neq 0$, where [KL89, KL92] implies that $Ш(A)$ is finite. The conjecture involves the Tamagawa numbers c_p of A (see Section 3.7), and the canonical volume Ω_A of $A(\mathbf{R})$ (see Section 4.2).

Conjecture 2.2 (Birch and Swinnerton-Dyer)**.** *Suppose $L(A,1) \neq 0$. Then*

$$\frac{L(A,1)}{\Omega_A} = \frac{\#Ш(A) \cdot \prod_{p\mid N} c_p}{\#A(\mathbf{Q})_{\mathrm{tor}} \cdot \#A^\vee(\mathbf{Q})_{\mathrm{tor}}},$$

where $A^\vee$ is the abelian variety dual of A.

Remark 2.3. Since $L(A,1) \neq 0$, finiteness of $Ш(A)$ and the existence of the Cassels-Tate pairing implies that $\#Ш(A) = \#Ш(A^\vee)$, so Conjecture 2.2 can also be viewed as a formula for $\#Ш(A^\vee)$.

The algorithms outlined in this paper take advantage of the fact that A is attached to a newform in order to compute the conjectural order of $Ш(A)$ away from certain bad primes.

3. Explicit Approaches to Modular Abelian Varieties

We use the algorithms of this section to enumerate the A_f, compute information about the invariants of A_f that appear in Conjecture 2.2, and to verify the hypothesis of Theorem 3.13 in order to construct nontrivial subgroups of $Ш(A_f)$. The second author has implemented the algorithms discussed in this paper, and made many of them part of the Magma computer algebra system [BCP97].

In Section 3.1, we discuss modular symbols, which are the basic tool we use in many of the computations, and in Section 3.2 we discuss how we systematically enumerate modular abelian varieties. There is an analogue for A_f of the usual elliptic-curve modular degree, which we discuss in Section 3.3, and which we use to rule out the existence of visible elements of $Ш(A_f)$ of a certain order. In Section 3.4 we describe how to compute the intersection of two abelian varieties, which will be needed to verify the hypothesis of Theorem 3.13. In Sections 3.5 and 3.6, we describe standard methods for bounding the torsion subgroup of an abelian variety above and below. Section 3.7 reviews an algorithm for computing the odd part of the Tamagawa number c_p when $p \,||\, N$, and discusses the Lenstra-Oort bound in the case when $p^2 \mid N$.

Unless otherwise stated, f is a newform, I_f its annihilator, and $A = A_f$ is the corresponding optimal quotient of $J_0(N)$.

3.1. **Modular Symbols.** Modular symbols are crucial to many algorithms for computing with modular abelian varieties, because they can be used to construct a *finite* presentation for $H_1(X_0(N), \mathbf{Z})$ in terms of paths between elements of $\mathbf{P}^1(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\}$. They were introduced by Birch [Bir71] and studied by Manin, Mazur, Merel, Cremona, and others.

Let $\mathfrak{M}_2$ be the free abelian group with basis the set of all symbols $\{\alpha, \beta\}$, with $\alpha, \beta \in \mathbf{P}^1(\mathbf{Q})$, modulo the three-term relations

$$\{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\} = 0,$$

and modulo any torsion. The group $\mathrm{GL}_2(\mathbf{Q})$ acts on the left on $\mathfrak{M}_2$ by

$$g\{\alpha, \beta\} = \{g(\alpha), g(\beta)\},$$

where g acts on α and β by a linear fractional transformation. The space $\mathfrak{M}_2(\Gamma_0(N))$ of *modular symbols* for $\Gamma_0(N)$ is the quotient of $\mathfrak{M}_2$ by the subgroup generated by all elements of the form $x - g(x)$, for $x \in \mathfrak{M}_2$ and g in $\Gamma_0(N)$, modulo any torsion. A *modular symbol* for $\Gamma_0(N)$ is an element of this space, and we frequently denote the equivalence class that defines a modular symbol by giving a representative element.

Let $\mathfrak{B}_2(\Gamma_0(N))$ be the free abelian group with basis the finite set $\Gamma_0(N)\backslash\mathbf{P}^1(\mathbf{Q})$. The boundary map $\delta : \mathfrak{M}_2(\Gamma_0(N)) \to \mathfrak{B}_2(\Gamma_0(N))$ sends $\{\alpha, \beta\}$ to $[\beta] - [\alpha]$, where $[\beta]$ denotes the basis element of $\mathfrak{B}_2(\Gamma_0(N))$ corresponding to $\beta \in \mathbf{P}^1(\mathbf{Q})$. The *cuspidal modular symbols* are the kernel $\mathfrak{S}_2(\Gamma_0(N))$ of δ, and the integral homology $H_1(X_0(N), \mathbf{Z})$ is canonically isomorphic to $\mathfrak{S}_2(\Gamma_0(N))$.

Cremona's book [Cre97, §2.2] contains a concrete description of how to compute $\mathfrak{M}_2(\Gamma_0(N)) \otimes \mathbf{Q}$ using Manin symbols, which are a finite set of generators for $\mathfrak{M}_2(\Gamma_0(N))$. In general, the easiest way we have found to compute $\mathfrak{M}_2(\Gamma_0(N))$ is to compute $\mathfrak{M}_2(\Gamma_0(N)) \otimes \mathbf{Q}$, then compute the $\mathbf{Z}$-submodule of $\mathfrak{M}_2(\Gamma_0(N)) \otimes \mathbf{Q}$ generated by the Manin symbols.

3.2. **Enumerating Newforms.** Since $X_0(N)$ is defined over $\mathbf{Q}$ it is defined over $\mathbf{R}$, so complex conjugation acts on $X_0(N)(\mathbf{C})$ hence on the homology $H_1(X_0(N), \mathbf{Z})$. In terms of modular symbols, complex conjugation acts by sending $\{\alpha, \beta\}$ to $\{-\alpha, -\beta\}$. Let $H_1(X_0(N), \mathbf{Z})^+$ denote the $+1$-eigenspace for the action of the involution induced by complex conjugation, which we can compute using modular symbols. We list all newforms of a given level N by decomposing the new subspace of $H_1(X_0(N), \mathbf{Q})^+$ under the action of the the Hecke operators and listing the corresponding systems of Hecke eigenvalues (see [Ste02a]). First we compute the characteristic polynomial of T_2, and use it to break up the new space. We apply this process recursively with $T_3, T_5, \ldots$ until either we have exceeded the bound coming from [Stu87] (see [AS]), or we have found a Hecke operator T_n whose characteristic polynomial is irreducible.

We *order the newforms* in a way that extends the ordering in [Cre97]: First sort by dimension, with smallest dimension first; within each dimension, sort in binary by the signs of the Atkin-Lehner involutions, e.g., $+++$, $++-$, $+-+$, $+--$, $-++$, etc. When two forms have the same Atkin-Lehner sign sequence, order by $|\operatorname{Tr}(a_p)|$ with ties broken by taking the positive trace first. We denote a Galois-conjugacy class of newforms by a bold symbol such as **389E**, which consists of a level and isogeny class, where **A** denotes the first class, **B** the second, **E** the fifth, **BB** the 28th, etc. As discussed in [Cre97, pg. 5], for certain small levels the above ordering, when restricted to elliptic curves, does not agree with the ordering used in the tables of [Cre97]. For example, our **446B** is Cremona's **446D**.

3.3. **The Modular Degree.** Since A_f is an optimal quotient, the dual map $A_f^\vee \to J_0(N)$ is injective and the composite $\theta_f : A_f^\vee \to A_f$ has finite degree. The map θ_f is a polarization, so $\deg(\theta_f)$ is a perfect square (see Lemma 3.14). The *modular degree* of A_f is the square root of the degree of θ_f:

$$\operatorname{moddeg}(A_f) = \sqrt{\deg(\theta_f)}.$$

When $\dim A_f = 1$, $\operatorname{moddeg}(A_f)$ is the usual modular degree, i.e., the degree of $X_0(N) \to A_f$.

If M is an abelian group, let $M^* = \operatorname{Hom}_{\mathbf{Z}}(M, \mathbf{Z})$. The Hecke algebra acts in a natural way on $H_1(X_0(N), \mathbf{Z})$ and $H_1(X_0(N), \mathbf{Z})^*$, and we have a natural restriction map

$$r_f : H_1(X_0(N), \mathbf{Z})^*[I_f] \to (H_1(X_0(N), \mathbf{Z})[I_f])^*.$$

The following proposition leads to an algorithm for computing the modular degree.

Proposition 3.1. $\operatorname{coker}(r_f) \cong \ker(\theta_f)$, *so* $\operatorname{moddeg}(A_f) = \sqrt{\#\operatorname{coker}(r_f)}$.

The proposition is proved in [KS00]. The proof makes use of the *Abel-Jacobi theorem*, which realizes the Jacobian $J_0(N)(\mathbf{C})$ as a complex torus:

$$0 \to H_1(X_0(N), \mathbf{Z}) \to \operatorname{Hom}(S_2(\Gamma_0(N)), \mathbf{C}) \to J_0(N)(\mathbf{C}) \to 0,$$

where $H_1(X_0(N), \mathbf{Z})$ is embedded as a lattice of full rank in the complex vector space $\operatorname{Hom}(S_2(\Gamma_0(N)), \mathbf{C})$ using the integration pairing, and this description of $J_0(N)(\mathbf{C})$ is compatible with the action of Hecke operators.

3.4. **Intersecting Complex Tori.** Let V be a finite dimensional complex vector space and let Λ be a lattice in V, so that $T = V/\Lambda$ is a complex torus. Suppose that V_A and V_B are subspaces of V such that $\Lambda_A = V_A \cap \Lambda$ and $\Lambda_B = V_B \cap \Lambda$ are lattices in V_A and V_B, respectively.

Proposition 3.2. *If $A \cap B$ is finite, then there is an isomorphism*

$$A \cap B \cong \left(\frac{\Lambda}{\Lambda_A + \Lambda_B}\right)_{\mathrm{tor}}.$$

Proof. Extend the exact sequence

$$0 \to A \cap B \to A \oplus B \xrightarrow{(x,y)\mapsto x-y} T$$

to the following diagram:

$$\begin{tikzcd}
 & \Lambda_A \oplus \Lambda_B \arrow[r] \arrow[d] & \Lambda \arrow[r] \arrow[d] & \Lambda/(\Lambda_A + \Lambda_B) \arrow[d] \\
0 \arrow[r] \arrow[d] & V_A \oplus V_B \arrow[r] \arrow[d] & V \arrow[r] \arrow[d] & V/(V_A + V_B) \arrow[d] \\
A \cap B \arrow[r] & A \oplus B \arrow[r] & T \arrow[r] & T/(A+B).
\end{tikzcd}$$

The middle row is exact because $A \cap B$ is finite so $V_A \cap V_B = 0$.

Using the snake lemma, which connects the kernel $A \cap B$ of $A \oplus B \to T$ to the cokernel of $\Lambda_A \oplus \Lambda_B \to \Lambda$, we obtain an exact sequence

$$0 \to A \cap B \to \Lambda/(\Lambda_A + \Lambda_B) \to V/(V_A + V_B).$$

Since $V/(V_A + V_B)$ is a **C**-vector space, the torsion part of $\Lambda/(\Lambda_A + \Lambda_B)$ must map to 0. No non-torsion in $\Lambda/(\Lambda_A + \Lambda_B)$ could map to 0, because if it did then $A \cap B$ would not be finite. The proposition follows. □

For abelian subvarieties of $J_0(N)$ attached to newforms, we use the proposition above as follows. The complex vector space $V = \mathrm{Hom}(S_2(\Gamma_0(N)), \mathbf{C})$ is the tangent space of $J_0(N)(\mathbf{C})$ at the identity. Setting $\Lambda = H_1(X_0(N), \mathbf{Z})$ and considering Λ as a lattice in V via the integration pairing, we have $J_0(N)(\mathbf{C}) \cong V/\Lambda$. Suppose f and g are non-conjugate newforms, and let I_f and I_g be their annihilators in the Hecke algebra $\mathbf{T}$, and let $A = A_f^\vee$ and $B = A_g^\vee$. Then $V_A = V[I_f]$ and $V_B = V[I_g]$ are the tangent spaces to A and B at the identity, respectively. The above proposition shows that the group $A \cap B$ is canonically isomorphic to $(\Lambda/(\Lambda_A + \Lambda_B))_{\mathrm{tor}}$. Here $\Lambda_A = \Lambda[I_f]$ and $\Lambda_B = \Lambda[I_g]$, because A_f and A_g are optimal quotients.

The following formula for the intersection of n subtori is obtained in a similar way to that of Proposition 3.2.

Proposition 3.3. *For $i = 1, \ldots, n$, with $n \geq 2$, let $A_i = V_i/\Lambda_i$ be a subtorus of $T = V/\Lambda$, and assume that each pairwise intersection $A_i \cap A_j$ is finite. Define a linear map*

$$f : V_1 \times \cdots \times V_n \longrightarrow V^{\oplus(n-1)}.$$

by $f(x_1, \ldots, x_n) = (x_1 - x_2,\, x_2 - x_3,\, x_3 - x_4,\, \ldots,\, x_{n-1} - x_n)$. Then

$$A_1 \cap \cdots \cap A_n \cong \left(\frac{\Lambda^{\oplus(n-1)}}{f(\Lambda_1 \oplus \cdots \oplus \Lambda_n)} \right)_{\mathrm{tor}}.$$

3.5. **Bounding the Torsion From Above.** In this section we recall the standard upper bound on the order of $\#A(\mathbf{Q})_{\mathrm{tor}}$, and illustrate its usefulness.

