Visibility of the Shafarevich-Tate Group at Higher Level

Dimitar P. Jetchev William A. Stein

Abstract. We study visibility of Shafarevich-Tate groups of modular abelian varieties in Jacobians of modular curves of higher level. We prove a theorem about the existence of visible elements at a specific higher level under hypotheses that can be verified explicitely. We also provide a table of examples of visible subgroups at higher level and state conjectures inspired by our data.

1 Introduction

1.1 Motivation

Mazur suggested that the Shafarevich-Tate group $\text{Ш}(K, E)$ of an abelian variety A over a number field K could be studied via a collection of finite subgroups (the *visible subgroups*) corresponding to different embeddings of the variety into larger abelian varieties C over K (see [Maz99] and [CM00]). The advantage of this approach is that the isomorphism classes of principal homogeneous spaces, for which one has *à priori* little geometric information, can be given a much more explicit description as K-rational points on the quotient abelian variety C/A (the reason why they are called *visible elements*).

Agashe, Cremona, Klenke and the second author built upon the ideas of Mazur and developed a systematic theory of visibility of Shafarevich-Tate groups of abelian varieties over number fields (see [Aga99b, AS02, AS05, CM00, Kle01, Ste00]). More precisely, Agashe and Stein provided sufficient conditions for the existence of visible sugroups of certain order in the Shafarevich-Tate group and applied their general theory to the case of newform subvarieties $A_{f/\mathbb{Q}}$ of the Jacobian $J_0(N)_{/\mathbb{Q}}$ of the modular curve $X_0(N)_{/\mathbb{Q}}$ (here, f is a newform of level N and weight 2 which is an eigenform for the Hecke operators acting on the space $S_2(\Gamma_0(N))$ of cuspforms of level N and weight 2). Unfortunately, there is no guarantee that a non-trivial element of $\text{Ш}(\mathbb{Q}, A_f)$ is visible for the embedding $A_f \hookrightarrow J_0(N)$.

In this paper we consider the case of modular abelian varieties over $\mathbb{Q}$ and make use of the algebraic and arithmetic properties of the corresponding newforms to provide sufficient conditions for the existence of visible elements of $Ш(\mathbb{Q}, A_f)$ in modular Jacobians of level a multiple of the base level N. More precisely, we consider morphism of the form $A_f \hookrightarrow J_0(N) \xrightarrow{\phi} J_0(MN)$, where ϕ is a suitable linear combination of degeneracy maps which makes the kernel of the composition morphism almost trivial (i.e., trivial away from the 2-part). For specific examples, the sufficient conditions can be verified explicitely. We also provide a table of examples where certain elements of $Ш(\mathbb{Q}, A_f)$ which are invisible in $J_0(N)$ become visible at a suitably chosen higher level. At the end, we state some general conjectures inspired by our results.

1.2 Organization of the paper

Section 2 discusses the basic definitions and notation for modular abelian varieties, modular forms, Hecke algebras, the Shimura construction and modular degrees. Section 3 is a brief introduction to visibility theory for Shafarevich-Tate groups. In Section 4 we state and prove an equivariant version of a theorem of Agashe-Stein (see [AS05, Thm 3.1]) which guarantees existence of visible elements. The theorem is more general because it makes use of the action of the Hecke algebra on the modular Jacobian.

In Section 5 we introduce the notion of *strong visibility* which is relevant for visualizing cohomology classes in Jacobians of modular curves whose level is a multiple of the level of the original abelian variety. Theorem 5.1.3 guarantees existence of strongly visible elements of the Shafarevich-Tate group under some hypotheses on the component groups, a congruence condition between modular forms, and irreducibility of the Galois representation. In Section 5.4 we prove a variant of the same theorem (Theorem 5.4.2) with more stringent hypotheses that are easier to verify in specific cases.

Section 6 discusses in detail two computational examples for which strongly visible elements of certain order exist which provides evidence for the Birch and Swinnerton-Dyer conjecture. We state a general conjecture (Conjecture 7.1.1) in Section 7 according to which every element of the Shafarevich-Tate group of a modular abelian variety becomes visible at higher level. We provide evidence for the the conjecture in Section 7.2 and tables of computational data in Section 7.4.

ACKNOWLEDGEMENT: The authors would like to thank David Helm, Ben Howard, Barry Mazur, Bjorn Poonen and Ken Ribet for discussions and comments on the paper.

2 Notation

1. Abelian varieties. For a number field K, $A_{/K}$ denotes an abelian variety over K. We denote the dual of A by $A^\vee_{/K}$. If $\varphi : A \to B$ is an isogeny of degree n, we denote the *complementary isogeny* by φ'; this is the isogeny $\phi' : B \to A$, such that $\varphi \circ \varphi' = \varphi' \circ \varphi = [n]$, the multiplication-by-$n$ map on A. Unless otherwise specified, Néron models of abelian varieties will be denoted by the corresponding caligraphic letters, e.g., $\mathcal{A}$ denotes the Néron model of A.

2. Galois cohomology. For a fixed algebraic closure $\overline{K}$ of K, G_K will be the Galois group $\mathrm{Gal}(\overline{K}/K)$. If v is any non-archimedean place of K, K_v and k_v will always mean the completion and the residue field of K at v, respectively. By K_v^{ur} we always mean the maximal unramified extension of the completion K_v. Given a G_K-module M, we let $\mathrm{H}^1(K, M)$ denote the Galois cohomology group $\mathrm{H}^1(G_K, M)$.

3. Component groups. The *component group* of A at v is the finite group $\Phi_{A,v} = \mathcal{A}_{k_v}/\mathcal{A}^0_{k_v}$ which also has a structure of a finite group scheme over k_v. The *Tamagawa number* of A at v is $c_{A,v} = \#\Phi_{A,v}(k_v)$, and the *component group order* of A at v is $\overline{c}_{A,v} = \#\Phi_{A,v}(\overline{k}_v)$.

4. Modular abelian varieties. Let $h = 0$ or 1. A *J_h-modular abelian variety* is an abelian variety $A_{/K}$ which is a quotient of $J_h(N)$ for some N, i.e., there exists a surjective morphism $J_h(N) \twoheadrightarrow A$ defined over K. We define the *level* of a modular abelian variety A to be the minimal N, such that A is a quotient of $J_h(N)$. The modularity theorem of Wiles et al. (see [BCDT01]) implies that all elliptic curves over $\mathbb{Q}$ are modular. Serre's modularity conjecture implies that the modular abelian varieties over $\mathbb{Q}$ are precisely the abelian varieties over $\mathbb{Q}$ of GL_2-type (see [Rib92, §4]).

5. Shimura construction. Let $f = \displaystyle\sum_{n=1}^{\infty} a_n q^n \in S_2(\Gamma_0(N))$ be a newform of level N and weight 2 for $\Gamma_0(N)$ which is an eigenform for all Hecke operators in the Hecke algebra $\mathbb{T}(N)$. Shimura (see [Shi94, Thm. 7.14]) associated to f an abelian subvariety $A_{f/\mathbb{Q}}$ of $J_0(N)$, simple over $\mathbb{Q}$, of dimension $d = [K : \mathbb{Q}]$, where $K = \mathbb{Q}(\dots, a_n, \dots)$ is the Hecke eigenvalue field. More precisely, if $I_f = \mathrm{Ann}_{\mathbb{T}(N)}(f)$ then A_f is the connected component containing the identity of the I_f-torsion subgroup of $J_0(N)$, i.e., $A_f = J_0(N)[I_f]^0 \subset J_0(N)$. The quotient $\mathbb{T}(N)/I_f$ of the Hecke algebra $\mathbb{T}(N)$ is a subalgebra of the endomorphism ring $\mathrm{End}_{\mathbb{Q}}(A_{/\mathbb{Q}})$. Also $L(A_f, s) = \displaystyle\prod_{i=1}^{d} L(f_i, s)$, where the f_i are the $G_{\mathbb{Q}}$-conjugates of f. We also consider the dual abelian variety $A_f^{\vee}$ which is a quotient variety of $J_0(N)$.

6. I-torsion submodules. If M is a module over a commutative ring R and I is an ideal of R, let

$$M[I] = \{x \in M : mx = 0 \text{ all } m \in I\}$$

be the *I-torsion submodule* of M.

7. Hecke algebras. Let $S_2(\Gamma)$ denote the space of cusp forms of weight 2 for any congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$. Let

$$\mathbb{T}(N) = \mathbb{Z}[\ldots, T_n, \ldots] \subseteq \mathrm{End}_{\mathbb{Q}}(J_0(N))$$

be the Hecke algebra, where T_n is the nth Hecke operator. $\mathbb{T}(N)$ also acts on $S_2(\Gamma_0(N))$ and the integral homology $H_1(X_0(N), \mathbb{Z})$.

8. Modular degree. If A is an abelian subvariety of $J_0(N)$, let

$$\theta : A \to J_0(N) \cong J_0(N)^\vee \to A^\vee$$

be the induced polarization. The *modular degree* of A is

$$m_A = \sqrt{\#\,\mathrm{Ker}(A \xrightarrow{\theta} A^\vee)}.$$

See [AS02] for why m_A is an integer and for an algorithm to compute it.

3 Visible Subgroups of Shafarevich-Tate Groups

Let K be a number field and $\iota : A_{/K} \hookrightarrow C_{/K}$ be an embedding of an abelian variety into another abelian variety over K.

