

Visualizing Elements of Shafarevich-Tate Groups at Higher Level

Dimitar Jetchev

William Stein*

August 8, 2005

Abstract

We consider visibility of Shafarevich-Tate groups of modular abelian varieties in modular Jacobians of higher level, and give hypotheses that imply the existence of visible elements at a specific higher level. We also give a table of elements that are visible at higher level, and make conjectures inspired by our results.

1 Introduction

This paper is about visibility of Shafarevich-Tate groups of modular abelian varieties in modular Jacobians of higher level. We prove a theorem that allows one to deduce the existence of visible elements of III at a specific higher level. We also give a table of examples of elements of III that are visible at higher level, and make conjectures inspired by our results.

In the rest of this introduction we explain the background and motivation for studying visibility of Shafarevich-Tate groups.

1.1 The Birch and Swinnerton-Dyer Conjecture

Let A be an abelian variety defined over a number field K of rank r and let $L(A, s)$ be the corresponding global Hasse-Weil L -function.

Conjecture 1.1 (Birch and Swinnerton-Dyer Conjecture). *The function $L(A, s)$ has an analytic continuation to a neighborhood of 1 and its order of vanishing at $s = 1$ is equal to r .*

The second conjecture is a precise formula for the r -th derivative of the L -function of in terms of the arithmetic and geometry of the variety. As we will need the conjectural formula only over \mathbb{Q} , we will not state it in the general case of a number field. We refer the reader to [Lan91, III, Conjecture 5.3] for the most general statement of the conjecture for abelian varieties over arbitrary number fields.

*This material is based upon work supported by the National Science Foundation under Grant No. 0400386.

Conjecture 1.2 (BSD Conjectural Formula). *Let A be an abelian variety over \mathbb{Q} . The Hasse-Weil L -function $L(A, s)$ extends to an analytic function in a neighborhood of $s = 1$ and it satisfies the formula*

$$\frac{L^{(r)}(A, 1)}{r!} = \frac{\Omega_A \cdot \prod c_{A,p} \cdot \text{Reg}_A \cdot \#\text{III}(A/\mathbb{Q})}{\#A(\mathbb{Q})_{\text{tor}} \cdot \#A^\vee(\mathbb{Q})_{\text{tor}}},$$

where $\Omega_A = \int_{A(\mathbb{R})} |\omega|$ for a nowhere vanishing Néron differential $\omega \in H^0(A, \Omega_A^d)$, $c_{A,p} = \#\Phi_{A,p}(\mathbb{F}_p)$ is the order of the group of rational points in the component group of the special fiber of the Néron model at the prime p , Reg_A is the discriminant of the canonical height pairing between $A(\mathbb{Q})$ and $A^\vee(\mathbb{Q})$, and

$$\text{III}(A/\mathbb{Q}) = \text{Ker} \left(H^1(\mathbb{Q}, A) \rightarrow \bigoplus_{\nu} H^1(\mathbb{Q}_\nu, A) \right)$$

is the Shafarevich-Tate group of the abelian variety A over \mathbb{Q} .

Kolyvagin proved Conjecture 1.1 when A is an elliptic curve over \mathbb{Q} and the order of vanishing of $L(E, s)$ at $s = 1$ is either 0 or 1 (see, e.g., [Gro91] and [BCDT01]). Very little is known when the order of vanishing is at least 2.

1.2 Visible Subgroups of Shafarevich-Tate Groups

Agashe, Cremona, Mazur, and the second author have studied visibility of Shafarevich-Tate groups of elliptic curves and abelian varieties (see [Aga99, AS05, AS02, Maz99a, CM00, Kle01, Ste00]). Suppose $i : A \hookrightarrow C$ is a closed immersion of abelian varieties over K . The *visible subgroup* of $H^1(K, A)$ with respect to i is

$$\text{Vis}_C H^1(K, A) = \text{Ker} (i_* : H^1(K, A) \rightarrow H^1(K, C)).$$

The visible subgroup of $\text{III}(A/K)$ relative to the embedding $A \hookrightarrow C$ is then

$$\begin{aligned} \text{Vis}_C \text{III}(A/K) &= \text{III}(A/K) \cap \text{Vis}_C H^1(K, A) \\ &= \text{Ker} (\text{III}(A/K) \rightarrow \text{III}(C/K)) \end{aligned}$$

One reason visibility is interesting is because it connects Shafarevich-Tate groups, which are mysterious subgroups of Galois cohomology, to Mordell-Weil groups of abelian varieties, i.e., it connects Conjectures 1.1 and 1.2.