Let $f = \sum a_n q^n$ be a weight 2 newform on $\Gamma_1(N)$ with Nebentypus character $\varepsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$ (recall that f is a form on $\Gamma_0(N)$ if and only if $\varepsilon = 1$), and let $A = A_f$ be the corresponding optimal quotient of $J_1(N)$, as in [Shi73]. Shimura proved in [Shi94, Ch. 7] that the local Euler factor of A_f at p is

$$L_p(A_f, s) \;=\; \prod_{\sigma : K_f \hookrightarrow \overline{\mathbf{Q}}} \frac{1}{1 - \sigma(a_p)p^{-s} + \sigma(\varepsilon(p))p^{1-2s}}$$

by showing that the characteristic polynomial F_p of Frobenius on any ℓ-adic Tate module of $A_{\mathbf{F}_p}$ (for $\ell \nmid pN$) is

$$F_p(X) = \prod_{\sigma : K_f \hookrightarrow \overline{\mathbf{Q}}} X^2 - \sigma(a_p)X + \sigma(\varepsilon(p))p,$$

where $K_f = \mathbf{Q}(\ldots, a_n, \ldots)$. Let $\mathbf{Q}(\varepsilon)$ be the field generated by the values of ε (note that $\mathbf{Q}(\varepsilon) \subset K_f$), and for any $p \nmid N$ let $G_p(X) \in \mathbf{Q}(\varepsilon)[X]$ be the characteristic polynomial of left multiplication by a_p on the $\mathbf{Q}(\varepsilon)$-vector space K_f, which is a polynomial of degree $d' = [K_f : \mathbf{Q}(\varepsilon)]$. Then

$$F_p(X) = \mathrm{Norm}_{\mathbf{Q}(\varepsilon)/\mathbf{Q}} \left(X^{d'} \cdot G_p \left(X + \frac{\varepsilon(p)p}{X} \right) \right),$$

so

$$\begin{aligned} \#A_{\mathbf{F}_p}(\mathbf{F}_p) &= \deg(1 - \mathrm{Frob}_p) = |\det(1 - \mathrm{Frob}_p)| \\ &= |F_p(1)| = |\mathrm{Norm}_{\mathbf{Q}(\varepsilon)/\mathbf{Q}}(G_p(1 + \varepsilon(p)p))|. \end{aligned}$$

If $p \nmid N$ is odd, standard facts about formal groups imply that the reduction map $A(\mathbf{Q})_{\mathrm{tor}} \to A_{\mathbf{F}_p}(\mathbf{F}_p)$ is injective, so

$$\#A(\mathbf{Q})_{\mathrm{tor}} \mid \gcd \left\{ \#A_{\mathbf{F}_p}(\mathbf{F}_p) \,:\, \text{primes } p \nmid 2N \right\}.$$

Likewise, since $A^\vee$ is isogenous to A, the same bound applies to $A^\vee(\mathbf{Q})_{\mathrm{tor}}$, since $A^\vee$ and A have the same L-series.

The upper bound is the same for every abelian variety isogenous to A, so it is not surprising that it is not sharp in general. For example, let E (resp., F) be the elliptic curve labeled **30A1** (resp. **30A2**) in Cremona's tables [Cre97]. Then E and F are isogenous, $E(\mathbf{Q}) \approx \mathbf{Z}/6\mathbf{Z}$, and $F(\mathbf{Q}) \approx \mathbf{Z}/12\mathbf{Z}$, so

$$12 \mid \gcd \left\{ \#E_{\mathbf{F}_p}(\mathbf{F}_p) \,:\, \text{primes } p \nmid 2N \right\}.$$

(Incidentally, since $\#E(\mathbf{F}_5) = 12$, the gcd is 12.) For answers to some related deep questions about this gcd, see [Kat81].

Example 3.4. Let

$$f = q + (-1 + \sqrt{2})q^2 + q^3 + (-2\sqrt{2} + 1)q^4 - 2\sqrt{2}q^5 + \cdots \in S_2(\Gamma_0(39))$$

be the form **39B**. Then $G_5(X) = X^2 - 8$, so

$$\#A_f(\mathbf{Q})_{\mathrm{tor}} \mid G_5(1 + 5) = 28.$$

We find in [FpS+01] that A_f is isogenous to the Jacobian J of $y^2 + (x^3 + 1)y = -5x^4 - 2x^3 + 16x^2 - 12x + 2$ and that $\#J(\mathbf{Q}) = 28$. However A_f is not isomorphic to J since, as reported in Table 2 of [FpS+01], the Tamagawa numbers of J are $c_3 = 28$, $c_{13} = 1$, whereas the methods of Section 3.7 below show that the Tamagawa numbers of A_f are $c_3 = 14$, $c_{13} = 2$. The authors do not know for sure whether $\#A_f(\mathbf{Q}) = 28$, but in Example 3.6 below we show that $14 \mid \#A_f(\mathbf{Q})$. (Also, using the computational techniques of this paper one sees that the Birch and Swinnerton-Dyer conjecture implies that $\#A_f(\mathbf{Q}) = 28$.)

Example 3.5. Let

$$f = q + (-\zeta_6 - 1)q^2 + (2\zeta_6 - 2)q^3 + \zeta_6 q^4 + (-2\zeta_6 + 1)q^5 + \cdots$$

be one of the two Galois-conjugate newforms in $S_2(\Gamma_1(13))$. This form has character $\varepsilon : (\mathbf{Z}/13\mathbf{Z})^* \to \mathbf{C}^*$ of order 6, and $A_f = J_1(13)$. We have $G_3(X) = X - 2\zeta_6 + 2$ and $\varepsilon(3) = -\zeta_6$, so

$$\begin{aligned}\#J_1(13)(\mathbf{Q})_{\mathrm{tor}} \mid \#J_1(13)(\mathbf{F}_3) &= |\operatorname{Norm}(G_3(1-3\zeta_6))| \\ &= |\operatorname{Norm}(-5\zeta_6+3)| = 19.\end{aligned}$$

In fact Ogg proved that $J_1(13)(\mathbf{Q})_{\mathrm{tor}} \approx \mathbf{Z}/19\mathbf{Z}$ (see [Ogg73] and [MT74]).

3.6. **Bounding the Torsion From Below.** A cusp $\alpha \in \Gamma_0(N)\backslash\mathbf{P}^1(\mathbf{Q}) \subset X_0(N)$ defines a point $(\alpha) - (\infty) \in J_0(N)(\overline{\mathbf{Q}})_{\mathrm{tor}}$. The rational cuspidal subgroup C of $J_0(N)(\mathbf{Q})_{\mathrm{tor}}$ generated by $\mathbf{Q}$-rational cusps is of interest because the order of the image of C in $A_f(\mathbf{Q})_{\mathrm{tor}}$ provides a lower bound on $\#A_f(\mathbf{Q})_{\mathrm{tor}}$. Stevens [Ste82, §1.3] computed the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on the subgroup of $J_0(N)(\overline{\mathbf{Q}})$ generated by all cusps (and for other congruence subgroups besides $\Gamma_0(N)$). He found that $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on the cusps through $\mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q}) \cong (\mathbf{Z}/N\mathbf{Z})^*$, and that $d \in (\mathbf{Z}/N\mathbf{Z})^*$ acts by $x/y \mapsto x/(d'y)$, where $dd' \equiv 1 \pmod{N}$. Thus, e.g., $(0) - (\infty) \in J_0(N)(\mathbf{Q})_{\mathrm{tor}}$, and if N is square-free then all cusps are rational.

To compute the image of C in $A_f(\mathbf{Q})_{\mathrm{tor}}$, first make a list of inequivalent cusps using, e.g., the method described in [Cre97, §2.2, pg. 17]. Keep only the $\mathbf{Q}$-rational cusps, which can be determined using the result of Stevens above and [Cre97, Prop. 2.2.3] (when N is squarefree all cusps are rational). Next compute the subgroup $\mathcal{C}$ of $\mathfrak{M}_2(\Gamma_0(N))$ generated by modular symbols $\{\alpha,\infty\}$, where α is a $\mathbf{Q}$-rational cusp. The image of C in $A_f(\mathbf{Q})_{\mathrm{tor}}$ is isomorphic to the image of $\mathcal{C}$ in

$$P = \Phi_f(\mathfrak{M}_2(\Gamma_0(N)))/\Phi_f(\mathfrak{S}_2(\Gamma_0(N))),$$

where $\Phi_f : \mathfrak{M}_2(\Gamma_0(N)) \to \mathrm{Hom}(S_2(\Gamma_0(N))[I_f], \mathbf{C})$ is defined by the integration pairing. To keep everything rational, note that P can be computed using any map with the same kernel as Φ_f; for example, such a map can be constructed by finding a basis for $\mathrm{Hom}(\mathfrak{M}_2(\Gamma_0(N)), \mathbf{Q})[I_f]$ as described at the end of Section 4.2).

Example 3.6. Let the notation be as in Example 3.4. The cusps on $X_0(39)$ are represented by 0, ∞, $-1/9$, and $-4/13$, and since $N = 39$ is squarefree, these cusps are all rational. Using MAGMA we find that the image of C in $A_f(\mathbf{Q})_{\mathrm{tor}}$ is isomorphic to $\mathbf{Z}/14\mathbf{Z}$. Thus $A_f(\mathbf{Q})_{\mathrm{tor}}$ is isomorphic to one of $\mathbf{Z}/14\mathbf{Z}$, $\mathbf{Z}/28\mathbf{Z}$, or $\mathbf{Z}/14\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, but we do not know which.

Example 3.7. Let

$$f = q + \frac{1+\sqrt{5}}{2}q^2 + \frac{1-\sqrt{5}}{2}q^3 + \frac{5+\sqrt{5}}{2}q^4 + \cdots \in S_2(\Gamma_0(175))$$

be the form **175D**. The cusps of $X_0(175)$ are represented by

$$0,\ \infty,\ \frac{1}{25},\ \frac{1}{28},\ \frac{1}{30},\ \frac{1}{35},\ \frac{1}{45},\ \frac{1}{60},\ \frac{1}{65},\ \frac{1}{70},\ \frac{1}{105},\ \frac{1}{140}.$$

The $\mathbf{Q}$-rational cusps in this list are $0, \infty, \frac{1}{25}, \frac{1}{28}$, and these generate a subgroup of $A_f(\mathbf{Q})_{\mathrm{tor}}$ of order 2. (Incidentally, the group generated by all cusps, both rational and not, is isomorphic to $\mathbf{Z}/32\mathbf{Z}$.) Using a_p for $p \leq 17$ and the method of the previous section, we see that $\#A_f(\mathbf{Q})_{\mathrm{tor}} \mid 4$. The authors do not know if the cardinality is 2 or 4.

Example 3.8. The form **209C** is

$$f = q + \alpha q^2 + (1/2\alpha^4 - \alpha^3 - 5/2\alpha^2 + 4\alpha + 1)q^3 + (\alpha^2 - 2)q^4 + \cdots,$$

where $\alpha^5 - 2\alpha^4 - 6\alpha^3 + 10\alpha^2 + 5\alpha - 4 = 0$. As above, we find that $\#A_f(\mathbf{Q})_{\mathrm{tor}}$ divides 5. The image of the (rational) cuspidal subgroup in $A_f(\overline{\mathbf{Q}})_{\mathrm{tor}}$ is isomorphic to $\mathbf{Z}/5\mathbf{Z}$, so $A_f(\mathbf{Q})_{\mathrm{tor}} \approx \mathbf{Z}/5\mathbf{Z}$.

3.7. **Tamagawa Numbers.** Suppose $p \mid N$ and let $\Phi_{A,p}$ denote the component group of A at p, which is defined by the following exact sequence:

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

where $\mathcal{A}_{\mathbf{F}_p}$ is the closed fiber of the Néron model of A over $\mathbf{Z}_p$ and $\mathcal{A}^0_{\mathbf{F}_p}$ is the component of $\mathcal{A}_{\mathbf{F}_p}$ that contains the identity.

Definition 3.9. The *Tamagawa number* of A at p is

$$c_p = c_{A,p} = \#\Phi_{A,p}(\mathbf{F}_p).$$

When $p \,||\, N$, the second author found a computable formula for $\#\Phi_{A,p}(\overline{\mathbf{F}}_p)$ and (sometimes only up to a power of 2) for $\#\Phi_{A,p}(\mathbf{F}_p)$. There is a discussion about how to compute this number in [KS00] and [CS02] contains a proof of the formula. Note also that in this case the Tamagawa number of A at p is the same as the Tamagawa number of $A^\vee$ at p.

When $p^2 \mid N$ the authors do not know an algorithm to compute c_p. However, in this case Lenstra and Oort (see [LO85]) proved that

$$\sum_{\ell \neq p} (\ell - 1)\,\mathrm{ord}_\ell(\#\Phi_{A,p}(\overline{\mathbf{F}}_p)) \leq 2\dim(A_f),$$

so if $\ell \mid \#\Phi_{A,p}(\overline{\mathbf{F}}_p)$ then $\ell \leq 2 \cdot \dim(A_f) + 1$ or $\ell = p$. (Here $\mathrm{ord}_\ell(x)$ denotes the exponent of the largest power of ℓ that divides x.)

Example 3.10. Let f be **39B** as in Example 3.4. Running the algorithm of [KS00], we find that $c_3 = 14$ and $c_{13} = 2$.

Example 3.11. Let f be **175D** as in Example 3.7. Running the algorithm of [KS00], we find that $c_7 = 1$, and the Lenstra-Oort bound implies that the only possible prime divisors of c_5 are 2, 3, and 5.