DEFINITION 3.0.1. The *visible subgroup* of $\mathrm{H}^1(K, A)$ relative to ι is

$$\mathrm{Vis}_C\, \mathrm{H}^1(K, A) = \mathrm{Ker}\left(\iota_* : \mathrm{H}^1(K, A) \to \mathrm{H}^1(K, C)\right).$$

The visible subgroup of $Ш(K, A)$ relative to the embedding ι is

$$\begin{aligned} \mathrm{Vis}_C\, Ш(K, A) &= Ш(K, A) \cap \mathrm{Vis}_C\, \mathrm{H}^1(K, A) \\ &= \mathrm{Ker}\left(Ш(K, A) \to Ш(K, C)\right) \end{aligned}$$

Let Q be the abelian variety $C/\iota(A)$, which is defined over K. The long exact sequence of Galois cohomology corresponding to the short exact sequence $0 \to A \to C \to Q \to 0$ gives rise to the following exact sequence

$$0 \to A(K) \to C(K) \to Q(K) \to \mathrm{Vis}_C\, \mathrm{H}^1(K, A) \to 0.$$

The last map being surjective means that the cohomology classes of $\mathrm{Vis}_C\, \mathrm{H}^1(K, A)$ are images of K-rational points on Q, which explains the meaning of the word *visible* in the definition. The group $\mathrm{Vis}_C\, \mathrm{H}^1(K, A)$ is finite since it is torsion and since the Mordell-Weil group $Q(K)$ is finitely generated.

Remark 3.0.2. If $A_{/K}$ is an abelian variety and $c \in \mathrm{H}^1(K, A)$ is any cohomology class, there exists an abelian variety $C_{/K}$ and an embedding $\iota : A \hookrightarrow C$ defined over K, such that $c \in \mathrm{Vis}_C\, \mathrm{H}^1(K, A)$, i.e., c is visible in C (see [AS02, Prop. 1.3]). The C of [AS02, Prop. 1.3] is the restriction of scalars of $A_L = A \times_K L$ down to K, where L is any finite extension of K such that c has trivial image in $\mathrm{H}^1(L, A)$.

4 Equivariant Visibility

Let K be a number field, let $A_{/K}$ and $B_{/K}$ be abelian subvarieties of an abelian variety $C_{/K}$, such that $C = A + B$ and $A \cap B$ is finite. Let $Q_{/K}$ denotes the quotient C/B. Let N be a positive integer divisible by all primes of bad reduction for C.

Let ℓ be a prime such that $B[\ell] \subset A$ and $e < \ell - 1$, where e is the largest ramification index of any prime of K lying over ℓ. Suppose that

$$\ell \nmid N \cdot \#B(K)_{\mathrm{tor}} \cdot \#Q(K)_{\mathrm{tor}} \cdot \prod_{v \mid N} c_{A,v} c_{B,v}.$$

Under those conditions, Agashe and Stein (see [AS02, Thm. 3.1]) construct a homomorphism $B(K)/\ell B(K) \to Ш(K, A)[\ell]$ whose kernel has $\mathbb{F}_\ell$-dimension bounded by the Mordell-Weil rank of $A(K)$.

In this paper, we refine [AS02, Prop. 1.3] by taking into account the algebraic structure coming from the endomorphism ring $\mathrm{End}_K(C)$. In particular, when we apply the theory to modular abelian varieties, we would like to use the additional structure coming from the Hecke algebra. There are numerous example (see [AS05]) where [AS02, Prop. 1.3] does not apply, but nevertheless, we can use our refinement to prove existence of visible elements of $Ш(\mathbb{Q}, A_f)$ at higher level (e.g., see Propositions 6.1.3 and 6.2.1 below).

4.1 The main theorem

Let $A_{/K}$, $B_{/K}$, $C_{/K}$, $Q_{/K}$, N and ℓ be as above. Let R be a commutative subring of $\mathrm{End}_K(C)$ that leaves A and B stable and let $\mathfrak{m}$ be a maximal ideal of R of residue characteristic ℓ. By the Néron mapping property, the subgroups $\Phi_{A,v}(k_v)$ and $\Phi_{B,v}(k_v)$ of k_v-points of the corresponding component groups can be viewed as R-modules.

Theorem 4.1.1 (Equivariant Visibility Theorem). *Suppose that $A(K)$ has rank zero and that the groups $Q(K)[\mathfrak{m}]$, $B(K)[\mathfrak{m}]$, $\Phi_{A,v}(k_v)[\mathfrak{m}]$ and $\Phi_{B,v}(k_v)[\ell]$ are all trivial for all nonarchimedean places v of K. Then there is an injective homomorphism of $R/\mathfrak{m}$-vector spaces*

$$(B(K)/\ell B(K))[\mathfrak{m}] \hookrightarrow \mathrm{Vis}_C(Ш(K, A))[\mathfrak{m}]. \tag{1}$$

Remark 4.1.2. Applying the above result for $R = \mathbb{Z}$, we recover the result of Agashe and Stein in the case when $A(K)$ has Mordell-Weil rank zero. We could relax the hypothesis that $A(K)$ is finite and instead give a bound on the dimension of the kernel of (1) in terms of the rank of $A(K)$ similar to the bound in [AS02, Thm. 3.1]. We will not need this stronger result in our paper.

4.2 Some commutative algebra

Before proving Theorem 4.1.1 we recall some well-known lemmas from commutative algebra. Let M be a module over a commutative ring R and let $\mathfrak{m}$ be a finitely generated prime ideal of R.

LEMMA 4.2.1. *If $M_{\mathfrak{m}}$ is Artinian, then $M_{\mathfrak{m}} \neq 0 \iff M[\mathfrak{m}] \neq 0$.*

Proof. ($\Longleftarrow$) We first prove that $M_{\mathfrak{m}} = 0$ implies $M[\mathfrak{m}] = 0$ by a slight modification of the proof of [AM69, Prop. I.3.8]. Suppose $M_{\mathfrak{m}} = 0$, yet there is a nonzero $x \in M[\mathfrak{m}]$. Let $I = \mathrm{Ann}_R(x)$. Then $I \neq (1)$ is an ideal that contains $\mathfrak{m}$, so $I = \mathfrak{m}$. Consider $\frac{x}{1} \in M_{\mathfrak{m}}$. Since $M_{\mathfrak{m}} = 0$, we have $x/1 = 0$, hence by definition of localization, x is killed by some element of $R - \mathfrak{m}$ (set-theoretic difference). But this is impossible since $\mathrm{Ann}_R(x) = \mathfrak{m}$.

($\Longrightarrow$) Next we prove that $M_{\mathfrak{m}} \neq 0$ implies $M[\mathfrak{m}] \neq 0$. Since $M_{\mathfrak{m}}$ is an Artinian module over the (local) ring $R_{\mathfrak{m}}$, by [AM69, Prop. 6.8], $M_{\mathfrak{m}}$ has a composition series:

$$M_{\mathfrak{m}} = M_0 \supset M_1 \supset \cdots \supset M_{n-1} \supset M_n = 0,$$

where by definition each quotient M_i/M_{i+1} is a simple $R_{\mathfrak{m}}$-module. In particular, M_{n-1} is a simple $R_{\mathfrak{m}}$-module. Suppose $x \in M_{n-1}$ is nonzero, and let $I = \mathrm{Ann}_{R_{\mathfrak{m}}}(x)$. Then

$$R_{\mathfrak{m}}/I \cong R_{\mathfrak{m}} \cdot x \subset M_{n-1},$$

so by simplicity $R_{\mathfrak{m}}/I \cong M_{n-1}$ is simple. Thus $I = \mathfrak{m}$, otherwise $R_{\mathfrak{m}}/I$ would have $\mathfrak{m}/I$ as a proper submodule. Thus $x \in M_{n-1}[\mathfrak{m}]$ is nonzero.

Write $x = [y, a]$ with $y \in M$ and $a \in R - \mathfrak{m}$, where $[y/a]$ means the class of y/a in the localization (same as (y, a) on page 36 of [AM69]). Since $a \in R - \mathfrak{m}$, the element a acts as a unit on $M_{\mathfrak{m}}$, hence $ax = [y/1] \in M_{n-1}$ is nonzero and also still annihilated by $\mathfrak{m}$ (by commutativity).

To say that $[y/1]$ is annihilated by $\mathfrak{m}$ means that for all $\alpha \in \mathfrak{m}$ there exists $t \in R - \mathfrak{m}$ such that $t\alpha y = 0$ in M. Since $\mathfrak{m}$ is finitely generated, we can write $\mathfrak{m} = (\alpha_1, \ldots, \alpha_n)$ and for each α_i we get corresponding elements $t_1, \ldots, t_n$ and a product $t = t_1 \cdots t_n$. Also $t \notin \mathfrak{m}$ since $\mathfrak{m}$ is a prime ideal and each $t_i \notin \mathfrak{m}$. Let $z = ty$. Then for all $\alpha \in \mathfrak{m}$ we have $\alpha z = t\alpha y = 0$. Also $z \neq 0$ since t acts as a unit on M_{n-1}. Thus $z \in M[\mathfrak{m}]$, and is nonzero, which completes the proof of the lemma. □

LEMMA 4.2.2. *Suppose $0 \to M_1 \to N \to M_2 \to 0$ is an exact sequence of R-modules each of whose localization at $\mathfrak{m}$ is Artinian. Then $N[\mathfrak{m}] \neq 0 \iff (M_1 \oplus M_2)[\mathfrak{m}] \neq 0$.*

Proof. By Lemma 4.2.1 we have $N[\mathfrak{m}] \neq 0$ if and only if $N_{\mathfrak{m}} \neq 0$. By Proposition 3.3 on page 39 of [AM69], the localized sequence

$$0 \to (M_1)_{\mathfrak{m}} \to N_{\mathfrak{m}} \to (M_2)_{\mathfrak{m}} \to 0$$

is exact. Thus $N_{\mathfrak{m}} \neq 0$ if and only if at least one of $(M_1)_{\mathfrak{m}}$ or $(M_2)_{\mathfrak{m}}$ is nonzero. Again by Lemma 4.2.1, at least one of $(M_1)_{\mathfrak{m}}$ or $(M_2)_{\mathfrak{m}}$ is nonzero if and only if at least one of $M_1[\mathfrak{m}]$ or $M_2[\mathfrak{m}]$ is nonzero. The latter is the case if and only if $(M_1 \oplus M_2)[\mathfrak{m}] \neq 0$. □

Remark 4.2.3. One could also prove the lemmas using the isomorphism $M[\mathfrak{m}] \cong \mathrm{Hom}_R(R/\mathfrak{m}, M)$ and exactness properties of Hom, but even with this approach many of the details in Lemma 4.2.1 still have to be checked.