3.8. **Visibility Theory.** We briefly recall visibility theory, which we will use to construct elements of Shafarevich-Tate groups. Section 6 contains another approach to the results reported in this section, but in the special case of elliptic curves.

Definition 3.12. Let $\iota : A \hookrightarrow J$ be an embedding of abelian varities over $\mathbf{Q}$. The *visible subgroup of* Ш(A) *with respect to the embedding* ι is

$$\mathrm{Vis}_J(\text{Ш}(A)) = \mathrm{Ker}(\text{Ш}(A) \to \text{Ш}(J)).$$

The following is a special case of Theorem 3.1 of [AS02b].

Theorem 3.13. *Let A and B be abelian subvarieties of an abelian variety J over $\mathbf{Q}$ such that $A(\overline{\mathbf{Q}}) \cap B(\overline{\mathbf{Q}})$ is finite. Let N be an integer divisible by the residue characteristics of primes of bad reduction for J (e.g., the conductor of J). Suppose p is a prime such that*

$$p \nmid 2 \cdot N \cdot \#(J/B)(\mathbf{Q})_{\mathrm{tor}} \cdot \#B(\mathbf{Q})_{\mathrm{tor}} \cdot \prod_\ell c_{A,\ell} \cdot c_{B,\ell},$$

where $c_{A,\ell} = \#\Phi_{A,\ell}(\mathbf{F}_\ell)$ *(resp.,* $c_{B,\ell}$*) is the Tamagawa number of* A *(resp.,* B*) at* ℓ*. Suppose furthermore that* $B[p](\overline{\mathbf{Q}}) \subset A(\overline{\mathbf{Q}})$ *as subgroups of* $J(\overline{\mathbf{Q}})$*. Then there is a natural map*

$$\varphi : B(\mathbf{Q})/pB(\mathbf{Q}) \to \mathrm{Vis}_J(Ш(A))$$

such that $\dim_{\mathbf{F}_p} \ker(\varphi) \leq \dim_{\mathbf{Q}} A(\mathbf{Q}) \otimes \mathbf{Q}$.

We return to the situation where $A = A_f$ is an optimal quotient of $J_0(N)$ attached to a newform. In Proposition 3.15 below we show that $\mathrm{Vis}_{J_0(N)}(Ш(A^\vee))$ is annihilated by multiplication by $\mathrm{moddeg}(A)$ (see also [CM, p.19]). We first state a lemma; the outline of the proof was indicated to us by B. Poonen.

Lemma 3.14. *Let* A *be an abelian variety over* k*, where* k *is a field, and let* $\lambda : A \to A^\vee$ *be a polarization. Suppose either that* k *has characteristic* 0 *or that its characteristic does not divide the degree of* λ*. Then there is a finite abelian group* H *such that* $\ker(\lambda) \approx H \times H$ *as groups.*

Proof. We work in the setting of Section 16 of [Mil86], using the notation used there. Consider the pairing

$$e^\lambda : \mathrm{Ker}(\lambda) \times \mathrm{Ker}(\lambda) \to \mu_m \subseteq \overline{k}^*,$$

as in [Mil86, p. 135], where m is an integer that kills $\mathrm{Ker}(\lambda)$. We will show that this pairing is nondegenerate.

Suppose $a \in \mathrm{Ker}(\lambda)$ is such that $e^\lambda(a, a') = 1$ for all $a' \in \mathrm{Ker}(\lambda)$. Let $a'' \in A^\vee[m]$. There exists an isogeny $\lambda' : A^\vee \to A$ such that $\lambda' \circ \lambda$ is multiplication by m on A and $\lambda \circ \lambda'$ is multiplication by m on $A^\vee$ (to construct λ', note that λ' is the quotient map $A^\vee \to A^\vee/\lambda(A[m])$). Pick an element $b \in A(\overline{k})$ such that $\lambda b = a''$. Then $mb = \lambda'(\lambda b) = \lambda'(a'')$. So $\overline{e}_m(a, a'') = \overline{e}_m(a, \lambda b) = e^\lambda(a, \lambda' a'') = 0$ (note that $\lambda(\lambda' a'') = m a'' = 0$, so that $\lambda' a'' \in \mathrm{Ker}(\lambda)$). This is true for all $a'' \in A^\vee[m]$, so the non-degeneracy of $\overline{e}_m$ ([Mil86, p. 131]) implies that $a = 0$.

Similarly, suppose $a' \in \mathrm{Ker}(\lambda)$ is such that $e^\lambda(a, a') = 1$ for all $a \in \mathrm{Ker}(\lambda)$. Since e^λ is skew-symmetric ([Mil86, p. 135]), this implies that $e^\lambda(a', a) = 1$ for all $a \in \mathrm{Ker}(\lambda)$. Then by the previous paragraph, $a' = 0$. This finishes the proof of non-degeneracy.

As mentioned before, the pairing e^λ is skew-symmetric. It is alternating because it extends to pairings on Tate modules (denoted by e_ℓ^λ in [Mil86, p. 132]), and the latter take values in a torsion-free group, so there is no distinction between skew-symmetric and alternating.

Now the lemma follows from the fact that if G is a finite abelian group with an alternating nondegenerate pairing, then there is a finite abelian group H such that $G \approx H \times H$ as groups (e.g., see [Del01, Prop. 2]). □

Proposition 3.15. *Let* $m_A = \mathrm{moddeg}(A)$*. We have*

$$\mathrm{Vis}_{J_0(N)}(Ш(A^\vee)) \subset Ш(A^\vee)[m_A].$$

Proof. The polarization θ_f (from Section 3.3) is the composite map $A^\vee \to J_0(N) \to A$. Let e_A be the exponent of the finite group $\ker(\theta_f)$. By Lemma 3.14, multiplication by m_A kills $\ker(\theta_f)$, so $e_A \mid m_A$. Also θ_f factors through multiplication by e_A, so there is a map $\theta'_f : A \to A^\vee$ such that $\theta'_f \circ \theta_f$ is multiplication by e_A. If ϕ is a map of abelian varieties (over $\mathbf{Q}$), let ϕ_* denote the corresponding map on

Shafarevich-Tate groups. Since $\mathrm{Vis}_{J_0(N)}(Ш(A^\vee))$ is contained in $\ker((\theta_f)_*)$, it is also contained in

$$\ker((\delta' \circ \delta)_*) = Ш(A^\vee)[e_A] \subset Ш(A^\vee)[m_A].$$

□

Since $Ш(A^\vee)[n]$ is finite for any n, we obtain the following corollary.

Corollary 3.16. $\mathrm{Vis}_{J_0(N)}(Ш(A^\vee))$ *is finite.*

4. The Quotient $L(A,1)/\Omega_A$

Fix a newform $f \in S_2(\Gamma_0(N))$, let I_f be the annihilator of f in $\mathbf{T}$, and $A = A_f = J_0(N)/I_f J_0(N)$ the corresponding optimal quotient. Suppose for the rest of this section that $L(A,1) \neq 0$.

4.1. **The Manin Constant.** When trying to compute the conjectural order of $Ш(A)$, we try to compute the quotient $L(A,1)/\Omega_A$, but find that it is easier to compute $c_A \cdot L(A,1)/\Omega_A$ where c_A is the Manin constant of A, which is defined as follows:

Definition 4.1 (Manin constant)**.** The *Manin constant* of A is

$$c_A = \#\left(\frac{S_2(\Gamma_0(N),\mathbf{Z})[I_f]}{H^0(\mathcal{A},\Omega_{\mathcal{A}/\mathbf{Z}})}\right) \in \mathbf{Z},$$

where we consider $H^0(\mathcal{A},\Omega_{\mathcal{A}/\mathbf{Z}})$ as a submodule of $S_2(\Gamma_0(N),\mathbf{Q})$ using

$$H^0(\mathcal{A},\Omega_{\mathcal{A}/\mathbf{Z}}) \to H^0(\mathcal{J},\Omega_{\mathcal{J}/\mathbf{Z}})[I_f] \to H^0(J,\Omega_{J/\mathbf{Q}})[I_f] \to S_2(\Gamma_0(N),\mathbf{Q})[I_f],$$

where $\mathcal{A}$ and $\mathcal{J}$ are the Néron models of A and J, respectively. (See [AS02a] for a discussion of why the image of $H^0(\mathcal{A},\Omega_{\mathcal{A}/\mathbf{Z}})$ is contained in $S_2(\Gamma_0(N),\mathbf{Z})$.)

Theorem 4.2. *If $\ell \mid c_A$ is a prime then $\ell^2 \mid 4N$.*

Proof. Mazur proved this when $\dim A = 1$ in [Maz78, §4], and we generalized his proof in [AS02a]. □

When $\dim A = 1$, Edixhoven [Edi91] obtained strong results towards the folklore conjecture that $c_A = 1$, and when A has arbitrary dimension the authors have made the following conjecture (see [AS02a] for evidence):

Conjecture 4.3. $c_A = 1$.

4.2. **A Formula for $L(A,1)/\Omega_A$.** If L and M are lattices in a real vector space V, then the *lattice index* $[L : M]$ is the absolute value of the determinant of a linear transformation of V taking L onto M. The lattice index satisfies the usual properties suggested by the notation, e.g., $[L : M] \cdot [M : N] = [L : N]$.

The *real volume* Ω_A is defined as follows. If L^* is a lattice in the cotangent space

$$T^* = H^0(A_{\mathbf{R}},\Omega_{A_{\mathbf{R}}}) = S_2(\Gamma_0(N),\mathbf{R})[I_f]$$

of $A_{\mathbf{R}}$, then L^* determines a lattice $L = \mathrm{Hom}(L^*,\mathbf{Z})$ in the tangent space $T = \mathrm{Hom}(T^*,\mathbf{R})$, and hence a measure on T by declaring that the quotient T/L has measure 1. The induced measure of $A(\mathbf{R})^0 = T/H_1(A(\mathbf{R}),\mathbf{Z})$ is then

$$\mu_L(A(\mathbf{R})^0) = [L : H_1(A(\mathbf{R}),\mathbf{Z})].$$

We also set

$$\mu_L(A(\mathbf{R})) = \mu_L(A(\mathbf{R})^0) \cdot c_\infty,$$

where $c_\infty = \#(A(\mathbf{R})/A(\mathbf{R})^0)$. Let $\mathcal{A}$ be the Néron model of A (see [BLR90]). The Néron differentials $H^0(\mathcal{A}, \Omega_{\mathcal{A}/\mathbf{Z}})$ define a lattice Λ^* in T^*, and we define $\Omega_A = \mu_\Lambda(A(\mathbf{R}))$.

Lemma 4.4. *$H_1(A(\mathbf{R}), \mathbf{Z}) \cong H_1(A(\mathbf{C}), \mathbf{Z})^+$.*

Proof. This lemma is well known, but we give a proof for the reader's convenience (which was suggested by H. Lenstra and B. Poonen). We have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & H_1(A(\mathbf{R}),\mathbf{Z}) \arrow[r] \arrow[d, "\psi"] & H_1(A(\mathbf{R}),\mathbf{R}) \arrow[r] \arrow[d, "\cong"] & A(\mathbf{R})^0 \arrow[r] \arrow[d, hook, "i"] & 0 \\
0 \arrow[r] & H_1(A(\mathbf{C}),\mathbf{Z})^+ \arrow[r] & H_1(A(\mathbf{C}),\mathbf{R})^+ \arrow[r, "\pi"] & A(\mathbf{C})^+ &
\end{tikzcd}$$

where the upper horizontal sequences is clearly exact, and the lower horizontal sequence is exact because it is the beginning of the long exact sequence of $\mathrm{Gal}(\mathbf{R}/\mathbf{C})$-cohomology that arises from

$$0 \to H_1(A(\mathbf{C}), \mathbf{Z}) \to H_1(A(\mathbf{C}), \mathbf{R}) \to A(\mathbf{C}) \to 0.$$

The middle vertical map is an isomorphism because if it were not then its kernel would be an uncountable set that maps to 0 in $A(\mathbf{R})^0$. The snake lemma then yields an exact sequence

$$0 \to \ker(\psi) \to 0 \to 0 \to \mathrm{coker}(\psi) \to 0,$$

which implies that ψ is an isomorphism. $\square$

Let

$$\Phi : H_1(X_0(N), \mathbf{Q}) \to \mathrm{Hom}(S_2(\Gamma_0(N))[I_f], \mathbf{C})$$

be the map induced by integration, scaled so that

$$\Phi(\{0, \infty\})(f) = L(f, 1)$$

(that $\{0, \infty\} \in H_1(X_0(N), \mathbf{Q})$ is the Manin-Drinfeld theorem, and that $\int_0^\infty f$ is a multiple of $L(f, 1)$ follows from the definition of $L(f, s)$ as a Mellin transform).

Theorem 4.5. *Recall that A is an abelian variety attached to a newform $f \in S_2(\Gamma_0(N))$, that c_∞ is the number of connected components of $A(\mathbf{R})$, that c_A is the Manin constant of A, that Ω_A is the Néron canonical volume of $A(\mathbf{R})$, and that Φ is the period mapping on homology induced by integrating homology classes on $X_0(N)$ against the $\mathbf{C}$-vector space spanned by the $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-conjugates of f. Then we have the following equation:*

$$c_\infty \cdot c_A \cdot \frac{L(A, 1)}{\Omega_A} = [\Phi(H_1(X_0(N), \mathbf{Z}))^+ : \Phi(\mathbf{T}\{0, \infty\})] \in \mathbf{Q},$$

where the lattice index on the right hand side should be interpreted as 0 if $\Phi(\mathbf{T}\{0, \infty\})$ has rank less than the dimension of A.

Proof. It is easier to compute with $\tilde{\Lambda}^* = S_2(\Gamma_0(N),\mathbf{Z})[I_f]$ than with Λ^*, so let $\tilde{\Omega}_A = \mu_{\tilde{\Lambda}}(A(\mathbf{R}))$. Note that $\tilde{\Omega}_A \cdot c_A = \Omega_A$, where c_A is the Manin constant. By Lemma 4.4 and Section 2.2,

$$\begin{aligned}\tilde{\Omega}_A &= c_\infty \cdot [\tilde{\Lambda} : H_1(A(\mathbf{R}),\mathbf{Z})]\\ &= c_\infty \cdot [\mathrm{Hom}(S_2(\Gamma_0(N),\mathbf{Z})[I_f],\mathbf{Z}) : \Phi(H_1(X_0(N),\mathbf{Z}))^+].\end{aligned}$$

For any ring R the pairing

$$\mathbf{T}_R \times S_2(\Gamma_0(N),R) \to R$$

given by $\langle T_n, f\rangle = a_1(T_n f)$ is perfect, so $(\mathbf{T}/I_f)\otimes R \cong \mathrm{Hom}(S_2(\Gamma_0(N),R)[I_f],R)$. Using this pairing, we may view Φ as a map

$$\Phi : H_1(X_0(N),\mathbf{Q}) \to (\mathbf{T}/I_f)\otimes \mathbf{C},$$

so that

$$\tilde{\Omega}_A = c_\infty \cdot [\mathbf{T}/I_f : \Phi(H_1(X_0(N),\mathbf{Z}))^+].$$

Note that $(\mathbf{T}/I_f)\otimes\mathbf{C}$ is isomorphic as a ring to a product of copies of $\mathbf{C}$, with one copy corresponding to each Galois conjugate $f^{(i)}$ of f. Let $\pi_i \in (\mathbf{T}/I_f)\otimes\mathbf{C}$ be the projector onto the subspace of $(\mathbf{T}/I_f)\otimes\mathbf{C}$ corresponding to $f^{(i)}$. Then $\Phi(\{0,\infty\})\cdot\pi_i = L(f^{(i)},1)\cdot\pi_i$. Since the π_i form a basis for the complex vector space $(\mathbf{T}/I_f)\otimes\mathbf{C}$, we see that

$$\det(\Phi(\{0,\infty\})) = \prod_i L(f^{(i)},1) = L(A,1).$$

Letting $H = H_1(X_0(N),\mathbf{Z})$, we have

$$\begin{aligned}[\Phi(H)^+ : \Phi(\mathbf{T}\{0,\infty\})] &= [\Phi(H)^+ : (\mathbf{T}/I_f)\cdot\Phi(\{0,\infty\})]\\ &= [\Phi(H)^+ : \mathbf{T}/I_f]\cdot[\mathbf{T}/I_f : \mathbf{T}/I_f\cdot\Phi(\{0,\infty\})]\\ &= \frac{c_\infty}{\tilde{\Omega}_A}\cdot\det(\Phi(\{0,\infty\}))\\ &= \frac{c_\infty c_A}{\Omega_A}\cdot L(A,1),\end{aligned}$$

which proves the theorem. □

Theorem 4.5 was inspired by the case when A is an elliptic curve (see [Cre97, §II.2.8]) or the winding quotient of $J_0(p)$ (see [Aga99]), and it generalizes to forms of weight > 2 (see [Ste00]).

Theorem 4.5 is true with Φ replaced by any linear map with the same kernel as Φ. One way to find such a linear map with image in a $\mathbf{Q}$-vector space is to compute a basis $\varphi_1,\ldots\varphi_d$ for $\mathrm{Hom}(H_1(X_0(N),\mathbf{Q}),\mathbf{Q})[I_f]$ and let $\Phi = \varphi_1\times\cdots\times\varphi_d$. Also, since $H_1(X_0(N),\mathbf{Z})^+$ and $\mathbf{T}\{0,\infty\}$ are contained in $H_1(X_0(N),\mathbf{Q})^+$, Theorem 4.5 implies that $L(A,1)/\Omega_A \in \mathbf{Q}$, a fact well known to the experts (see [Gro94, Prop. 2.7] for the statement, but without proof).

4.3. **The Denominator of $L(A,1)/\Omega_A$.** In this section, we prove a result about the denominator of the rational number $L(A,1)/\Omega_A$ and compare it to what is predicted by the Birch and Swinnerton-Dyer conjecture.

Proposition 4.6. *Let z be the point in $J_0(N)(\mathbf{Q})$ defined by the degree 0 divisor $(0)-(\infty)$ on $X_0(N)$, and let $n = n_f$ be the order of the image of z in $A(\mathbf{Q})$. Then the denominator of $c_\infty\cdot c_A\cdot L(A,1)/\Omega_A$ divides n.*

Proof. Let x be the image of z in $A(\mathbf{Q})$, and let $I = \mathrm{Ann}_{\mathbf{T}}(x)$ be the ideal of elements of $\mathbf{T}$ that annihilate x. Since f is a newform, the Hecke operators T_p, for $p \mid N$, act as 0 or ± 1 on $A(\mathbf{Q})$ (see, e.g., [DI95, §6]). If $p \nmid N$, then a standard calculation (see, e.g., [Cre97, §2.8]) shows that $T_p(x) = (p+1)x$.

Let C be the cyclic subgroup of $A(\mathbf{Q})$ of order n generated by x. Consider the map $\mathbf{T} \to C$ given by $T_p \mapsto T_p(x)$. The kernel of this map is I, and the map is surjective because its image is an additive group that contains x, and C is the smallest such group. Thus the map induces an isomorphism $\mathbf{T}/I \xrightarrow{\cong} C$. □

Conjecture 2.2 predicts that

$$\#A(\mathbf{Q}) \cdot \#A^\vee(\mathbf{Q}) \cdot \frac{L(A,1)}{\Omega_A} = \#\text{Ш}(A) \cdot \prod c_p \in \mathbf{Z},$$

and since $n \mid \#A(\mathbf{Q})$, Proposition 4.6 implies that

$$c_\infty \cdot c_A \cdot \#A(\mathbf{Q}) \cdot \frac{L(A,1)}{\Omega_A} \in \mathbf{Z}.$$

Since c_∞ is a power of 2, and c_A is conjecturally 1 (if N is prime, then by Theorem 4.2 it is a power of 2), Proposition 4.6 provides theoretical evidence for Conjecture 2.2, and also reflects a surprising amount of cancellation between $\prod c_p$ and $\#A^\vee(\mathbf{Q})$.

5. Results and Conclusions

We computed all 19608 abelian varieties $A = A_f$ attached to newforms of level $N \leq 2333$. Interesting data about some of these abelian varieties is summarized in Tables 1–4, which use the notation described in this section.

Suppose that A is one of the 10360 of these for which $L(A,1) \neq 0$, so Conjecture 2.2 asserts that Ш(A) has order

$$\#\text{Ш}_? = \frac{L(A,1)}{\tilde{\Omega}_A \cdot c_A} \cdot \frac{\#A(\mathbf{Q})_{\mathrm{tor}} \cdot \#A^\vee(\mathbf{Q})_{\mathrm{tor}}}{\prod_{p \mid N} c_p}.$$

(See Section 4.2 for the definition of $\tilde{\Omega}_A$ and c_A.)

For any rational number x, let x^{odd} be the *odd part* of x. If a and b are rational numbers with $a \neq 0$, we say that $a \mid b$ if b/a is an integer.

Define integers S_l and S_u such that

$$S_l \mid \mathrm{numer}(\#\text{Ш}_?^{\mathrm{odd}}) \mid S_u$$

as follows:

$\mathbf{S}_u$ The *upper bound* S_u is the odd part of the numerator of

$$\frac{L(A,1)}{\tilde{\Omega}_A} \cdot \frac{T^2}{\prod_{p \| N} c_p},$$

where T is the upper bound on $\#A(\mathbf{Q})$ and $\#A^\vee(\mathbf{Q})$ computed using Section 3.5 using a_p for $p \leq 17$. Since the Manin constant and the Tamagawa numbers are integers, S_u is an upper bound on the odd part of $\#\text{Ш}_?$.

$\mathbf{S}_l$ The *lower bound* S_l is defined as follows: Let $S_{l,1}$ be the odd part of the rational number

$$\frac{L(A,1)}{\tilde{\Omega}_A} \cdot \frac{\#C \cdot \#D}{\prod_{p \| N} c_p},$$

where $C \subset A(\mathbf{Q})_{\rm tor}$ and D is the part of C coprime to the modular degree of A. Usually C is the group generated by the image of $(0)-(\infty)$, and in all cases it contains this subgroup. More precisely, when A is an elliptic curve, we instead let C and D be the full torsion subgroup $A(\mathbf{Q})_{\rm tor}$, because it is easy to calculate. When A is not an elliptic curve it would be better to let C be the subgroup generated by all rational cusps, but the authors only realized this after completing the calculations, so we did not do this.

If N is square free, we let $S_l = S_{l,1}$. Otherwise, let $S_{l,2}$ be the largest part of $S_{l,1}$ coprime to all primes whose square divides N. This takes care of the Manin constant, which only involves primes whose square divides N. To take care of Tamagawa numbers, remove all primes $p \leq 2\dim(A)+1$ from $S_{l,2}$ to obtain S_l.

Remark 5.1. When N is square free we have

$$S_l \mid \#\text{Ш}_?^{\rm odd} \mid S_u$$

since c_A is a power of 2 and no Tamagawa numbers have been omitted from the formulas for S_l and S_u. For every $N \leq 2333$ we found that S_l is an integer, so when $N \leq 2333$ is squarefree, $\#\text{Ш}_?^{\rm odd}$ is an integer. Since Conjecture 2.2 asserts that $\#\text{Ш}_?$ is the order of a group, hence an integer, our data gives evidence for Conjecture 2.2.

Tables 1–4 list every A of level $N \leq 2333$ such that $S_l > 1$. The A column contains the label of A (see Section 3.2), and the next column (labeled dim) contains $\dim A$. A star next to the label for A indicates that we have proved that the odd part of $\#\text{Ш}(A)$ is at least as large as conjectured by the Birch and Swinnerton-Dyer conjecture. *This is the case for* 37 *of the* 168 *examples.* The columns labeled S_l contains the number S_l defined above. If $S_l = S_u$ then the column labeled S_u contains an $=$ sign, and otherwise, it contains S_u (there are only 13 cases in which $S_u \neq S_l$). The column labeled $\text{moddeg}(A)^{\rm odd}$ contains the odd part m of the modular degree of A, written as a product $\gcd(m, S_u)\cdot {\scriptstyle m/\gcd(S_u,m)}$, where ${\scriptstyle m/\gcd(S_u,m)}$ is shrunk to save space. The only non-square-free levels of A_f for which $S_l > 1$ are 1058, 1664, 2224, and 2264.

The column labeled B contains all B such that $L(B,1)=0$ and

$$\gcd(S_l, \#(A^\vee \cap \tilde{B}^\vee)) > 1.$$

(In retrospect, it would probably have been more interesting to list those B such that $\gcd(S_u, \#(A^\vee \cap \tilde{B}^\vee)) > 1$.) Here if $B = A_g$ for some newform g of level dividing N, and $\tilde{B}^\vee$ is the abelian subvariety of $J_0(N)$ generated by all images of $B^\vee$ under the degeneracy maps. Thus, e.g., when $B^\vee$ is of level N, $\tilde{B}^\vee = B^\vee$. The next column, labeled dim, contains the dimension of B.

The final two columns contain information about the relationship between A and B. The one labeled $A^\vee \cap \tilde{B}^\vee$ contains the abelian group structure of the indicated abelian group, where e.g., $[a^b c^d]$ means the abelian group $(\mathbf{Z}/a\mathbf{Z})^b \times (\mathbf{Z}/c\mathbf{Z})^d$. The column labeled Vis contains a divisor of the order of $\text{Vis}_C(\text{Ш}(A^\vee))$, where $C = A^\vee + \tilde{B}^\vee$ (note that $\text{Vis}_C(\text{Ш}(A^\vee)) \subset \text{Vis}_{J_0(N)}(\text{Ш}(A^\vee))$).

The table is divided into three vertical regions, where the columns in the first region are about A only, the columns of the second region are about B only, and the third column is about the relationship between A and B.

5.1. **Example: Level 389.** We illustrate what is involved in computing the first line of Table 1. Using the method sketched in Section 3.2, we find that $S_2(\Gamma_0(389))$ contains exactly five Galois-conjugacy classes of newforms, and these are defined over extensions of $\mathbf{Q}$ of degrees 1, 2, 3, 6, and 20. Thus $J = J_0(389)$ decomposes, up to isogeny, as a product $A_1 \times A_2 \times A_3 \times A_6 \times A_{20}$ of abelian varieties, where $\dim A_d = d$ and A_d is the optimal quotient corresponding to the appropriate Galois-conjugacy class of newforms.

Next we consider the arithmetic of the A_d. Using Theorem 4.5 we find that

$$L(A_1, 1) = L(A_2, 1) = L(A_3, 1) = L(A_6, 1) = 0,$$

and

$$\frac{L(A_{20}, 1)}{\Omega_{A_{20}}} = \frac{5^2 \cdot 2^{11}}{97 \cdot c_A},$$

where c_A is the Manin constant attached to A_{20}, which, by Theorem 4.2, is of the form 2^n with $n \geq 0$. Using the algorithms of Sections 3.5, 3.6, 3.7, we find that $\#A_{20}(\mathbf{Q}) = c_{389} = 97$. Thus Conjecture 2.2 predicts that $\#\text{Ш}(A_{20}) = 5^2 \cdot 2^{11}/c_A$. The following proposition provides support for this conjecture.