Remark 4.2.4. In Theorem 4.1.1, we have $R \subset \mathrm{End}(C)$, hence R is finitely generated as a $\mathbb{Z}$-module, so R is noetherian.

LEMMA 4.2.5. *Let G be a finite cyclic group, M be a finite G-module that is also a module over a commutative ring R such that the action of G and R commute (i.e., M is an $R[G]$-module). Suppose $\mathfrak{p}$ is a finitely-generated prime ideal of R, and $H^0(G,M)[\mathfrak{p}] = 0$. Then $H^1(G,M)[\mathfrak{p}] = 0$.*

Proof. Argue as in [Se79, Prop. VIII.4.8], but noting that all modules are modules over R and maps are morphisms of R-modules. $\square$

4.3 PROOF OF THEOREM 4.1.1

Proof of Theorem 4.1.1. We argue as in the proof of [AS02, Thm. 3.1]. The construction of the map (1) is similar to the one in the proof of [AS02, Lem. 3.6]. We have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & B[\ell] \arrow[r] \arrow[d] & B \arrow[r, "\ell"] \arrow[d] \arrow[dr, "\psi"] & B \arrow[r] \arrow[d, "\pi"] & 0 \\
0 \arrow[r] & A \arrow[r] & C \arrow[r] & Q \arrow[r] & 0,
\end{tikzcd}$$

where $\psi : B \to Q$ is the composition of the inclusion $B \hookrightarrow C$ with the quotient map $C \to Q$, and the existence of the morphism $\pi : B \to Q$ follows from the inclusion $B[\ell] \subset \mathrm{Ker}(\psi) = A \cap B$. By naturality for the long exact sequence of Galois cohomology we obtain the following commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & M_0 \arrow[d] & M_1 \arrow[d] & M_2 \arrow[d] & \\
0 \arrow[r] & B(K)/(B(K)[\ell]) \arrow[r, "\ell"] \arrow[d] & B(K) \arrow[r] \arrow[d] \arrow[dr, "\pi"] & B(K)/\ell B(K) \arrow[r] \arrow[d, "\varphi"] & 0 \\
0 \arrow[r] & C(K)/A(K) \arrow[r] \arrow[d] & Q(K) \arrow[r] & \mathrm{Vis}_C(\mathrm{H}^1(K,A)) \arrow[r] & 0 \\
 & M_3. & & &
\end{tikzcd}$$

Here, M_0, M_1 and M_2 denote the kernels of the corresponding vertical maps and M_3 denotes the cokernel of the first map. Since R preserves A, B, and

$B[\ell]$, all objects in the diagram are R-module and the morphisms of abelian varieties are also R-module homomorphisms.

The snake lemma yields an exact sequence

$$0 \to M_0 \to M_1 \to M_2 \to M_3.$$

By hypothesis, $B(K)[\mathfrak{m}] = 0$, so $N_0 = \mathrm{Ker}(B(K) \to C(K)/A(K))$ has no $\mathfrak{m}$ torsion. Noting that $B(K)[\ell] \subset N_0$, it follows that $M_0 = N_0/(B(K)[\ell])$ has no $\mathfrak{m}$ torsion either, by Lemma 4.2.2. Also, $M_1[\mathfrak{m}] = 0$ again since $B(K)[\mathfrak{m}] = 0$.

By the long exact sequence on Galois cohomology, the quotient $C(K)/B(K)$ is isomorphic to a subgroup of $Q(K)$ and by hypothesis $Q(K)[\mathfrak{m}] = 0$, so $(C(K)/B(K))[\mathfrak{m}] = 0$. Since Q is isogenous to A and $A(K)$ is finite and $C(K)/B(K) \hookrightarrow Q(K)$, we see that $C(K)/B(K)$ is finite. Thus M_3 is a quotient of the finite R-module $C(K)/B(K)$, which has no $\mathfrak{m}$-torsion, so Lemma 4.2.2 implies that $M_3[\mathfrak{m}] = 0$. The same lemma implies that M_1/M_0 has no $\mathfrak{m}$-torsion, since it is a quotient of the finite module M_1, which has no $\mathfrak{m}$-torsion. Thus, we have an exact sequence

$$0 \to M_1/M_0 \to M_2 \to M_3 \to 0,$$

and both of M_1/M_0 and M_3 have trivial $\mathfrak{m}$-torsion. It follows by Lemma 4.2.2, that $M_2[\mathfrak{m}] = 0$. Therefore, we have an injective morphism of $R/\mathfrak{m}$-vector spaces

$$\varphi : (B(K)/\ell B(K))[\mathfrak{m}] \hookrightarrow \mathrm{Vis}_C(H^1(K, A))[\mathfrak{m}].$$

It remains to show that for any $x \in B(K)$, we have $\varphi(x) \in \mathrm{Vis}_C(\text{Ш}(K, A))$, i.e., that $\varphi(x)$ is locally trivial.

We proceed exactly as in Section 3.5 of [AS05]. In both cases $\mathrm{char}(v) \neq \ell$ and $\mathrm{char}(v) = \ell$ we arrive at the conclusion that the restriction of $\varphi(x)$ to $\mathrm{H}^1(K_v, A)$ is an element $c \in \mathrm{H}^1(K_v^{\mathrm{ur}}/K_v, A(K_v^{\mathrm{ur}}))$. (Note that in the case $\mathrm{char}(v) \neq \ell$ the proof uses our hypothesis that $\ell \nmid \#\Phi_{B,v}(k_v)$.) By [Mil86, Prop I.3.8], there is an isomorphism

$$\mathrm{H}^1(K_v^{\mathrm{ur}}/K_v, A(K_v^{\mathrm{ur}})) \cong \mathrm{H}^1(\overline{k}_v/k_v, \Phi_{A,v}(\overline{k}_v)). \tag{2}$$

We will use our hypothesis that

$$\Phi_{A,v}(k_v)[\mathfrak{m}] = \Phi_{B,v}(k_v)[\ell] = 0$$

for all v of bad reduction to deduce that the image of φ lies in $\mathrm{Vis}_C(\text{Ш}(K, A))[\mathfrak{m}]$. Let d denote the image of c in $\mathrm{H}^1(\overline{k}_v/k_v, \Phi_{A,v}(\overline{k}_v))$. The construction of d is compatible with the action of R on Galois cohomology, since (as is explained in the proof of [Mil86, Prop. I.3.8]) the isomorphism (2) is induced from the exact sequence of $\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v)$-modules

$$0 \to \mathcal{A}^0(K_v^{\mathrm{ur}}) \to \mathcal{A}(K_v^{\mathrm{ur}}) \to \Phi_{A,v}(\overline{k}_v) \to 0,$$

where $\mathcal{A}$ is the Néron model of A and $\mathcal{A}^0$ is the subgroup scheme whose generic fiber is A and whose closed fiber is the identity component of $\mathcal{A}_{k_v}$. Since $\varphi(x) \in \mathrm{H}^1(K, A)[\mathfrak{m}]$, it follows that

$$d \in \mathrm{H}^1(\overline{k}_v/k_v, \Phi_{A,v}(\overline{k}_v))[\mathfrak{m}].$$

Lemma 4.2.5, our hypothesis that $\Phi_{A,v}(k_v)[\mathfrak{m}] = 0$, and that

$$\mathrm{H}^1(\overline{k}_v/k_v, \Phi_{A,v}(\overline{k}_v)) = \varinjlim \mathrm{H}^1(\mathrm{Gal}(k_v'/k_v), \Phi_{A,v}(k_v'))),$$

together imply that $\mathrm{H}^1(\overline{k}_v/k_v, \Phi_{A,v}(\overline{k}_v))[\mathfrak{m}] = 0$, hence $d = 0$. Thus $c = 0$, so $\varphi(x)$ is locally trivial, which completes the proof. □

5 Strong Visibility at Higher Level

5.1 Strongly visible subgroups

Let $A_{/\mathbb{Q}}$ be an abelian subvariety of $J_0(N)_{/\mathbb{Q}}$ and let $p \nmid N$ be a prime. Let

$$\varphi = \delta_1^* + \delta_p^* : J_0(N) \to J_0(pN), \tag{3}$$

where δ_1^* and δ_p^* are the pullback maps on equivalence classes of degree-zero divisors of the degeneracy maps $\delta_1, \delta_p : X_0(pN) \to X_0(N)$. Let $\mathrm{H}^1(\mathbb{Q}, A)^{\mathrm{odd}}$ be the prime-to-2-part of the group $\mathrm{H}^1(\mathbb{Q}, A)$.

Definition 5.1.1 (Strongly Visibility). The *strongly visible* subgroup of $\mathrm{H}^1(\mathbb{Q}, A)$ for $J_0(pN)$ is

$$\mathrm{Vis}_{pN}\,\mathrm{H}^1(\mathbb{Q}, A) = \mathrm{Ker}\left(\mathrm{H}^1(\mathbb{Q}, A)^{\mathrm{odd}} \xrightarrow{\varphi_*} \mathrm{H}^1(\mathbb{Q}, J_0(pN))\right) \subset \mathrm{H}^1(\mathbb{Q}, A).$$

Also,

$$\mathrm{Vis}_{pN}\,\text{Ш}(\mathbb{Q}, A) = \text{Ш}(\mathbb{Q}, A) \cap \mathrm{Vis}_{pN}\,\mathrm{H}^1(\mathbb{Q}, A).$$

The reason we replace $\mathrm{H}^1(\mathbb{Q}, A)$ by $\mathrm{H}^1(\mathbb{Q}, A)^{\mathrm{odd}}$ is that the kernel of φ is a 2-group (see [Rib90b]).