Proposition 5.2. *There is a natural inclusion*

$$(\mathbf{Z}/5\mathbf{Z})^2 \cong A_1(\mathbf{Q})/5A_1(\mathbf{Q}) \hookrightarrow \mathrm{Vis}_{J_0(389)}(\text{Ш}(A_{20}^\vee)).$$

Proof. Let $A = A_{20}^\vee$, $B = A_1^\vee$ and $J = A + B \subset J_0(389)$. Using Proposition 3.3, we find that $A \cap B \cong (\mathbf{Z}/4)^2 \times (\mathbf{Z}/5\mathbf{Z})^2$, so $B[5] \subset A$. Since 5 does not divide the numerator of $(389 - 1)/12$, it does not divide the Tamagawa numbers or the orders of the torsion groups, so Theorem 3.13 yields the asserted injection. To see that $(\mathbf{Z}/5\mathbf{Z})^2 \cong A_1(\mathbf{Q})/5A_1(\mathbf{Q})$ use the standard elliptic curves algorithms [Cre97]. □

5.2. **Invisible Elements of Ш(A).** Tables 1–4 suggest that much of $\text{Ш}(A^\vee)$ is invisible in $J_0(N)$. This is because Corollary 3.15 implies that if a prime divides $\#\text{Ш}(A^\vee)$ but not $\mathrm{moddeg}(A^\vee)$ then $\text{Ш}(A^\vee)$ contains an element of order p that is invisible. We find many examples in the table where p divides the conjectural order of $\text{Ш}(A^\vee)$, but $p \nmid \mathrm{moddeg}(A^\vee)$.

Invisible elements might become visible at higher level (see [AS02b, §4.3] for a discussion and example).

5.3. **The Part of Ш(A) That Must be a Perfect Square.** When $\dim A = 1$, properties of the Cassels-Tate pairing imply that if $\text{Ш}(A)$ is finite then $\#\text{Ш}(A)$ is a perfect square, and the fact that one finds in examples (see [Cre97]) that $\#\text{Ш}_?$ is a perfect square is computational evidence for Conjecture 2.2.

In contrast, when the dimension is greater than one, Poonen and Stoll [PS99] discovered Jacobians J such that $\text{Ш}(J)$ has order twice a square, and the second author found for each prime $p < 25000$ an abelian variety A of dimension $p-1$ such that $\#\text{Ш}(A) = pn^2$ for some integer n (see [Ste03]).

Proposition 5.3. *Let $A = A_f$ be a quotient of $J_0(N)$ and ℓ be a prime that does not divide the modular degree of A. Suppose that $\text{Ш}(A)[\ell^\infty]$ is finite. Then $\#\text{Ш}(A)[\ell^\infty]$ is a perfect square.*

Proof. The Cassels-Tate pairing (see [Tat63, §3]) induces a pairing

$$\phi : \text{Ш}(A)[\ell^\infty] \times \text{Ш}(A^\vee)[\ell^\infty] \to \mathbf{Q}/\mathbf{Z}.$$

Since $Ш(A)[\ell^\infty]$ is finite, it follows from [Tat63, Thm. 3.2] that $Ш(A^\vee)[\ell^\infty]$ is also finite and ϕ is non-degenerate. In particular, $\#Ш(A^\vee)[\ell^\infty] = \#Ш(A)[\ell^\infty]$.

Since $J_0(N)$ is a Jacobian, it possesses a canonical polarization arising from the theta divisor; this divisor is rational over $\mathbf{Q}$, since $X_0(N)$ always has a point over $\mathbf{Q}$ (the cusp ∞ is rational). This polarization induces a polarization $\theta : A^\vee \to A$, which also comes from a divisor that is rational over $\mathbf{Q}$. Hence, by [Tat63, Thm. 3.3] (see also [PS99, Thm. 5]), the pairing

$$\phi' : Ш(A^\vee)[\ell^\infty] \times Ш(A^\vee)[\ell^\infty] \to \mathbf{Q}/\mathbf{Z}$$

obtained by composing θ with the pairing ϕ above is alternating.

Since ℓ does not divide the modular degree of A, it does not divide the degree of the isogeny θ. Hence θ induces an isomorphism $Ш(A^\vee)[\ell^\infty] \xrightarrow{\cong} Ш(A)[\ell^\infty]$. Thus by the non-degeneracy of the pairing ϕ, the pairing ϕ' is also non-degenerate. Since ϕ' is also alternating, it follows from arguments similar to those in [Cas63, p. 260] that $\#Ш(A^\vee)[\ell^\infty]$ is a perfect square. Since $\#Ш(A)[\ell^\infty] = \#Ш(A^\vee)[\ell^\infty]$, we see that $\#Ш(A)[\ell^\infty]$ is also a perfect square.

$\square$

For the entries in Tables 1–4, $Ш(A)$ is finite, so if $\ell \nmid \mathrm{moddeg}(A)$ then the ℓ-power part of $\#Ш(A)$ must be a perfect square. When $S_l = S_u$ and the level is square free, then S_l is the odd part of the conjectural order of $Ш(A)$. We found that S_l is a perfect square whenever $S_l = S_u$, which provides evidence for Conjecture 2.2.

Table 1. Visibility of Nontrivial Odd Parts of Shafarevich-Tate Groups

A	dim	S_l	S_u	$\mathrm{moddeg}(A)^{\mathrm{odd}}$	B	dim	$A^\vee \cap \tilde{B}^\vee$	Vis
389E$*$	20	5^2	$=$	5	**389A**	1	$[20^2]$	5^2
433D$*$	16	7^2	$=$	$7\cdot 111$	**433A**	1	$[14^2]$	7^2
446F$*$	8	11^2	$=$	$11\cdot 359353$	**446B**	1	$[11^2]$	11^2
551H	18	3^2	$=$	169	NONE			
563E$*$	31	13^2	$=$	13	**563A**	1	$[26^2]$	13^2
571D$*$	2	3^2	$=$	$3^2\cdot 127$	**571B**	1	$[3^2]$	3^2
655D$*$	13	3^4	$=$	$3^2\cdot 9799079$	**655A**	1	$[36^2]$	3^4
681B	1	3^2	$=$	$3\cdot 125$	**681C**	1	$[3^2]$	$-$
707G$*$	15	13^2	$=$	$13\cdot 800077$	**707A**	1	$[13^2]$	13^2
709C$*$	30	11^2	$=$	11	**709A**	1	$[22^2]$	11^2
718F$*$	7	7^2	$=$	$7\cdot 5371523$	**718B**	1	$[7^2]$	7^2
767F	23	3^2	$=$	1	NONE			
794G	12	11^2	$=$	$11\cdot 34986189$	**794A**	1	$[11^2]$	$-$
817E	15	7^2	$=$	$7\cdot 79$	**817A**	1	$[7^2]$	$-$
959D	24	3^2	$=$	583673	NONE			
997H$*$	42	3^4	$=$	3^2	**997B**	1	$[12^2]$	3^2
					997C	1	$[24^2]$	3^2
1001F	3	3^2	$=$	$3^2\cdot 1269$	**1001C**	1	$[3^2]$	$-$
					91A	1	$[3^2]$	$-$
1001L	7	7^2	$=$	$7\cdot 2029789$	**1001C**	1	$[7^2]$	$-$
1041E	4	5^2	$=$	$5^2\cdot 13589$	**1041B**	2	$[5^2]$	$-$
1041J	13	5^4	$=$	$5^3\cdot 21120929983$	**1041B**	2	$[5^4]$	$-$
1058D	1	5^2	$=$	$5\cdot 483$	**1058C**	1	$[5^2]$	$-$
1061D	46	151^2	$=$	$151\cdot 10919$	**1061B**	2	$[2^2 302^2]$	$-$
1070M	7	$3\cdot 5^2$	$3^2\cdot 5^2$	$3\cdot 5\cdot 1720261$	**1070A**	1	$[15^2]$	$-$
1077J	15	3^4	$=$	$3^2\cdot 1227767047943$	**1077A**	1	$[9^2]$	$-$
1091C	62	7^2	$=$	1	NONE			
1094F$*$	13	11^2	$=$	$11^2\cdot 172446773$	**1094A**	1	$[11^2]$	11^2
1102K	4	3^2	$=$	$3^2\cdot 31009$	**1102A**	1	$[3^2]$	$-$
1126F$*$	11	11^2	$=$	$11\cdot 13990352759$	**1126A**	1	$[11^2]$	11^2
1137C	14	3^4	$=$	$3^2\cdot 64082807$	**1137A**	1	$[9^2]$	$-$
1141I	22	7^2	$=$	$7\cdot 528921$	**1141A**	1	$[14^2]$	$-$
1147H	23	5^2	$=$	$5\cdot 729$	**1147A**	1	$[10^2]$	$-$
1171D$*$	53	11^2	$=$	$11\cdot 81$	**1171A**	1	$[44^2]$	11^2
1246B	1	5^2	$=$	$5\cdot 81$	**1246C**	1	$[5^2]$	$-$
1247D	32	3^2	$=$	$3^2\cdot 2399$	**43A**	1	$[36^2]$	$-$
1283C	62	5^2	$=$	$5\cdot 2419$	NONE			
1337E	33	3^2	$=$	71	NONE			
1339G	30	3^2	$=$	5776049	NONE			
1355E	28	3	3^2	$3^2\cdot 2224523985405$	NONE			
1363F	25	31^2	$=$	$31\cdot 34889$	**1363B**	2	$[2^2 62^2]$	$-$
1429B	64	5^2	$=$	1	NONE			
1443G	5	7^2	$=$	$7^2\cdot 18525$	**1443C**	1	$[7^1 14^1]$	$-$
1446N	7	3^2	$=$	$3\cdot 17459029$	**1446A**	1	$[12^2]$	$-$

Table 2. Visibility of Nontrivial Odd Parts of Shafarevich-Tate Groups

A	dim	S_l	S_u	$\mathrm{moddeg}(A)^{\mathrm{odd}}$	B	dim	$A^\vee \cap \tilde{B}^\vee$	Vis
1466H$*$	23	13^2	$=$	$13\cdot 25631993723$	**1466B**	1	$[26^2]$	13^2
1477C$*$	24	13^2	$=$	$13\cdot 57037637$	**1477A**	1	$[13^2]$	13^2
1481C	71	13^2	$=$	70825	NONE			
1483D$*$	67	$3^2\cdot 5^2$	$=$	$3\cdot 5$	**1483A**	1	$[60^2]$	$3^2\cdot 5^2$
1513F	31	3	3^4	$3\cdot 759709$	NONE			
1529D	36	5^2	$=$	535641763	NONE			
1531D	73	3	3^2	3	**1531A**	1	$[48^2]$	$-$
1534J	6	3	3^2	$3^2\cdot 635931$	**1534B**	1	$[6^2]$	$-$
1551G	13	3^2	$=$	$3\cdot 110659885$	**141A**	1	$[15^2]$	$-$
1559B	90	11^2	$=$	1	NONE			
1567D	69	$7^2\cdot 41^2$	$=$	$7\cdot 41$	**1567B**	3	$[4^4 1148^2]$	$-$
1570J$*$	6	11^2	$=$	$11\cdot 228651397$	**1570B**	1	$[11^2]$	11^2
1577E	36	3	3^2	$3^2\cdot 15$	**83A**	1	$[6^2]$	$-$
1589D	35	3^2	$=$	6005292627343	NONE			
1591F$*$	35	31^2	$=$	$31\cdot 2401$	**1591A**	1	$[31^2]$	31^2
1594J	17	3^2	$=$	$3\cdot 259338050025131$	**1594A**	1	$[12^2]$	$-$
1613D$*$	75	5^2	$=$	$5\cdot 19$	**1613A**	1	$[20^2]$	5^2
1615J	13	3^4	$=$	$3^2\cdot 13317421$	**1615A**	1	$[9^1 18^1]$	$-$
1621C$*$	70	17^2	$=$	17	**1621A**	1	$[34^2]$	17^2
1627C$*$	73	3^4	$=$	3^2	**1627A**	1	$[36^2]$	3^4
1631C	37	5^2	$=$	6354841131	NONE			
1633D	27	$3^6\cdot 7^2$	$=$	$3^5\cdot 7\cdot 31375$	**1633A**	3	$[6^4 42^2]$	$-$
1634K	12	3^2	$=$	$3\cdot 3311565989$	**817A**	1	$[3^2]$	$-$
1639G$*$	34	17^2	$=$	$17\cdot 82355$	**1639B**	1	$[34^2]$	17^2
1641J$*$	24	23^2	$=$	$23\cdot 1491344147471$	**1641B**	1	$[23^2]$	23^2
1642D$*$	14	7^2	$=$	$7\cdot 123398360851$	**1642A**	1	$[7^2]$	7^2
1662K	7	11^2	$=$	$11\cdot 16610917393$	**1662A**	1	$[11^2]$	$-$
1664K	1	5^2	$=$	$5\cdot 7$	**1664N**	1	$[5^2]$	$-$
1679C	45	11^2	$=$	6489	NONE			
1689E	28	3^2	$=$	$3\cdot 172707180029157365$	**563A**	1	$[3^2]$	$-$
1693C	72	1301^2	$=$	1301	**1693A**	3	$[2^4 2602^2]$	$-$
1717H$*$	34	13^2	$=$	$13\cdot 345$	**1717B**	1	$[26^2]$	13^2
1727E	39	3^2	$=$	118242943	NONE			
1739F	43	659^2	$=$	$659\cdot 151291281$	**1739C**	2	$[2^2 1318^2]$	$-$
1745K	33	5^2	$=$	$5\cdot 1971380677489$	**1745D**	1	$[20^2]$	$-$
1751C	45	5^2	$=$	$5\cdot 707$	**103A**	2	$[505^2]$	$-$
1781D	44	3^2	$=$	61541	NONE			
1793G$*$	36	23^2	$=$	$23\cdot 8846589$	**1793B**	1	$[23^2]$	23^2
1799D	44	5^2	$=$	201449	NONE			
1811D	98	31^2	$=$	1	NONE			
1829E	44	13^2	$=$	3595	NONE			
1843F	40	3^2	$=$	8389	NONE			
1847B	98	3^6	$=$	1	NONE			
1871C	98	19^2	$=$	14699	NONE			