Remark 5.1.2. We could obtain more visible subgroups by considering the map $\delta_1^* - \delta_p^*$ in Definition 5.1.1. However, the methods of this paper do not apply to this map.

For a positive integer N, let

$$\nu(N) = \frac{1}{6} \cdot \prod_{q^r \| N} (q^r + q^{r-1}) = \frac{1}{6} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)].$$

We call the number $\nu(N)$ the *Sturm bound* (see [Stu87]).

Theorem 5.1.3. *Let $A_{/\mathbb{Q}} = A_f$ be a newform abelian subvariety of $J_0(N)$ for which $L(A_{/\mathbb{Q}}, 1) \neq 0$ and let $p \nmid N$ be a prime. Suppose that there is a maximal ideal $\lambda \subset \mathbb{T}(N)$ and an elliptic curve $E_{/\mathbb{Q}}$ of conductor pN such that:*

1. *[Nondivisibility] The residue characteristic ℓ of λ satisfies*

$$\ell \nmid 2 \cdot N \cdot p \cdot \prod_{q \mid N} c_{E,q}.$$

2. *[Component Groups] For each prime $q \mid N$,*

$$\Phi_{A,q}(\mathbb{F}_q)[\lambda] = 0.$$

3. *[Fourier Coefficients] Let $a_n(E)$ be the n-th Fourier coefficient of the modular form attached to E, and $a_n(f)$ the n-th Fourier coefficient of f. Assume that $a_p(E) = -1$,*

$$a_p(f) \equiv -(p+1) \pmod{\lambda} \quad \textit{and} \quad a_q(f) \equiv a_q(E) \pmod{\lambda},$$

for all primes $q \neq p$ with $q \leq \nu(pN)$.

4. *[Irreducibility] The mod ℓ representation $\overline{\rho}_{E,\ell}$ is irreducible.*

Then there is an injective homomorphism

$$E(\mathbb{Q})/\ell E(\mathbb{Q}) \hookrightarrow \mathrm{Vis}_{pN}(\text{Ш}(\mathbb{Q}, A_f))[\lambda].$$

Remark 5.1.4. In fact, we have

$$E(\mathbb{Q})/\ell E(\mathbb{Q}) \hookrightarrow \mathrm{Ker}(\text{Ш}(\mathbb{Q}, A_f) \to \text{Ш}(\mathbb{Q}, C))[\lambda] \subset \mathrm{Vis}_{pN}(\text{Ш}(\mathbb{Q}, A_f))[\lambda],$$

where $C \subset J_0(pN)$ is isogenous to $A_f \times E$.

5.2 Some auxiliary lemmas

We will use the following lemmas in the proof of Theorem 5.1.3. The notation is as in the previous section. In addition, if $f \in S_2(\Gamma_0(N))$, we denote by $a_n(f)$ the n-th Fourier coefficient of f and by K_f and $\mathcal{O}_f$ the Hecke eigenvalue field and its ring of integers, respectively.

LEMMA 5.2.1. *Suppose $A_f \subset J_0(N)$ and $A_g \subset J_0(pN)$ are attached to newforms f and g of level N and pN, respectively, with $p \nmid N$. Suppose that there is a prime ideal λ of residue characteristic $\ell \nmid 2pN$ in an integrally closed subring $\mathcal{O}$ of $\overline{\mathbb{Q}}$ that contains the ring of integers of the composite field $K = K_f K_g$ such that for $q \leq \nu(pN)$,*

$$a_q(f) \equiv \begin{cases} a_q(g) \pmod{\lambda} & \textit{if } q \neq p, \\ (p+1)a_p(g) \pmod{\lambda} & \textit{if } q = p. \end{cases}$$

Assume that $a_p(g) = -1$. Let $\lambda_f = \mathcal{O}_f \cap \lambda$ and $\lambda_g = \mathcal{O}_g \cap \lambda$ and assume that $A_f[\lambda_f]$ is an irreducible $G_{\mathbb{Q}}$-module. Then we have an equality

$$\varphi(A_f[\lambda_f]) = A_g[\lambda_g]$$

of subgroups of $J_0(pN)$, where φ is as in (3).

Proof. Our hypothesis that $a_p(f) \equiv -(p+1) \pmod{\lambda_f}$ implies, by the proofs in [Rib90b], that

$$\varphi(A_f[\lambda_f]) \subset \varphi(A_f) \cap J_0(pN)_{p\text{-new}},$$

where $J_0(pN)_{p\text{-new}}$ is the p-new abelian subvariety of $J_0(N)$.

By [Rib90b, Lem. 1], the operator $U_p = T_p$ on $J_0(pN)$ acts as -1 on $\varphi(A_f[\lambda_f])$. Consider the action of U_p on the 2-dimensional vector space spanned by $\{f(q), f(q^p)\}$. The matrix of U_p with respect to this basis is

$$U_p = \begin{pmatrix} a_p(f) & p \\ -1 & 0 \end{pmatrix}.$$

In particular, neither of $f(q)$ and $f(q^p)$ is an eigenvector for U_p. The characteristic polynomial of U_p acting on the span of $f(q)$ and $f(q^p)$ is $x^2 - a_p(f)x + p$. Using our hypothesis on $a_p(f)$ again, we have

$$x^2 - a_p(f)x + p \equiv x^2 + (p+1)x + p \equiv (x+1)(x+p) \pmod{\lambda}.$$

Thus we can choose an algebraic integer α such that

$$f_1(q) = f(q) + \alpha f(q^p)$$

is an eigenvector of U_p with eigenvalue congruent to -1 modulo λ. (It does not matter for our purposes whether $x^2+a_p(f)x+p$ has distinct roots; nonetheless, since $p \nmid N$, [CV92, Thm. 2.1] implies that it does have distinct roots.) The cusp form f_1 has the same prime-indexed Fourier coefficients as f at primes other than p. Enlarge $\mathcal{O}$ if necessary so that $\alpha \in \mathcal{O}$. The p-th coefficient of f_1 is congruent modulo λ to -1 and f_1 is an eigenvector for the full Hecke algebra. It follows from the recurrence relation for coefficients of the eigenforms that

$$a_n(g) \equiv a_n(f_1) \pmod{\lambda}$$

for all integers $n \leq \nu(pN)$.

By [Stu87], we have $g \equiv f_1 \pmod{\lambda}$, so $a_q(g) \equiv a_q(f) \pmod{\lambda}$ for all primes $q \neq p$. Thus by the Brauer-Nesbitt theorem [CR62], the 2-dimensional $G_{\mathbb{Q}}$-representations $\varphi(A_f[\lambda_f])$ and $A_g[\lambda_g]$ are isomorphic.

Let $\mathfrak{m}$ be a maximal ideal of the Hecke algebra $\mathbb{T}(pN)$ that annihilates the module $A_g[\lambda_g]$. Note that $A_g[\mathfrak{m}] = A_g[\lambda_g]$ since $A_g[\mathfrak{m}] \subset A_g[\lambda_g]$ and $A_g[\lambda_g] \cong \varphi(A_f[\lambda_f])$ is irreducible as a $G_{\mathbb{Q}}$-module. The maximal ideal $\mathfrak{m}$ gives rise to a Galois representation $\overline{\rho}_{\mathfrak{m}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}(pN)/\mathfrak{m})$ isomorphic to $A_g[\lambda_g]$, which is irreducible since the Galois module $A_f[\lambda_f]$ is irreducible. Finally, we apply [Wil95, Thm. 2.1(i)] for $H = (\mathbb{Z}/N\mathbb{Z})^\times$ (i.e., $J_H = J_0(N)$) to conclude that $J_0(N)(\overline{\mathbb{Q}})[\mathfrak{m}] \cong (\mathbb{T}(pN)/\mathfrak{m})^2$, i.e., the representation $\overline{\rho}_{\mathfrak{m}}$ occurs with multiplicity one in $J_0(pN)$. Thus

$$A_g[\lambda_g] = \varphi(A_f[\lambda_f]).$$

□

LEMMA 5.2.2. *Suppose $\varphi : A \to B$ and $\psi : B \to C$ are homomorphisms of abelian varieties over a number field K, with φ an isogeny and ψ injective. Suppose n is an integer that is relatively prime to the degree of φ. If $G = \mathrm{Vis}_C(\text{Ш}(\mathbb{Q}, B))[n^\infty]$, then there is some injective homomorphism*

$$f : G \hookrightarrow \mathrm{Ker}\left\{(\psi \circ \varphi)_* : \text{Ш}(\mathbb{Q}, A) \longrightarrow \text{Ш}(\mathbb{Q}, C)\right\},$$

such that $\varphi_*(f(G)) = G$.