Table 3. Visibility of Nontrivial Odd Parts of Shafarevich-Tate Groups

A	dim	S_l	S_u	$\mathrm{moddeg}(A)^{\mathrm{odd}}$	B	dim	$A^\vee \cap \tilde{B}^\vee$	Vis
1877B	86	7^2	=	1	NONE			
1887J	12	5^2	=	$5 \cdot 10825598693$	**1887A**	1	$[20^2]$	–
1891H	40	7^4	=	$7^2 \cdot 44082137$	**1891C**	2	$[4^2 196^2]$	–
1907D$*$	90	7^2	=	$7 \cdot 165$	**1907A**	1	$[56^2]$	7^2
1909D$*$	38	3^4	=	$3^2 \cdot 9317$	**1909A**	1	$[18^2]$	3^4
1913B$*$	1	3^2	=	$3 \cdot 103$	**1913A**	1	$[3^2]$	3^2
1913E	84	$5^4 \cdot 61^2$	=	$5^2 \cdot 61 \cdot 103$	**1913A**	1	$[10^2]$	–
					1913C	2	$[2^2 610^2]$	–
1919D	52	23^2	=	675	NONE			
1927E	45	3^2	3^4	52667	NONE			
1933C	83	$3^2 \cdot 7$	$3^2 \cdot 7^2$	$3 \cdot 7$	**1933A**	1	$[42^2]$	3^2
1943E	46	13^2	=	62931125	NONE			
1945E$*$	34	3^2	=	$3 \cdot 571255479184807$	**389A**	1	$[3^2]$	3^2
1957E$*$	37	$7^2 \cdot 11^2$	=	$7 \cdot 11 \cdot 3481$	**1957A**	1	$[22^2]$	11^2
					1957B	1	$[14^2]$	7^2
1979C	104	19^2	=	55	NONE			
1991C	49	7^2	=	1634403663	NONE			
1994D	26	3	3^2	$3^2 \cdot 46197281414642501$	**997B**	1	$[3^2]$	–
1997C	93	17^2	=	1	NONE			
2001L	11	3^2	=	$3^2 \cdot 44513447$	NONE			
2006E	1	3^2	=	$3 \cdot 805$	**2006D**	1	$[3^2]$	–
2014L	12	3^2	=	$3^2 \cdot 126381129003$	**106A**	1	$[9^2]$	–
2021E	50	5^6	=	$5^2 \cdot 729$	**2021A**	1	$[100^2]$	5^4
2027C$*$	94	29^2	=	29	**2027A**	1	$[58^2]$	29^2
2029C	90	$5^2 \cdot 269^2$	=	$5 \cdot 269$	**2029A**	2	$[2^2 2690^2]$	–
2031H$*$	36	11^2	=	$11 \cdot 1014875952355$	**2031C**	1	$[44^2]$	11^2
2035K	16	11^2	=	$11 \cdot 218702421$	**2035C**	1	$[11^1 22^1]$	–
2038F	25	5	5^2	$5^2 \cdot 92198576587$	**2038A**	1	$[20^2]$	–
					1019B	1	$[5^2]$	–
2039F	99	$3^4 \cdot 5^2$	=	13741381043009	NONE			
2041C	43	3^4	=	61889617	NONE			
2045I	39	3^4	=	$3^3 \cdot 3123399893$	**2045C**	1	$[18^2]$	–
					409A	13	$[9370199679^2]$	–
2049D	31	3^2	=	29174705448000469937	NONE			
2051D	45	7^2	=	$7 \cdot 674652424406369$	**2051A**	1	$[56^2]$	–
2059E	45	$5 \cdot 7^2$	$5^2 \cdot 7^2$	$5^2 \cdot 7 \cdot 167359757$	**2059A**	1	$[70^2]$	–
2063C	106	13^2	=	8479	NONE			
2071F	48	13^2	=	36348745	NONE			
2099B	106	3^2	=	1	NONE			
2101F	46	5^2	=	$5 \cdot 11521429$	**191A**	2	$[155^2]$	–
2103E	37	$3^2 \cdot 11^2$	=	$3^2 \cdot 11 \cdot 87441292307157179261 1$	**2103B**	1	$[33^2]$	11^2
2111B	112	211^2	=	1	NONE			
2113B	91	7^2	=	1	NONE			
2117E$*$	45	19^2	=	$19 \cdot 1078389$	**2117A**	1	$[38^2]$	19^2

Table 4. Visibility of Nontrivial Odd Parts of Shafarevich-Tate Groups

A	dim	S_l	S_u	$\mathrm{moddeg}(A)^{\mathrm{odd}}$	B	dim	$A^\vee \cap \tilde{B}^\vee$	Vis
2119C	48	7^2	$=$	89746579	NONE			
2127D	34	3^2	$=$	$3\cdot 18740561792121901$	**709A**	1	$[3^2]$	$-$
2129B	102	3^2	$=$	1	NONE			
2130Y	4	7^2	$=$	$7\cdot 83927$	**2130B**	1	$[14^2]$	$-$
2131B	101	17^2	$=$	1	NONE			
2134J	11	3^2	$=$	1710248025389	NONE			
2146J	10	7^2	$=$	$7\cdot 1672443$	**2146A**	1	$[7^2]$	$-$
2159E	57	13^2	$=$	31154538351	NONE			
2159D	56	3^4	$=$	233801	NONE			
2161C	98	23^2	$=$	1	NONE			
2162H	14	3	3^2	$3\cdot 6578391763$	NONE			
2171E	54	13^2	$=$	271	NONE			
2173H	44	199^2	$=$	$199\cdot 3581$	**2173D**	2	$[398^2]$	$-$
2173F	43	19^2	$3^2\cdot 19^2$	$3^2\cdot 19\cdot 229341$	**2173A**	1	$[38^2]$	19^2
2174F	31	5^2	$=$	$5\cdot 21555702093188316107$	NONE			
2181E	27	7^2	$=$	$7\cdot 7217996450474835$	**2181A**	1	$[28^2]$	$-$
2193K	17	3^2	$=$	$3\cdot 15096035814223$	**129A**	1	$[21^2]$	$-$
2199C	36	7^2	$=$	$7^2\cdot 13033437060276603$	NONE			
2213C	101	3^4	$=$	19	NONE			
2215F	46	13^2	$=$	$13\cdot 1182141633$	**2215A**	1	$[52^2]$	$-$
2224R	11	79^2	$=$	79	**2224G**	2	$[79^2]$	$-$
2227E	51	11^2	$=$	259	NONE			
2231D	60	47^2	$=$	91109	NONE			
2239B	110	11^4	$=$	1	NONE			
2251E$*$	99	37^2	$=$	37	**2251A**	1	$[74^2]$	37^2
2253C$*$	27	13^2	$=$	$13\cdot 14987929400988647$	**2253A**	1	$[26^2]$	13^2
2255J	23	7^2	$=$	15666366543129	NONE			
2257H	46	$3^6\cdot 29^2$	$=$	$3^3\cdot 29\cdot 175$	**2257A**	1	$[9^2]$	$-$
					2257D	2	$[2^2 174^2]$	$-$
2264J	22	73^2	$=$	73	**2264B**	2	$[146^2]$	$-$
2265U	14	7^2	$=$	$7^2\cdot 73023816368925$	**2265B**	1	$[7^2]$	$-$
2271I$*$	43	23^2	$=$	$23\cdot 392918345997771783$	**2271C**	1	$[46^2]$	23^2
2273C	105	7^2	$=$	7^2	NONE			
2279D	61	13^2	$=$	96991	NONE			
2279C	58	5^2	$=$	1777847	NONE			
2285E	45	151^2	$=$	$151\cdot 138908751161$	**2285A**	2	$[2^2 302^2]$	$-$
2287B	109	71^2	$=$	1	NONE			
2291C	52	3^2	$=$	427943	NONE			
2293C	96	479^2	$=$	479	**2293A**	2	$[2^2 958^2]$	$-$
2294F	15	3^2	$=$	$3\cdot 6289390462793$	**1147A**	1	$[3^2]$	$-$
2311B	110	5^2	$=$	1	NONE			
2315I	51	3^2	$=$	$3\cdot 4475437589723$	**463A**	16	$[13426312769169^2]$	$-$
2333C	101	83341^2	$=$	83341	**2333A**	4	$[2^6 166682^2]$	$-$

6. Appendix by J. Cremona and B. Mazur: "Explaining" Shafarevich-Tate via Mordell-Weil

Introduction. In our article [CM] we discussed the notion of visibility and offered some tables of examples of that phenomenon. We gave, however, very little theoretical discussion in that article. Here we wish to take the opportunity to correct some gaps in our commentary on our tables and to offer the details of the proof of a general criterion that is sometimes useful to test visibility. Regarding Table 1 of [CM] we said that for each pair (E, p) that occurs there and for which there is a corresponding "F" on the table of the same conductor of E, the Shafarevich-Tate group of E is *explained* by the Mordell-Weil group of F, in the technical sense that we gave to the word *explained* in that article. Now this is indeed the case for all entries of our table such that E has semistable reduction at p and it is also the case for those entries where the conductor of F properly divides the conductor of E. We will review why this is so, below. It is also true that for each of the remaining 7 entries ($E =$ **2601H**, **2718D**, **2900D**, **3555E**, **3879E**, **3933A**, **5499E**) a nontrivial subgroup of the Shafarevich-Tate group of E is *explained* by the Mordell-Weil group of the corresponding F, but we wish to notify our readers that we have not yet checked whether or not *all* of the "Ш" of these 7 elliptic curves is so explained. These 7 cases deserve to be looked at (the issue being local at the prime 3 for all but **2900D**, where it is local at the prime 5). Regarding Table 2 of [CM], although our commentary in [CM] does not say this clearly, for all the entries E of that table for which there is a corresponding F of the same conductor we only have checked that $E[2] = F[2]$ in $J_0(N)$ and nothing more, except, of course, for those entries we particularly signal to have shown something less; namely, in the language of our article, that they "seem to satisfy a 2-congruence." In these latter cases where we signal that we have shown something less, W. Stein has checked that in fact $E[2] \neq F[2]$ in $J_0(N)$.

Let p be an odd prime number. If E is an (optimal) elliptic curve over $\mathbf{Q}$ of conductor N then E may be unambiguously identified (up to sign) with a sub-abelian variety of the modular jacobian $J_0(N)$ (over $\mathbf{Q}$). If (E, F, p) is an entry of Table 1 of [CM] such that E and F are of the same conductor N we checked that we have equality of the finite group schemes $E[p]_{/\mathbf{Q}} = F[p]_{/\mathbf{Q}}$ in $J_0(N)_{/\mathbf{Q}}$. For the remaining three entries we checked that there is an isomorphism of finite group schemes $\iota : E[p]_{/\mathbf{Q}} \cong F[p]_{/\mathbf{Q}}$. In both cases, identifying the two finite group schemes let H denote the common cohomology group,

$$H := H^1(G_{\mathbf{Q}}, E[p]_{/\mathbf{Q}}) = H^1(G_{\mathbf{Q}}, F[p]_{/\mathbf{Q}}),$$

and $S_E \subset H$, and $S_F \subset H$ the p-Selmer groups of, respectively, E and F. What we will show is that

Proposition 6.1. *For each of the entries (E, p) in Table 1 of* [CM] *such that p is a prime of semistable reduction for E and for which there is a "corresponding" F, we have*

$$S_E = S_F \subset H.$$

To discuss this, we need some notation.

Let $X := \mathrm{Spec}(\mathbf{Z})$, $Y := \mathrm{Spec}(\mathbf{Z}[1/p]) = X - \mathrm{Spec}(\mathbf{F}_p)$, and $\eta := \mathrm{Spec}(\mathbf{Q})$. Let $E_\eta := E$ be our elliptic curve over $\mathbf{Q}$ of conductor N, $E_{/X}$ the Néron model over X of E_η and $E^o_{/X} \subset E_{/X}$ the "connected component" of Néron (meaning the open subgroup scheme every fiber of which is connected). We have, of course, similar notation for the corresponding elliptic curve F. Let $E[p]_{/X}$ denote the closed subgroup scheme given as the kernel of multiplication by p in the Néron model: $E[p]_{/X} \subset E_{/X}$. We have, in general, that the restriction $E[p]_{/Y}$ of $E[p]_{/X}$ to the base Y is an étale quasi-finite flat group scheme; and if p^2 doesn't divide N we have that the group scheme $E[p]_{/X}$ is a quasi-finite flat group scheme [Gro72, Prop. 3.1(d), pg. 343]. The étale quasi-finite flat group scheme $E[p]_{/Y}$ can be characterized by the following features:

(i) Its generic fiber is the group scheme $E[p]_{/\eta} \subset J_0(N)_{/\eta}$,

and (one has a choice here) either:

(ii) $E[p]_{/Y} \subset J_0(N)_{/Y}$ is a closed étale quasi-finite flat) subgroup scheme,

or:

(ii') $E[p]_{/Y}$ enjoys the Néronian property over the base Y.