Proof. Let m be the degree of the isogeny $\varphi : A \to B$. Consider the complementary isogeny $\varphi' : B \to A$, which satisfies $\varphi \circ \varphi' = \varphi' \circ \varphi = [m]$. By hypothesis m is coprime to n, so $\gcd(m, \#G) = \gcd(m, n^\infty) = 1$, hence

$$\varphi_*(\varphi'_*(G)) = [m]G = G.$$

Thus $\varphi'_*(G)$ maps, via φ_*, to $G \subset \text{Ш}(\mathbb{Q}, B)$, which in turn maps to 0 in $\text{Ш}(\mathbb{Q}, C)$. □

LEMMA 5.2.3. *Let M be an odd integer coprime to N and let R be the subring of $\mathbb{T}(N)$ generated by all Hecke operators T_n with $\gcd(n, M) = 1$. Then $R = \mathbb{T}(N)$.*

Proof. See the lemma on page 491 of [Wil95]. (The condition that M is odd is necessary, as there is a counterexample when $N = 23$ and $M = 2$.) □

LEMMA 5.2.4. *Suppose λ is a maximal ideal of $\mathbb{T}(N)$ with generators a prime ℓ and $T_n - a_n$ (for all $n \in \mathbb{Z}$), with $a_n \in \mathbb{Z}$. For each integer $p \nmid N$, let λ_p be the ideal in $\mathbb{T}(N)$ generated by ℓ and all $T_n - a_n$, where n varies over integers coprime to p. Then $\lambda = \lambda_p$.*

Proof. Since $\lambda_p \subset \lambda$ and λ is maximal, it suffices to prove that λ_p is maximal. Let R be the subring of $\mathbb{T}(N)$ generated by Hecke operators T_n with $p \nmid n$. The quotient R/λ_p is a quotient of $\mathbb{Z}$ since each generator T_n is equivalent to an integer. Also, $\ell \in \lambda_p$, so $R/\lambda_p = \mathbb{F}_\ell$. But by Lemma 5.2.3, $R = \mathbb{T}(N)$, so $\mathbb{T}(N)/\lambda_p = \mathbb{F}_\ell$, hence λ_p is a maximal ideal. □

LEMMA 5.2.5. *Suppose that A is an abelian variety over a field K. Let R be a commutative subring of $\mathrm{End}(A)$ and I an ideal of R. Then*

$$(A/A[I])[I] \cong A[I^2]/A[I],$$

where the isomorphism is an isomorphism of $R[G_K]$-modules.

Proof. Let $a + A[I]$, for some $a \in A$, be an I-torsion element of $A/A[I]$. Then by definition, $xa \in A[I]$ for each $x \in I$. Therefore, $a \in A[I^2]$. Thus $a + A[I] \mapsto a + A[I]$ determines a well-defined homomorphism of $R[G_K]$-modules

$$\varphi : (A/A[I])[I] \to A[I^2]/A[I].$$

Clearly this homomorphism is injective. It is also surjective as every element $a + A[I] \in A[I^2]/A[I]$ is I-torsion as an element of $A/A[I]$, as $Ia \in A[I]$. Therefore, φ is an isomorphism of $R[G_K]$-modules. □

Lemma 5.2.6. *Let ℓ be a prime and let $\phi : E \to E'$ be an isogeny of elliptic curves of degree coprime to ℓ defined over a number field K. If v is any place of K then $\ell \mid c_{E,v}$ if and only if $\ell \mid c_{E',v}$.*

Proof. Consider the complementary isogeny $\phi' : E' \to E$. Both ϕ and ϕ' induce homomorphisms $\phi : \Phi_{E,v}(k_v) \to \Phi_{E',v}(k_v)$ and $\phi' : \Phi_{E',v}(k_v) \to \Phi_{E,v}(k_v)$ and $\phi \circ \phi'$ and $\phi' \circ \phi$ are multiplication-by-n maps. Since $(n, \ell) = 1$ then $\# \ker \phi$ and $\# \ker \phi'$ must be coprime to ℓ which implies the statement. $\square$

5.3 Proof of Theorem 5.1.3

Proof of Theorem 5.1.3. By [BCDT01] E is modular, so there is a rational newform $f \in S_2^{\mathrm{new}}(pN)$ which is an eigenform for the Hecke operators and an isogeny $E \to E_f$ defined over $\mathbb{Q}$, which by Hypothesis 4 can be chosen to have degree coprime to ℓ. Indeed, every cyclic rational isogeny is a composition of rational isogenies of prime degree, and E admits no rational ℓ-isogeny since $\overline{\rho}_{E,\ell}$ is irreducible.

By Hypothesis 1 the Tamagawa numbers of E are coprime to ℓ. Since E and E_f are related by an isogeny of degree coprime to ℓ, the Tamagawa numbers of E_f are also not divisible by ℓ by Lemma 5.2.6. Moreover, note that

$$E(\mathbb{Q}) \otimes \mathbb{F}_\ell \cong E_f(\mathbb{Q}) \otimes \mathbb{F}_\ell.$$

Let $\mathfrak{m}$ be the ideal of $\mathbb{T}(pN)$ generated by ℓ and $T_n - a_n(E)$ for all integers n coprime to p. Note that $\mathfrak{m}$ is maximal by Lemma 5.2.4.

Let φ be as in (3), and let $A = \varphi(A_f)$. Note that if $T_n \in \mathbb{T}(pN)$ then $T_n(E_f) \subset E_f$ since E_f is attached to a newform, and if, moreover $p \nmid n$, then $T_n(A) \subset A$ since the Hecke operators with index coprime to p commute with the degeneracy maps. Lemma 5.2.1 implies that

$$E_f[\ell] = E_f[\mathfrak{m}] = \varphi(A_f[\lambda]) \subset A,$$

so $\Psi = E_f[\ell]$ is a subgroup of A as a $G_{\mathbb{Q}}$-module. Let

$$C = (A \times E_f)/\Psi,$$

where we embed Ψ in $A \times E_f$ anti-diagonally, i.e., by the map $x \mapsto (x, -x)$. The antidiagonal map $\Psi \to A \times E_f$ commutes with the Hecke operators T_n for $p \nmid n$, so $(A \times E_f)/\Psi$ is preserved by the T_n with $p \nmid n$. Let R be the subring of $\mathrm{End}(C)$ generated by the action of all Hecke operators T_n, with $p \nmid n$. Also note that $T_p \in \mathrm{End}(J_0(pN))$ acts by Hypothesis 3 as -1 on E_f, but T_p need *not* preserve A.

Suppose for the moment that we have verified that the hypothesis of Theorem 4.1.1 are satisfied with A, $B = E_f$, C, $Q = C/B$, R as above and $K = \mathbb{Q}$. Then we obtain an injective homomorphism

$$E(\mathbb{Q})/\ell E(\mathbb{Q}) \cong E_f(\mathbb{Q})/\ell E_f(\mathbb{Q}) \hookrightarrow \mathrm{Ker}(\text{Ш}(\mathbb{Q}, A) \to \text{Ш}(\mathbb{Q}, C))[\mathfrak{m}].$$

We then apply Lemma 5.2.2 with $n = \ell$, A_f, A, and C, respectively, to see that

$$E_f(\mathbb{Q})/\ell E_f(\mathbb{Q}) \subset \mathrm{Ker}(\text{Ш}(\mathbb{Q}, A_f) \to \text{Ш}(\mathbb{Q}, C))[\lambda].$$

That $E_f(\mathbb{Q})/\ell E_f(\mathbb{Q})$ lands in the λ-torsion is because the subgroup of $\mathrm{Vis}_C(\text{Ш}(\mathbb{Q}, E_f))$ that we constructed is $\mathfrak{m}$-torsion.

Finally, consider $A \times E_f \to J_0(pN)$ given by $(x, y) \mapsto x + y$. Note that Ψ maps to 0, since $(x, -x) \mapsto 0$ and the elements of Ψ are of the form $(x, -x)$. We have a (not-exact!) sequence of maps

$$\text{Ш}(\mathbb{Q}, A_f) \to \text{Ш}(\mathbb{Q}, C) \to \text{Ш}(\mathbb{Q}, J_0(pN)),$$

hence inclusions

$$\begin{aligned} E_f(\mathbb{Q})/\ell E_f(\mathbb{Q}) &\subseteq \mathrm{Ker}(\text{Ш}(\mathbb{Q}, A_f) \to \text{Ш}(\mathbb{Q}, C)) \\ &\subseteq \mathrm{Ker}(\text{Ш}(\mathbb{Q}, A_f) \to \text{Ш}(\mathbb{Q}, J_0(pN))), \end{aligned}$$

which gives the conclusion of the theorem.

It remains to verify the hypotheses of Theorem 4.1.1. That $C = A + B$ is clear from the definition of C. Also, $A \cap E_f = E_f[\ell]$, which is finite. We explained above when defining R that each of A and E_f is preserved by R. Since $K = \mathbb{Q}$ and ℓ is odd the condition $1 = e < \ell - 1$ is satisfied. That $A(\mathbb{Q})$ is finite follows from our hypothesis that $L(A_f, 1) \neq 0$ (by [KL89]).

It remains is to verify that the groups

$$Q(\mathbb{Q})[\mathfrak{m}], \quad E_f(\mathbb{Q})[\mathfrak{m}], \quad \Phi_{A,q}(\mathbb{F}_q)[\mathfrak{m}], \quad \text{and } \Phi_{E_f,q}(\mathbb{F}_q)[\ell],$$

are 0 for all primes $q \mid pN$. Since $\ell \in \mathfrak{m}$, we have by Hypothesis 4 that

$$E_f(\mathbb{Q})[\mathfrak{m}] = E_f(\mathbb{Q})[\ell] = 0.$$

We will now verify that $Q(\mathbb{Q})[\mathfrak{m}] = 0$. From the definition of C and Ψ we have $Q \cong A/\Psi$. Let λ_p be as in Lemma 5.2.4 with $a_n = a_n(E)$. The map φ induces an isogeny of 2-power degree

$$A_f/(A_f[\lambda]) \to A/\Psi.$$

Thus there is λ_p-torsion in $(A_f/(A_f[\lambda]))(\mathbb{Q})$ if and only if there is $\mathfrak{m}$-torsion in $(A/\Psi)(\mathbb{Q})$. Thus it suffices to prove that $(A_f/A_f[\lambda])(\mathbb{Q})[\lambda_p] = 0$.

By Lemma 5.2.4, we have $\lambda_p = \lambda$, and by Lemma 5.2.5,

$$(A_f/A_f[\lambda])[\lambda] \cong A_f[\lambda^2]/A_f[\lambda].$$

By [Maz77, §II.14], the quotient $A_f[\lambda^2]/A_f[\lambda]$ injects into a direct sum of copies of $A_f[\lambda]$ as Galois modules. But $A_f[\lambda] \cong E[\ell]$ is irreducible, so $(A_f[\lambda^2]/A_f[\lambda])(\mathbb{Q}) = 0$, as required.

By Hypothesis 2, we have $\Phi_{A_f,q}(\mathbb{F}_q)[\lambda] = 0$ for each prime divisor $q \mid N$.Since A is 2-power isogenous to A_f and ℓ is odd, this verifies the Tamagawa number hypothesis for A. Our hypothesis that $a_p(E) = -1$ implies that Frob_p acts on $\Phi_{E_f,p}(\overline{\mathbb{F}}_p)$ as -1. Thus $\Phi_{E_f,p}(\mathbb{F}_p)[\ell] = 0$ since ℓ is odd. This completes the proof. $\square$

Remark 5.3.1. An essential ingrediant in the proof of the above theorem is the multiplicity one result used in the paper of Wiles (see [Wil95, Thm. 2.1.]). Since this result holds for Jacobians J_H of the curves $X_H(N)$ that are intermediate covers for the covering $X_1(N) \to X_0(N)$ corresponding to subgroups $H \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$ (i.e., the Galois group of $X_1(N) \to X_H$ is H), one should be able to give a generalization of Theorem 5.1.3 which holds for newform subvarieties of J_H. This requires generalizing some results from [Rib90b] to arbitrary H.

5.4 A VARIANT OF THEOREM 5.1.3 WITH SIMPLER HYPOTHESIS

PROPOSITION 5.4.1. *Suppose $A = A_f \subset J_0(N)$ is a newform abelian variety and q is a prime that exactly divides N. Suppose $\mathfrak{m} \subset \mathbb{T}(N)$ is a non-Eisenstein maximal ideal of residue characteristic ℓ and that $\ell \nmid m_A$, where m_A is the modular degree of A. Then $\Phi_{A,q}(\overline{\mathbb{F}}_q)[\mathfrak{m}] = 0$.*

Proof. The component group of $\Phi_{J_0(N),q}(\overline{\mathbb{F}}_q)$ is Eisenstein by [Rib87], so

$$\Phi_{J_0(N),q}(\overline{\mathbb{F}}_q)[\mathfrak{m}] = 0.$$

By Lemma 4.2.2, the image of $\Phi_{J_0(N),q}(\overline{\mathbb{F}}_q)$ in $\Phi_{A^\vee,q}(\overline{\mathbb{F}}_q)$ has no $\mathfrak{m}$ torsion. By the main theorem of [CS01], the cokernel $\Phi_{J_0(N),q}(\overline{\mathbb{F}}_q)$ in $\Phi_{A^\vee,q}(\overline{\mathbb{F}}_q)$ has order that divides m_A. Since $\ell \nmid m_A$, it follows that the cokernel also has no $\mathfrak{m}$ torsion. Thus Lemma 4.2.2 implies that $\Phi_{A^\vee,q}(\overline{\mathbb{F}}_q)[\mathfrak{m}] = 0$. Finally, the modular polarization $A \to A^\vee$ has degree m_A, which is coprime to ℓ, so the induced map $\Phi_{A,q}(\overline{\mathbb{F}}_q) \to \Phi_{A^\vee,q}(\overline{\mathbb{F}}_q)$ is an isomorphism on ℓ primary parts. In particular, that $\Phi_{A^\vee,q}(\overline{\mathbb{F}}_q)[\mathfrak{m}] = 0$ implies that $\Phi_{A,q}(\overline{\mathbb{F}}_q)[\mathfrak{m}] = 0$. $\square$

If E is a semistable elliptic curve over $\mathbb{Q}$ with discriminant Δ, then we see using Tate curves that $\overline{c}_p = \mathrm{ord}_p(\Delta)$.

THEOREM 5.4.2. *Suppose $A = A_f \subset J_0(N)$ is a newform abelian variety with $L(A_{/\mathbb{Q}}, 1) \neq 0$ and N square free, and let ℓ be a prime. Suppose that $p \nmid N$ is a prime, and that there is an elliptic curve E of conductor pN such that:*

1. *[Rank] The Mordell-Weil rank of $E(\mathbb{Q})$ is positive.*
2. *[Divisibility] We have $a_p(E) = -1$, $\ell \mid \overline{c}_{E,p}$, and*
$$\ell \nmid 2 \cdot N \cdot p \cdot c_{E,p} \cdot \prod_{q \mid N} \overline{c}_{E,q}.$$
3. *[Irreducibility] The mod ℓ representation $\overline{\rho}_{E,\ell}$ is irreducible.*
4. *[Noncongruence] The representation $\overline{\rho}_{E,\ell}$ is not isomorphic to any representation $\overline{\rho}_{g,\lambda}$ where $g \in S_2(\Gamma_0(N))$ is a newform of level dividing N that is not conjugate to f.*

Then there is an element of order ℓ in $Ш(\mathbb{Q}, A_f)$ that is not visible in $J_0(N)$ but is strongly visible in $J_0(pN)$. More precisely, there is an inclusion

$$E(\mathbb{Q})/\ell E(\mathbb{Q}) \hookrightarrow \mathrm{Ker}(Ш(\mathbb{Q}, A_f) \to Ш(\mathbb{Q}, C))[\lambda] \subset \mathrm{Vis}_{pN}(Ш(\mathbb{Q}, A_f))[\lambda],$$

where $C \subset J_0(pN)$ is isogenous to $A_f \times E$, the homomorphism $A_f \to C$ has degree a power of 2, and λ is the maximal ideal of $\mathbb{T}(N)$ corresponding to $\overline{\rho}_{E,\ell}$.

Proof. The divisibility assumptions of Hypothesis 2 on the $\overline{c}_{E,q}$ imply that the Serre level of $\overline{\rho}_{E,\ell}$ is N and since $\ell \nmid N$, the Serre weight is 2 (see [RS01, Thm. 2.10]). Since ℓ is odd, Ribet's level lowering theorem [Rib91] implies that there is *some* newform $h = \sum b_n q^n \in S_2(\Gamma_0(N))$ and a maximal ideal λ over ℓ such that $a_q(E) \equiv b_q \pmod{\lambda}$ for all primes $q \neq p$. By our non-congruence hypothesis, the only possibility is that h is a $G_{\mathbb{Q}}$-conjugate of f. Since we can replace f by any Galois conjugate of f without changing A_f, we may assume that $f = h$. Also $a_p(f) \equiv -(p+1) \pmod{\lambda}$, as explained in [Rib83, pg. 506].

Hypothesis 3 implies that λ is not Eisenstein, and by assumption $\ell \nmid m_A$, so Proposition 5.4.1 implies that $\Phi_{A,q}(\overline{\mathbb{F}}_q)[\lambda] = 0$ for each $q \mid N$.

The theorem now follows from Theorem 5.1.3. □

Remark 5.4.3. The condition $a_p(E) = -1$ is redundant. Indeed, we have $\overline{c}_{E,p} \neq c_{E,p}$ since $\overline{c}_{E,p}$ is divisible by ℓ and $c_{E,p}$ is not. By studying the action of Frobenius on the component group at p one can show that this implies that E has nonsplit multiplicative reduction, so $a_p(E) = -1$.

Remark 5.4.4. The non-congruence hypothesis of Theorem 5.4.2 can be verified using modular symbols as follows. Let $W \subset H_1(X_0(N), \mathbb{Z})_{\mathrm{new}}$ be the saturated submodule of $H_1(X_0(N), \mathbb{Z})$ that corresponds to all newforms in $S_2(\Gamma_0(N))$ that are not Galois conjugate to f. Let $\overline{W} = W \otimes \mathbb{F}_\ell$. We require that the intersection of the kernels of $T_q|_{\overline{W}} - a_q(E)$, for $q \neq p$, has dimension 0.

6 Computational Examples

In this section we give examples that illustrate how to use Theorem 5.4.2 to prove existence of elements of the Shafarevich-Tate group of a newform subvariety of $J_0(N)$ (for 767 and 959) which are invisible at the base level, but become visible in a modular Jacobian of higher level.

Hypothesis 6.0.5. The statements in this section all make the hypothesis that certain commands of the computer algebra system Magma [BCP97] produce correct output.

6.1 Level 767

Consider the modular Jacobian $J_0(767)$. Using the modular symbols package in Magma, one decomposes $J_0(767)$ (up to isogeny) into a product of six optimal quotients of dimensions 2, 3, 4, 10, 17 and 23. The duals of these quotients are subvarieties $A_2, A_3, A_4, A_{10}, A_{17}$ and A_{23} defined over $\mathbb{Q}$, where A_d has dimension d. Consider the subvariety A_{23}.

We first show that the Birch and Swinnerton-Dyer conjectural formula predicts that the orders of the groups $Ш(\mathbb{Q}, A_{23})$ and $Ш(\mathbb{Q}, A_{23}^\vee)$ are both divisible by 9.

PROPOSITION 6.1.1. *Assume [AS05, Conj. 2.2]. Then*

$$3^2 \mid \#Ш(\mathbb{Q}, A_{23}) \quad \textit{and} \quad 3^2 \mid \#Ш(\mathbb{Q}, A_{23}^\vee).$$

Proof. Let $A = A_{23}^\vee$. We use [AS05, §3.5 and §3.6] (see also [Ka81]) to compute a multiple of the order of the torsion subgroup $A(\mathbb{Q})_{\mathrm{tor}}$. This multiple is obtained by injecting the torsion subgroup into the group of $\mathbb{F}_p$-rational points on the reduction of A for odd primes p of good reduction and then computing the order of that group. Hence, the multiple is an isogeny invariant, so one gets the same multiple for $A^\vee(\mathbb{Q})_{\mathrm{tor}}$. For producing a divisor of $\#A(\mathbb{Q})_{\mathrm{tor}}$, we use the injection of the subgroup of rational cuspidal divisor classes of degree 0 into $A(\mathbb{Q})_{\mathrm{tor}}$. Using the implementation in Magma we obtain $120 \mid \#A(\mathbb{Q})_{\mathrm{tor}} \mid 240$. To compute a divisor of $A^\vee(\mathbb{Q})_{\mathrm{tor}}$, we use the algorithm described in [AS05, §3.3] to find that the modular degree $m_A = 2^{34}$, which is not divisible by any odd primes, hence $15 \mid \#A^\vee(\mathbb{Q})_{\mathrm{tor}} \mid 240$.