Similar statements hold for $F[p]_{/X}$.

Let Φ be the (punctual) sheaf of abelian groups for the flat topology over X which fits into the exact sequence (of abelian sheaves over X)

$$0 \to E^o \to E \to \Phi \to 0. \tag{1}$$

We will use the same notation to indicate the corresponding exact sequence of sheaves for the étale topology over X. Since E^0 and E are smooth group schemes, the long exact sequences of cohomology derived from the short exact sequence (1), viewed either as sheaves of abelian groups for the flat or étale topology, coincide; cf Section 11 *Appendice: Un théorème de comparaison de la cohomologie étale et de la cohomologie fppf* in [Gro68]. Thinking now of Φ as a sheaf for the étale topology, denote by Φ_ℓ its stalk at the prime ℓ. So Φ_ℓ is representable as a finite étale group scheme over the field $\mathbf{F}_\ell$. We have that

$$\Phi = \bigoplus_{\ell \mid N} (i_\ell)_* \Phi_\ell,$$

where $i_\ell : \mathrm{Spec}\mathbf{F}_\ell \hookrightarrow X$ is the natural closed immersion. We have an exact sequence

$$0 \to E^o(X) \to E(\mathbf{Q}) \to H^0(X,\Phi) \to H^1(X,E^o) \to H^1(X,E) \to H^1(X,\Phi), \tag{2}$$

where cohomology is computed for the étale topology. We have, for either topology,

$$H^i(X,\Phi) = \bigoplus_{\ell \mid N} H^i(\mathrm{Spec}(\mathbf{F}_\ell), \Phi_\ell).$$

Viewing (1) as an exact sequence of sheaves for the flat topology, and passing to the associated cohomology sequence we see that (2) may be thought of, ambiguously as computed for either the étale or the flat topology.

If p is an odd prime number, the p-primary component of the Shafarevich-Tate group of E is the p-primary component of the image of $H^1(X,E^o) \to H^1(X,E)$ (see the appendix to [Maz72]), or equivalently the intersection of the kernels of

$$H^1(X,E) \to H^1(\mathrm{Spec}(\mathbf{F}_\ell), \Phi_\ell).$$

Let p be an odd prime number. Let $E' \subset E$ be the open subgroup scheme of E which is the inverse image of $p\Phi \subset \Phi$, so that we have an exact sequence of sheaves for the flat (or étale) topology:

$$0 \to E' \to E \to \Phi/p\Phi \to 0, \tag{3}$$

and if p is a prime of semistable reduction for E (equivalently: p^2 doesn't divide N) we have an exact sequence of flat group schemes

$$0 \to E[p] \to E \to E' \to 0. \tag{4}$$

Put

$$E[p]^o_{/X} := E[p]_{/X} \bigcap E^o_{/X}.$$

Then $E[p]^o_{/X}$ is an open (quasi-finite) subgroup scheme of $E[p]_{/X}$. Let $\tilde{E}[p]_{/X}$ be any "intermediate" open (quasi-finite) subgroup scheme

$$E[p]^o_{/X} \subset \tilde{E}[p]_{/X} \subset E[p]_{/X}$$

so that we have the exact sequence of sheaves for the finite flat topology

$$0 \to \tilde{E}[p]_{/X} \to E[p]_{/X} \to \Psi \to 0, \tag{5}$$

with Ψ a subquotient of Φ.

Consider the following hypothesis:

$\mathbf{A}(E, p, \ell)$: The Galois module $\Phi_\ell/p\Phi_\ell$ is either trivial, or else is a non-constant cyclic Galois module over $\mathbf{F}_\ell$.

Let $\mathbf{A}(E, p)$ denote the conjunction of Hypotheses $\mathbf{A}(E, p, \ell)$ for all prime numbers ℓ, or equivalently, for all ℓ dividing N.

Lemma 6.2. *These are equivalent formulations of Hypothesis* $\mathbf{A}(E, p)$*.*

(a) *$\Phi/p\Phi$ is cohomologically trivial; that is,* $H^0(X, \Phi/p\Phi) = H^1(X, \Phi/p\Phi) = 0$*.*
(b) *If Ψ is any subquotient of Φ, Ψ is "p-cohomologically trivial" in the sense that the p-primary components of $H^i(X, \Psi)$ vanish for all i.*

Moreover, if $p \geq 5$, or if $p = 3$ and E has no Néron fibers of type IV or IV, the above conditions are equivalent to:*

(c) *For every ℓ at which E has split multiplicative reduction, p does not divide the order of the group of connected components of the Néron fiber of E at ℓ.*

Proof. The equivalence of Hypothesis $\mathbf{A}(E, p)$ with (a) and with (b) is straightforward using standard exact sequences plus the fact that the p-primary components of the (underlying abelian group of) Φ_ℓ is cyclic since $p > 2$; and noting that a (finite) G-module of prime order with nontrivial G-action has trivial cohomology. For (c) we are using that if $p > 2$ the p-primary component of Φ_ℓ vanishes for all primes ℓ of additive reduction for E except when $p = 3$ and the Néron fiber type of E at ℓ is IV or IV*. $\square$

A morphism $G_1 \to G_2$ of flat (commutative, finite type) groups schemes over X will be said to *induce an isomorphism on p-cohomology* if the induced mappings

$$H^i(X, G_1) \otimes \mathbf{Z}_p \to H^i(X, G_2) \otimes \mathbf{Z}_p$$

are isomorphisms for all $i \geq 0$, where cohomology is computed for the flat topology.

Lemma 6.3. *Let p be an odd prime number for which $\mathbf{A}(E, p)$ holds. We have that the natural morphisms*

$$E^o_{/X} \to E'_{/X} \qquad \text{and} \qquad E'_{/X} \to E_{/X}$$

induce isomorphisms on p-cohomology. If p is of semistable reduction for E, we also have that

$$\tilde{E}[p]_{/X} \to E[p]_{/X}$$

induces isomorphisms on p-cohomology, for any of the open subgroup schemes $\tilde{E}[p]_{/X}$ in $E[p]_{/X}$ described above.

Proof. These all sit in short exact sequences of sheaves of abelian groups for the flat topology over X where the third sheaf is p-cohomologically trivial. □

Corollary 6.4. *If $p > 2$ and $\mathbf{A}(E,p)$ holds we have natural isomorphisms*

$$H^0(X, E^o) \otimes \mathbf{Z}_p \cong H^0(X, E') \otimes \mathbf{Z}_p \cong E(\mathbf{Q}) \otimes \mathbf{Z}_p$$

and

$$Ш(E) \otimes \mathbf{Z}_p \cong H^1(X, E^o) \otimes \mathbf{Z}_p \cong H^1(X, E') \otimes \mathbf{Z}_p \cong H^1(X, E) \otimes \mathbf{Z}_p.$$

Corollary 6.5. *Let p be an odd prime number, semistable for E, and suppose that $\mathbf{A}(E,p)$ holds.*

(i) *The image of the natural (injective) coboundary mapping*

$$0 \to E(\mathbf{Q})/pE(\mathbf{Q}) \hookrightarrow H^1(G_{\mathbf{Q}}, E[p])$$

attached to the Kummer sequence is contained in the image of the natural injection

$$H^1(X, E[p]^o) \hookrightarrow H^1(G_{\mathbf{Q}}, E[p]).$$

(ii) *We have an exact sequence*

$$0 \to E(\mathbf{Q})/pE(\mathbf{Q}) \to H^1(X, \tilde{E}[p]) \to Ш(E)[p] \to 0$$

for any of the open subgroup schemes $\tilde{E}[p]_{/X} \subset E[p]_{/X}$ defined above.

(iii) *The image of $H^1(X, \tilde{E}[p]) \hookrightarrow H^1(G_{\mathbf{Q}}, E[p])$ is equal to the p-Selmer subgroup,*

$$S_p(E) \subset H^1(G_{\mathbf{Q}}, E[p]).$$

Proof. All this follows from straightforward calculations using the cohomological exact sequences associated to the exact sequences (1)–(5) in the light of the previous discussion. □

To set things up for our application, let us record the following:

Corollary 6.6. *Let $E_{/\mathbf{Q}}$ and $F_{/\mathbf{Q}}$ be elliptic curves over $\mathbf{Q}$. Let p be an odd prime number of semistable reduction for E and F, and for which $\mathbf{A}(E,p)$ and $\mathbf{A}(F,p)$ both hold. Define $\tilde{E}[p]_{/X} \subset E[p]_{/X}$ to be the open quasi-finite subgroup scheme whose restriction to Y is equal to $E[p]_{/Y}$ and whose fiber at $\mathbf{F}_p$ is equal to $E[p]^o_{/\mathbf{F}_p} = (E[p] \bigcap E^o)_{/\mathbf{F}_p}$. Define $\tilde{F}[p]_{/X}$ similarly. Suppose, finally, that we have an isomorphism of $G_{\mathbf{Q}}$-modules $\iota : F[p]_{/\mathbf{Q}} \cong E[p]_{/\mathbf{Q}}$ which extends to an injection of quasi-finite flat group schemes*

$$\tilde{F}[p]_{/X} \hookrightarrow \tilde{E}[p]_{/X}.$$

Letting

$$H := H^1(G_{\mathbf{Q}}, E[p]) = H^1(G_{\mathbf{Q}}, F[p])$$

(making the identification via ι) we have that the p-Selmer groups $S_p(E) \subset H$ and $S_p(F) \subset H$ are the same.

Proposition 6.7. *Let (E, F, p) be a triple which is an entry of Table 1 of* [CM]*. Suppose further that p is of semistable reduction for E and for F. Then, with the notation of the previous corollary, the p-Selmer groups $S_p(E) \subset H$ and $S_p(F) \subset H$ are the same. In the terminology of* [CM] *the Shafarevich-Tate group of E is explained by the Mordell-Weil group of F.*

Proof. As mentioned above, we have checked that $E[p]_{/\mathbf{Q}} = F[p]_{/\mathbf{Q}} \subset J_0(N)$ whenever the pair E and F (appearing as entry of Table 1 of [CM]) have the same conductor. We have checked that $E[p]_{/\mathbf{Q}} \cong F[p]_{/\mathbf{Q}}$ for the three entries where E and F have different conductor ($E =$ **2932A**, **3306B**, and **5136B**). We have checked that Hypothesis $A(E, p, \ell)$ and $A(F, p, \ell)$ hold for all quadruples (E, F, p, ℓ) such that (E, F, p) occurs as an entry in Table 1 of [CM] (even when p is not semistable for E and F) with the exception of the entry $(E, F, p, \ell) = (\mathbf{2366D}, \mathbf{2366E}, 3, 13)$.

Sublemma 6.8. *Under the hypotheses of our proposition, the isomorphism of $G_{\mathbf{Q}}$-modules $\iota : E[p]_{/\mathbf{Q}} \cong F[p]_{/\mathbf{Q}}$ extends to an injection of quasi-finite flat group schemes*

$$\tilde{E}[p]_{/X} \hookrightarrow \tilde{F}[p]_{/X}$$

which is an isomorphism except in two instances ($E =$ **3306B***, and* **5136B***).*

Proof. First, since $\tilde{E}[p]_{/Y} = E[p]_{/Y}$, $\tilde{F}[p]_{/Y} = F[p]_{/Y}$, and, as we mentioned at the beginning, both of these quasi-finite, flat (étale) group schemes $F[p]_{/Y}$ and $E[p]_{/Y}$ enjoy the Néronian property, the isomorphism ι extends to an isomorphism $\tilde{E}[p]_{/Y} \cong \tilde{F}[p]_{/Y}$. The remaining question is then local about p. If p is of good reduction for E, then $\tilde{E}[p]_{/X_p}$ and $\tilde{F}[p]_{/X_p}$ are both finite flat group schemes of odd order, so by Fontaine's Theorem [Fon75], the isomorphism between their generic fibers extends to an isomorphism over X_p. (Compare: Theorem I.1.4 in [Maz77].) A standard result allows us to *patch* the isomorphism extending ι over Y with the isomorphism ("extending ι") over X_p to get the extension of ι to an isomorphism of group schemes over X, $\tilde{E}[p]_{/X} \cong \tilde{F}[p]_{/X}$. Now consider the case where p is of bad reduction. By the assumptions of our proposition, p is then of multiplicative reduction for E, and hence the fiber of E over $\mathbf{F}_p$ is a finite multiplicative type group scheme of order p. We therefore have that $\tilde{E}[p]_{/X_p}$ sits in an exact sequence

$$0 \to \mathcal{C}_{/X_p} \to \tilde{E}[p]_{/X_p} \to \mathcal{E}_{/X_p} \to 0 \tag{6}$$

where $\mathcal{C}_{/X_p}$ is a finite flat group scheme of order p (and with fiber of multiplicative type in characteristic p) and where $\mathcal{E}_{/X_p}$ is an étale quasi-finite group scheme, with trivial fiber in characteristic p.