Next, we use [AS05, §4] to compute the ratio of the special value of the L-function of $A_{/\mathbb{Q}}$ at 1 over the real Néron period Ω_A. We obtain $\dfrac{L(A_{/\mathbb{Q}},1)}{\Omega_A} = c_A \cdot \dfrac{2^9 \cdot 3}{5}$, where $c_A \in \mathbb{Z}$ is the Manin constant. Since $c_A \mid 2^{\dim(A)}$ by [ARS06] then

$$\frac{L(A_{/\mathbb{Q}},1)}{\Omega_A} = \frac{2^{n+2} \cdot 3}{5},$$

for some $0 \leq n \leq 23$. In particular, the modular abelian variety $A_{/\mathbb{Q}}$ has rank zero over $\mathbb{Q}$.

Next, using the algorithms from [CS01, KS00] we compute the Tamagawa number $c_{A,13} = 1920 = 2^3 \cdot 3 \cdot 5$. We also find that $2 \mid c_{A,59}$ is a power of 2 because W_{59} acts as 1 on A, and on the component group $\mathrm{Frob}_{59} = -W_{59}$, so the fixed subgroup $\Phi_{A,59}(\mathbb{F}_{59})$ of Frobenius is a 2-group (for more details, see [Rib90a, Prop. 3.7–8]).

Finally, the Birch and Swinnerton-Dyer conjectural formula for abelian varieties of Mordell-Weil rank zero (see [AS05, Conj. 2.2]) asserts that

$$\frac{L(A_{/\mathbb{Q}},1)}{\Omega_A} = \frac{\#Ш(\mathbb{Q}, A) \cdot c_{A,13} \cdot c_{A,59}}{\#A(\mathbb{Q})_{\mathrm{tor}} \cdot \#A^\vee(\mathbb{Q})_{\mathrm{tor}}}.$$

By substituting what we computed above, we obtain $3^2 \mid \#Ш(\mathbb{Q}, A)$. Since $L(A_{/\mathbb{Q}}, 1) \neq 0$, [KL89] implies that $Ш(\mathbb{Q}, A)$ is finite. By the nondegeneracy of the Cassels-Tate pairing, $\#Ш(\mathbb{Q}, A) = \#Ш(A^\vee/\mathbb{Q})$. Thus, if the BSD conjectural formula is true then $3^2 \mid \#Ш(\mathbb{Q}, A) = \#Ш(\mathbb{Q}, A^\vee)$. ∎

We next observe that there are no visible elements of odd order for the embedding $A_{23/\mathbb{Q}} \hookrightarrow J_0(767)_{/\mathbb{Q}}$.

LEMMA 6.1.2. *Any element of* $\text{Ш}(\mathbb{Q}, A_{23})$ *which is visible in* $J_0(767)$ *has order a power of* 2.

Proof. Since $m_{A_{23}} = 2^{34}$, [AS05, Prop. 3.15] implies that any element of $\text{Ш}(\mathbb{Q}, A_{23})$ that is visible in $J_0(767)$ has order a power of 2. □

Finally, we use Theorem 5.4.2 to prove the existence of non-trivial elements of order 3 in $\text{Ш}(\mathbb{Q}, A_{23})$ which are invisible at level 767, but become visible at higher level. In particular, we prove unconditionally that $3 \mid \#\text{Ш}(\mathbb{Q}, A_{23})$ which provides evidence for the Birch and Swinnerton-Dyer conjectural formula.

PROPOSITION 6.1.3. *There is an element of order 3 in* $\text{Ш}(\mathbb{Q}, A_{23})$ *which is not visible in* $J_0(767)$ *but is strongly visible in* $J_0(2 \cdot 767)$.

Proof. Let $A = A_{23}$, and note that A has rank 0, since $L(A_{/\mathbb{Q}}, 1) \neq 0$. Using Cremona's database [Cre] we find that the elliptic curve

$$E: \qquad y^2 + xy = x^3 - x^2 + 5x + 37$$

has conductor $2 \cdot 767$ and Mordell-Weil group $E(\mathbb{Q}) = \mathbb{Z} \oplus \mathbb{Z}$. Also

$$c_2 = 2, c_{13} = 2, c_{59} = 1, \overline{c}_2 = 6, \overline{c}_{13} = 2, \overline{c}_{59} = 1.$$

We apply Theorem 5.4.2 with $\ell = 3$ and $p = 2$. Since E does not admit any rational 3-isogeny (by [Cre]), Hypothesis 3 is satisfied. The level is square free and the modular degree of A is a power of 2, so Hypothesis 2 is satisfied.

We have $a_3(E) = -3$. Using Magma we find

$$\det(T_3|_{\overline{W}} - (-3)) \equiv 1 \pmod{3},$$

which verifies the noncongruence hypothesis and completes the proof. □

6.2 LEVEL 959

We do similar computations for a 24-dimensional abelian subvariety of $J_0(959)$. We have $959 = 7 \cdot 137$, which is square free. There are five newform abelian subvarieties of the Jacobian, A_2, A_7, A_{10}, A_{24} and A_{26}, whose dimensions are the corresponding subscripts. Let $A_f = A_{24}$ be the 24-dimensional newform abelian subvariety.

PROPOSITION 6.2.1. *There is an element of order 3 in* $\text{Ш}(A_f/\mathbb{Q})$ *which is not visible in* $J_0(959)$ *but is strongly visible in* $J_0(2 \cdot 959)$.

Proof. Using Magma we find that $m_A = 2^{32} \cdot 583673$, which is coprime to 3. Thus we apply Theorem 5.4.2 with $\ell = 3$ and $p = 2$. Consulting [Cre] we find the curve E=1918C1, with Weierstrass equation

$$y^2 + xy + y = x^3 - 22x - 24,$$

with Mordell-Weil group $E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})$, and

$$c_2 = 2, c_7 = 2, c_{137} = 1, \overline{c}_2 = 6, \overline{c}_7 = 2, \overline{c}_{137} = 1.$$

Using [Cre] we find that E has no rational 3-isogeny. The modular form attached to E is

$$g = q - q^2 - 2q^3 + q^4 - 2q^5 + \cdots ,$$

and we have

$$\det(T_2|_{\overline{W}} - (-2)) = 2177734400 \equiv 2 \pmod 3,$$

which completes the verification. □

7 Conjecture, evidence and more computational data

We state several conjectures, provide some evidence and finally, provide a table that we computed using similar techniques to those in Section 6

7.1 The conjecture

The two examples computed in Section 6 show that for an abelian subvariety A of $J_0(N)$ an invisible element of $\text{Ш}(\mathbb{Q}, A)$ at the base level N might become visible at a multiple level NM. We state a general conjecture according to which any element of $\text{Ш}(\mathbb{Q}, A)$ should have such a property.

CONJECTURE 7.1.1. *Let $h = 0$ or 1. Suppose A is a J_h-modular abelian variety and $c \in \text{Ш}(\mathbb{Q}, A)$. Then there is a J_h-modular abelian variety C and an inclusion $\iota : A \to C$ such that $\iota_* c = 0$.*

Remark 7.1.2. For any prime ℓ, the Jacobian $J_h(N)$ comes equipped with two morphisms $\alpha^*, \beta^* : J_h(N) \to J_h(N\ell)$ induced by the two degeneracy maps $\alpha, \beta : X_h(\ell N) \to X_h(N)$ between the modular curves of levels ℓN and N, and it is natural to consider visibility of $\text{Ш}(\mathbb{Q}, A)$ in $J_h(N\ell)$ via morphisms ι constructed from these degeneracy maps.

Remark 7.1.3. It would be interesting to understand the set of all levels N of J_h-modular abelian varieties C that satisfy the conclusion of the conjecture.

7.2 THEORETICAL EVIDENCE FOR THE CONJECTURES

The first piece of theoretical evidence for Conjecture 7.1.1 is Remark 3.0.2, according to which any cohomology class $c \in \mathrm{H}^1(K, A)$ is visible in some abelian variety $C_{/K}$.

The next proposition gives evidence for elements of $\text{Ш}(\mathbb{Q}, E)$ for an elliptic curve E and elements of order 2 or 3.

PROPOSITION 7.2.1. *Suppose E is an elliptic curve over $\mathbb{Q}$. Then Conjecture 7.1.1 for $h = 0$ is true for all elements of order 2 and 3 in $\text{Ш}(\mathbb{Q}, E)$.*

Proof. We first show that there is an abelian variety C of dimension 2 and an injective homomorphism $i : E \hookrightarrow C$ such that $c \in \mathrm{Vis}_C(\text{Ш}(\mathbb{Q}, E))$. If c has order 2, this follows from [AS02, Prop. 2.4] or [Kle01], and if c has order 3, this follows from [Maz99, Cor. pg. 224]. The quotient C/E is an elliptic curve, so C is isogenous to a product of two elliptic curves. Thus by [BCDT01], C is a quotient of $J_0(N)$, for some N. □

We also prove that Conjecture 7.1.1 is true with $h = 1$ for all elements of $\text{Ш}(\mathbb{Q}, A)$ which split over abelian extensions.

PROPOSITION 7.2.2. *Suppose $A_{/\mathbb{Q}}$ is a J_1-modular abelian variety over $\mathbb{Q}$ and $c \in \text{Ш}(\mathbb{Q}, A)$ splits over an abelian extension of $\mathbb{Q}$. Then Conjecture 7.1.1 is true for c with $h = 1$.*

Proof. Suppose K is an abelian extension such that $\mathrm{res}_K(c) = 0$ and let $C = \mathrm{Res}_{K/\mathbb{Q}}(A_K)$. Then c is visible in C (see Section 3.0.2). It remains to verify that C is modular. As discussed in [Mil72, pg. 178], for any abelian variety B over K, we have an isomorphism of Tate modules

$$\mathrm{Tate}_\ell(\mathrm{Res}_{K/\mathbb{Q}}(B_K)) \cong \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} \mathrm{Tate}_\ell(B_K),$$

and by Faltings's isogeny theorem [Fal86], the Tate module determines an abelian variety up to isogeny. Thus if $B = A_f$ is an abelian variety attached to a newform, then $\mathrm{Res}_{K/\mathbb{Q}}(B_K)$ is isogenous to a product of abelian varieties A_{f^χ}, where χ runs through Dirichlet characters attached to the abelian extension $K/\mathbb{Q}$. Since A is isogenous to a product of abelian varieties of the form A_f (for various f), it follows that the restriction of scalars C is modular. □

Remark 7.2.3. Suppose that E is an elliptic curve and $c \in \text{Ш}(\mathbb{Q}, E)$. Is there an abelian extension $K/\mathbb{Q}$ such that $\mathrm{res}_K(c) = 0$? The answer is "yes" if and only if there is a K-rational point (with K-abelian) on the locally trivial principal homogeneous space corresponding to c (this homogenous space is a genus one curve). Recently, M. Ciperiani and A. Wiles proved that any genus one curve over $\mathbb{Q}$ which has local points everywhere and whose Jacobian is a semistable elliptic curve admits a point over a solvable extension of $\mathbb{Q}$ (see [CW06]). Unfortunately, this paper does not answer our question about the existence of abelian points.

Remark 7.2.4. As explained in [Ste04], if $K/\mathbb{Q}$ is an abelian extension of prime degree then there is an exact sequence

$$0 \to A \to \mathrm{Res}_{K/\mathbb{Q}}(E_K) \xrightarrow{\mathrm{Tr}} E \to 0,$$

where A is an abelian variety with $L(A_{/\mathbb{Q}}, s) = \prod L(f_i, s)$ (here, the f_i's are the $G_{\mathbb{Q}}$-conjugates of the twist of the newform f_E attached to E by the Dirichlet character associated to $K/\mathbb{Q}$). Thus one could approach the question in the previous remark by investigating whether or not $L(f_E, \chi, 1) = 0$ which one could do using modular symbols (see [CFK06]). The authors expect that L-functions of twists of degree larger than three are very unlikely to vanish at $s = 1$ (see [CFK06]), which suggests that in general, the question might have a negative answer for cohomology classes of order larger than 3.

7.3 Visibility of Kolyvagin cohomology classes

It would also be interesting to study visibility at higher level of Kolyvagin cohomology classes. The following is a first "test question" in this direction.

QUESTION 7.3.1. Suppose $E \subset J_0(N)$ is an elliptic curve with conductor N, and fix a prime ℓ such that $\overline{\rho}_{E,\ell}$ is surjective. Fix a quadratic imaginary field K that satisfies the Heegner hypothesis for E. For any prime p satisfying the conditions of [Rub89, Prop. 5], let $c_p \in \mathrm{H}^1(\mathbb{Q}, E)[\ell]$ be the corresponding Kolyvagin cohomology class. There are two natural homomorphisms $\delta_1^*, \delta_p^* : E \to J_0(Np)$. When is

$$(\delta_1^* \pm \delta_\ell^*)_*(c_\ell) = 0 \in \mathrm{H}^1(\mathbb{Q}, J_0(Np))?$$

When is

$$\mathrm{res}_v((\delta_1^* \pm \delta_\ell^*)_*(c_\ell)) = 0 \in \mathrm{H}^1(\mathbb{Q}_v, J_0(Np))?$$

7.4 Table of Strong Visibility at Higher Level

The following is a table that gives the known examples of $A_{f/\mathbb{Q}}$ with square free conductor $N \leq 1339$, such that the Birch and Swinnerton-Dyer conjectural formula predicts an odd prime divisor ℓ of $Ш(\mathbb{Q}, A_f)$, but ℓ does not divide the modular degree of A_f. These were taken from [AS05]. If there is an entry in the fourth column, this means we have verified the hypothesis of Theorem 5.4.2, hence there really is a nonzero element in $Ш(\mathbb{Q}, A_f)$ that is not visible in $J_0(N)$, but is strongly visible in $J_0(pN)$. The notation in the fourth column is (p, E, q), where p is the prime used in Theorem 5.4.2, E is an elliptic curve, denoted using a Cremona label, and $q \neq p$ is a prime such that

$$\bigcap_{q' \leq q} \mathrm{Ker}(T'_q|_{\overline{W}} - a_{q'}(E)) = 0.$$

A_f	dim	$\ell \mid Ш(A_f)$?	moddeg	(p, E, q)'s
551H	18	3	$2^? \cdot 13^2$	(2, 1102A1, -)
767E	23	3	2^{34}	(2, 1534B1, 3)
959D	24	3	$2^{32} \cdot 583673$	(2, 1918C1, 5), (7, 5369A1,2)
1337E	33	3	$2^{59} \cdot 71$	(2, 2674A1, 5)
1339G	30	3	$2^{48} \cdot 5776049$	(2, 2678B1, 3), (11, 14729A1,2)

REFERENCES

[Aga99b] A. Agashe, *On invisible elements of the Tate-Shafarevich group*, C. R. Acad. Sci. Paris Sér. I Math. 328 (1999), no. 5, 369–374.

[AS02] A. Agashe and W. A. Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory 97 (2002), no. 1, 171–185.

[AS05] A. Agashe and W. Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. 74 (2005), no. 249, 455–484 (electronic), With an appendix by J. Cremona and B. Mazur.

[ARS06] A. Agashe, K. A. Ribet and W. Stein, *The Manin constant*, to appear in Quarterly J. of Pure and Applied Math. volume in honor of J. Coates.

[AM69] M. F. Atiyah and I. G.Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., (1969).

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), no. 4, 843–939 (electronic).

[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).

[CW06] M. Ciperiani, A. Wiles, *Solvable points on genus one curves*, preprint (2006).

[CFK06] C. David, J. Fearnly, H. Kisilevsky, *Vanishing of twisted L-functions of elliptic curves*, to appear in Experiment. Math.

[CM00] J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. 9 (2000), no. 1, 13–28.

[CV92] R. F. Coleman, J. F. Voloch, *Companion forms and Kodaira-Spencer theory*, Invent. Math., 110, (1992), 2, 263–281.

[CS01] B.Conrad, W. A. Stein, *Component groups of purely toric quotients*, Math. Res. Lett., 8, 5–6, (2001), 745–766.

[Cre] J. E. Cremona, *Tables of Elliptic Curves,* `http://www.maths.nott.ac.uk/personal/jec/ftp/data/`

[CR62] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962, Pure and Applied Mathematics, Vol. XI.

[Fal86] G. Faltings, *Finiteness theorems for abelian varieties over number fields*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, Translated from the German original [Invent. Math. 73 (1983), no. 3, 349–366; ibid. 75 (1984), no. 2, 381] by Edward Shipz, pp. 9–27.

[Ka81] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. 62 (1981), no. 3, 481–502.

[Kle01] T. Klenke, *Modular Varieties and Visibility*, Ph.D. thesis, Harvard University (2001).

[KS00] D. R. Kohel and W. A. Stein, *Component Groups of Quotients of* $J_0(N)$, Proc. ANTS-IV, Springer, 2000.

[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.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math., 47, (1977), 33–186.

[Maz99] ———, *Visualizing elements of order three in the Shafarevich-Tate group*, Asian J. Math. 3 (1999), no. 1, 221–232, Sir Michael Atiyah: a great mathematician of the twentieth century.

[Mil72] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. 17 (1972), 177–190.

[Mil86] ———, *Arithmetic duality theorems*, Academic Press Inc., Boston, Mass., (1986), x+421.

[Rib83] K. A. Ribet, *Congruence relations between modular forms*, Proc. International Congress of Mathematicians, 503–514, (1983).

[Rib87] ———, *On the component groups and the Shimura subgroup of* $J_0(N)$, Séminaire de Théorie des Nombres, 1987–1988 (Talence, 1987–1988), Exp. No. 6, 10, Univ. Bordeaux I.

[Rib90a] ———, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math., 100 1990, no. 2, 431–476.

[Rib90b] ______, *Raising the levels of modular representations*, Séminaire de Théorie des Nombres, Paris 1987–88, Birkhäuser Boston, Boston, MA, 1990, pp. 259–271.

[Rib91] ______, *Lowering the levels of modular representations without multiplicity one*, International Mathematics Research Notices, (1991), 15–19.

[Rib92] ______, *Abelian varieties over* $\mathbf{Q}$ *and modular forms*, Algebra and topology 1992 (Taejŏn), Korea Adv. Inst. Sci. Tech., Taejŏn, 1992, pp. 53–79.

[RS01] K. A. Ribet and W. A. Stein, *Lectures on Serre's conjectures*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., 9, 143–232, Amer. Math. Soc., Providence, RI, (2001).

[Rub89] K. Rubin, *The work of Kolyvagin on the arithmetic of elliptic curves*, Arithmetic of complex manifolds (Erlangen, 1988), 128–136, Springer, Berlin, (1989).

[Se79] J-P. Serre, *Local fields*, Springer-Verlag, New York, (1979).

[Shi94] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, reprint of the 1971 original, Kan Memorial Lectures, 1, Princeton University Press, (1994).

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

[Ste04] W. A. Stein, *Shafarevich-Tate Groups of Nonsquare Order*, Modular Curves and Abelian Varieties, Progress of Mathematics (2004), 277–289.

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

[Wil95] A. J. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2), 141(3), (1995), 443–551.

Dimitar P. Jetchev
Department of Mathematics
University of California
Berkeley, CA 94720-3840
`jetchev@math.berkeley.edu`

William A. Stein
Department of Mathematics
University of Washington
Seattle, WA 98195-4350
`wstein@u.washington.edu`