Let us take a moment to recall (see [Maz78, Lem. 1.1]) the construction of such an exact sequence (6): working in the category of formal schemes, let $\hat{X}_p := \mathrm{Spf}(\mathbf{Z}_p)$, and let $\hat{\mathcal{C}}_{/\hat{X}_p}$ be the formal completion of the zero-section in $\tilde{E}[p]_{/X_p}$. One checks that $\hat{\mathcal{C}}_{/\hat{X}_p}$ may be identified with a finite flat formal group scheme over $\hat{X}_p$ which admits a closed immersion into the formal group scheme over $\hat{X}_p$ associated to $\tilde{E}[p]_{/X_p}$. A standard algebrization argument establishes that there is a (unique) finite flat subgroup scheme $\mathcal{C}_{/X_p} \subset \tilde{E}[p]_{/X_p}$ whose associated formal group scheme over $\hat{X}_p$ is $\hat{\mathcal{C}}_{/\hat{X}_p}$. The exact sequence (6) is then obtained by letting $\mathcal{E}_{/X_p}$ be the evident quotient (quasi-finite flat) group scheme, and noting that, by construction, its special fiber is trivial.

Now let us return to the proof of the sublemma. Since the restriction of ι to $\mathcal{C}_{/X_p}$ (a finite flat multiplicative type group scheme of order p) is injective over the generic point, it follows (by elementary considerations, or by Fontaine's Theorem cited above) that ι restricted to $\mathcal{C}_{/X_p}$ is an injection over X_p. Since $\mathcal{E}_{/X_p}$ has trivial fiber in characteristic p, ι is an injection as was to be proved. In all cases under consideration, then,

$$\iota : \tilde{E}[p]_{/X} \hookrightarrow \tilde{F}[p]_{/X}$$

is an injection. If E is of good reduction at p, or if F is of bad reduction at p, ι is therefore an isomorphism. The cases remaining are when E is of bad reduction at p and F is of good reduction (i.e., $E =$ **3306B**, and **5136B**) in which case we can only assert that ι is an injection. $\square$

Returning to our proposition, suppose that $\tilde{F}[p]_{/X_p}$ is finite flat (which happens in the two cases signalled above: $E =$ **3306B**, and **5136B**). Then the isomorphism induced by ι on generic fibers

$$\tilde{E}[p]_{/\mathbf{Q}_p} \cong \tilde{F}[p]_{/\mathbf{Q}_p}$$

restricted to the $G_{\mathbf{Q}_p}$-stable subgroup $\mathcal{C}_{/\mathbf{Q}_p} \subset \tilde{E}[p]_{/\mathbf{Q}_p}$ extends to a morphism of the finite flat group scheme $\mathcal{C}_{/X_p}$ into $\tilde{F}[p]_{/X_p}$. This extended morphism $j : \mathcal{C}_{/X_p} \to \tilde{F}[p]_{X_p}$ is necessarily a closed immersion since $\mathcal{C}_{/X_p}$ is a multiplicative type finite flat group scheme. Since $\mathcal{E}_{/X_p}$ has trivial fiber in characteristic p an application of the standard patching argument (as used in the previous case) allows us to put together the isomorphism of group schemes over Y extending ι with the closed immersion j over X_p to get a closed immersion

$$\tilde{E}[p]_{/X} \hookrightarrow \tilde{F}[p]_{/X}.$$

Finally suppose that both E and F have multiplicative reduction at p. We then have exact sequences (**6**) for each of our quasi-finite flat group schemes $\tilde{E}[p]_{/X_p}$ and $\tilde{F}[p]_{/X_p}$. Let V denote their common generic fiber (identified via ι) considered as two-dimensional $\mathbf{F}_p$-vector space with $G_{\mathbf{Q_p}}$-action. Let $\mathcal{C}(E) \subset V$ and $\mathcal{C}(F) \subset V$ denote the one-dimensional subspaces given by the generic fibers of the finite flat subgroup schemes $\mathcal{C}_{/X_p}$ corresponding to the exact sequence (6) for for E and for F respectively. Suppose, first, that these one-dimensional $\mathbf{F}_p$-subspaces $\mathcal{C}(E)$ and $\mathcal{C}(F)$ are different. It then follows that the $G_{\mathbf{Q}_p}$-representation V splits as the direct sum of $\mathcal{C}(E)$ and $\mathcal{C}(F)$, both $\mathbf{F}_p$-subspaces being isomorphic, as $I_{\mathbf{Q_p}}$-modules to μ_p, where $I_{\mathbf{Q_p}} \subset G_{\mathbf{Q_p}}$ is the inertia subgroup of $G_{\mathbf{Q}_p}$. But this contradicts the fact that V is self-Cartier dual (under the Weil pairing). Consequently, $\mathcal{C}(E) = \mathcal{C}(F) \subset V$. From the above discussion it follows that we can extend ι to an isomorphism $\tilde{E}[p]_{/X_p} \cong \tilde{F}[p]_{/X_p}$.

Our proposition then follows (from Corollary 6.6) for all entries in Table 1 of [CM] where p is of semistable reduction for E once we produce special arguments to cover the three special cases $E =$ **3306B**, **5136B** and **2366D**. The first two of these cases are "special" because we only have an injection $\tilde{E}[p]_{/X_p} \hookrightarrow \tilde{F}[p]_{/X_p}$ and not an isomorphism. However, the cokernel of this morphism restricted to the fiber in characteristic 3 is, in both of these cases, a cyclic group with nontrivial $G_{\mathbf{Q_3}}$-action and hence is 3-cohomologically trivial. In particular, the injection $\tilde{E}[p]_{/X_p} \hookrightarrow \tilde{F}[p]_{/X_p}$ induces an isomorphism on flat cohomology over X, and the argument for these two cases proceeds as before. This leaves $(E, F, p) = (\mathbf{2366D}, \mathbf{2366E}, 3)$

which is the only example of an entry (E, F, p) in our table, where E has a $\mathbf{Q}$-rational point of order p, and (this is no accident) where Hypothesis $\mathbf{A}(E, p)$ and Hypothesis $\mathbf{A}(F, p)$ fail. (Indeed there are no other failures of Hypothesis $\mathbf{A}(F, p)$ for any of the (E, F, p)'s occurring in Table 1 of [CM] and only one other failure of Hypothesis $\mathbf{A}(E, p)$, which is for $(E, p, \ell) = (\mathbf{2932A}, 3, 2)$.)

Let us now deal with the case $(E, F, p) = (\mathbf{2366D}, \mathbf{2366E}, 3)$. The subgroup C of $\mathbf{Q}$-rational points of order 3 on E specialize in characteristic 13 to yield an isomorphism

$$C \cong \Phi_{13}$$

and the same for the subgroup of $\mathbf{Q}$-rational points of order 3 on F. We make use of this information to cut down the group schemes $\tilde{E}[3]_{/X}$ and $\tilde{F}[3]_{/X}$ and define open subgroup schemes: $\tilde{\tilde{E}}[3]_{/X} \subset \tilde{E}[3]_{/X}$ and $\tilde{\tilde{E}}[3]_{/X} \subset \tilde{E}[3]_{/X}$ by requiring that these closed immersions of subgroup schemes be isomorphisms outside characteristic 13, and that the "double-tilded" group schemes each have trivial fiber in characteristic 13. We get via the above argument an isomorphism of group schemes $\tilde{\tilde{E}}[3]_{/X} \cong \tilde{\tilde{F}}[3]_{/X}$ extending ι, and an identification of the 3-Selmer groups of E and F with $H^1(X, \tilde{\tilde{E}}[3])$ and $H^1(X, \tilde{\tilde{F}}[3])$ respectively. Our proposition is proved. $\square$

It remains to say a few words about why, in the 7 cases of entries (E, F, p) in our Table 1 of [CM] for which p is a prime of additive reduction for E *some* nontrivial elements of the Shafarevich-Tate group of E are explained by the Mordell-Weil group of F. Briefly, the reason is as follows. By the *inflated* p-Selmer group of E (and of F) let us mean the subgroup of H obtained by insisting upon all the local Selmer conditions at primes different from p, but putting no condition at p. The p-Selmer group of E (and of F) are, in all 7 instances, $\mathbf{F}_p$-vector spaces of dimension 2 and therefore, the inflated p-Selmer groups are of dimensions either 2 or 3. Working over Y rather than over X, the above argument applied to these 7 remaining cases gives us an identification of the *inflated* p-Selmer groups of E and of F in H. But the true p-Selmer groups (vector spaces of dimension 2) being subspaces in a vector space of dimension ≤ 3 must have a nontrivial intersection.

References

[Aga99] A. Agashe, *On invisible elements of the Tate-Shafarevich group*, C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), no. 5, 369–374. MR **2000e**:11083

[AS] A. Agashe and W. A. Stein, Appendix to Joan-C. Lario and René Schoof: *Some computations with Hecke rings and deformation rings*, to appear in J. Exp. Math.

[AS02a] A. Agashe and W. A. Stein, *The generalized Manin constant, congruence primes, and the modular degree*, In preparation (2002).

[AS02b] A. Agashe and W. A. Stein, *Visibility of Shafarevich-Tate Groups of Abelian Varieties*, to appear in J. of Number Theory (2002).

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1 484 478

[Bir71] B. J. Birch, *Elliptic curves over* $\mathbf{Q}$*: A progress report*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, R.I., 1971, pp. 396–400. MR **47**:3395

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990. MR **91i**:14034

[Cas63] J. W. S. Cassels, *Corrigendum: "Arithmetic on curves of genus* 1*. III. The Tate-Šafarevič and Selmer groups"*, Proc. London Math. Soc. (3) **13** (1963), 768. MR **29**:1213

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997. MR **99e**:11068

[CM] J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28. MR 1 758 797

[CS02] B. Conrad and W. A. Stein, *Component Groups of Purely Toric Quotients*, to appear in Math Research Letters (2002).

[Del01] C. Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* $\mathbf{Q}$, Experiment. Math. **10** (2001), no. 2, 191–196.

[DI95] F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem, Providence, RI, 1995, pp. 39–133. MR **97g**:11044

[Edi91] B. Edixhoven, *On the Manin constants of modular elliptic curves*, Arithmetic algebraic geometry (Texel, 1989), Birkhäuser Boston, Boston, MA, 1991, pp. 25–39. MR **92a**:11066

[Eme01] M. Emerton, *Optimal quotients of modular Jacobians.* Preprint.

[FpS+01] E. V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll, and J. L. Wetherell, *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. Comp. **70** (2001), no. 236, 1675–1697. MR 1 836 926

[Fon75] J-M. Fontaine, *Groupes finis commutatifs sur les vecteurs de Witt*, C. R. Acad. Sci. Paris Sér. A-B **280** (1975), Ai, A1423–A1425. MR **51**:10353

[Gro94] B. H. Gross, *L-functions at the central critical point*, Motives (Seattle, WA, 1991), Amer. Math. Soc., Providence, RI, 1994, pp. 527–535. MR **95a**:11060

[Gro68] A. Grothendieck, *Le groupe de Brauer. III. Exemples et compléments*, Dix Exposés sur la Cohomologie des Schémas, North-Holland, Amsterdam, 1968, pp. 88–188. MR **39**:5586c

[Gro72] A. Grothendieck, *Modèles de Néron et monodromie* in *Groupes de monodromie en géométrie algébrique. I*, Springer-Verlag, Berlin, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Vol. 288. MR **50**:7134

[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR **87j**:11057

[Kat81] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502. MR **82d**:14025

[KL89] V. A. Kolyvagin and D. Y. 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. MR **91c**:11032

[KL92] V. A. Kolyvagin and D. Y. Logachev, *Finiteness of* Ш *over totally real fields*, Math. USSR Izvestiya **39** (1992), no. 1, 829–853. MR **93d**:11063

[KS00] D. R. Kohel and W. A. Stein, *Component Groups of Quotients of $J_0(N)$*, Proceedings of the 4th International Symposium (ANTS-IV), Leiden, Netherlands, July 2–7, 2000 (Berlin), Springer, 2000. MR 1 850 621

[Lan91] S. Lang, *Number theory. III*, Springer-Verlag, Berlin, 1991, Diophantine geometry. MR **93a**:11048

[LO85] H. W. Lenstra, Jr. and F. Oort, *Abelian varieties having purely additive reduction*, J. Pure Appl. Algebra **36** (1985), no. 3, 281–298. MR **86e**:14020

[Maz72] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266. MR **56**:3020

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978). MR **80c**:14015

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR **80h**:14022

[MT74] B. Mazur and J. Tate, *Points of order* 13 *on elliptic curves*, Invent. Math. **22** (1973/74), 41–49. MR **50**:327

[Mil86] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

[Ogg73] A. P. Ogg, *Rational points on certain elliptic modular curves*, Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, R.I., 1973, pp. 221–231. MR **49**:2743

[PS99] B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. MR **2000m**:11048

[Shi73] G. Shimura, *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan **25** (1973), no. 3, 523–544. MR **47**:6709

[Shi94] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1. MR **95e**11048

[Ste82] G. Stevens, *Arithmetic on modular curves*, Birkhäuser Boston Inc., Boston, Mass., 1982. MR **87b**:11050

[Ste00] W. A. Stein, *Explicit approaches to modular abelian varieties*, Ph.D. thesis, University of California, Berkeley (2000).

[Ste02a] W. A. Stein, *An introduction to computing modular forms using modular symbols*, to appear in an MSRI Proceedings (2002).

[Ste03] W. A. Stein, *Shafarevich-Tate groups of nonsquare order*, Submitted (2003).

[Stu87] J. Sturm, *On the congruence of modular forms*, Number theory (New York, 1984–1985), Springer, Berlin, 1987, pp. 275–280. MR **88h**:11031

[Tat63] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295. MR **31**:168

[Tat66] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1966 (reprinted in 1995), pp. Exp. No. 306, 415–440. MR 1 610 977

Department of Mathematics, U niversity of Texas, Austin, Texas 78712
E-mail address: agashe@math.utexas.edu

Department of Mathematics, Harvard University, Cambridge, Massachussetts 02138
E-mail address: was@math.harvard.edu