More precisely, if $i : A \hookrightarrow C$ is a closed immersion, the quotient $Q = C/i(A)$ is an abelian variety, and the short exact sequence $0 \rightarrow A \rightarrow C \rightarrow Q \rightarrow 0$ gives rise to an exact sequence

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

Since the map $Q(K) \rightarrow \text{Vis}_C H^1(K, A)$ is surjective, the cohomology classes of $\text{Vis}_C H^1(K, A)$ “arise” from K -rational points for Q . This is the reason why one

calls those classes “visible”. The group $\text{Vis}_C H^1(K, A)$ is finitely generated since the Mordell-Weil group $Q(K)$ is finitely generated. Thus $\text{Vis}_C H^1(K, A)$ is finite because it is torsion.

One basic property related to visibility is that any element of $H^1(K, A)$ becomes visible in some abelian variety. More specifically, if A is an abelian variety and $c \in H^1(K, A)$, then there exists a closed immersion $i : A \hookrightarrow C$ for some abelian variety C over K , such that $c \in \text{Vis}_C H^1(K, A)$ (see [AS02, Prop. 1.3] or the appendix to this paper). The variety C is obtained as the restriction of scalars of $A_L = A \times_K L$ down to K , where L is a finite extension of K such that c has trivial image in $H^1(L, A)$. There is no canonical choice of C as we expect that there are many distinct extensions L with the above property and these extensions should give rise to nonisomorphic C . It might also happen that there exist abelian varieties C such that c is visible in C , but C does not arise via a restriction of scalars construction.

The situation with restriction of scalars is analogous to that in number fields, where an ideal I of the ring of integers \mathcal{O}_K of a field K can be trivialized in an extension. If $n > 1$ with $I^n = (\alpha)\mathcal{O}_K$ principal, then $I \cdot \mathcal{O}_L = (\sqrt[n]{\alpha})\mathcal{O}_L$ is a principal ideal in the integers of $L = K(\sqrt[n]{\alpha})$. This choice of α is only well defined up to units, so L is not canonical. In contrast, the Hilbert class field $H = H(K)$ of K is a canonical extension of K , and in H every ideal of \mathcal{O}_K becomes principal.

It would be interesting if there exists an analogue of the Hilbert class field H in the setting of abelian varieties. More precisely, for a given abelian variety A over K does there exist a “canonically defined” abelian variety $C(A)$ over K and a closed immersion $A \hookrightarrow C(A)$, such that any element of $\text{III}(A/K)$ becomes visible in $\text{III}(C(A)/K)$. One expects this last question to be at least as hard as the question about the finiteness of $\text{III}(A/K)$.

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 investigate visibility of elements of $\text{III}(A)$ in modular Jacobians of levels multiples of the conductor of A .

1.3 Organization of this Paper

In Section 2 we state our main conjectures about visibility in the context of modular abelian varieties and provide theoretical evidence for these conjectures. In Section 2.3 we state open questions about existence of points on locally trivial torsors over abelian extensions and about visibility of Kolyvagin cohomology classes.

Section 3 is devoted to the proof of the main result of the paper according to which there exists visible elements of certain prime order in the Shafarevich-Tate group under certain hypothesis which could be verified in practice using modular symbols. The result is similar to [AS02, Thm 3.1] except that it is more general because of the additional algebraic structure coming from the Hecke action on the Galois cohomology of the modular abelian variety.

In Section 4 we introduce the notion of *strong visibility* which is relevant for visualizing cohomology classes in Jacobians of modular curves whose level is a prime

times the conductor of the original abelian variety. We prove Theorem 4.3 which guarantees existence of strongly visible elements of the Shafarevich-Tate group under some hypothesis on the component group, some congruence between modular forms, and an irreducibility condition for certain Galois representation. In Section 4.3 we prove a variant of the same theorem for which the hypotheses are easier to verify in practice. At the end of the section we give computational examples for which strongly visible elements of certain order exist.

The appendix of the paper contains a new geometric proof that any cohomology class can be visualized in some abelian variety. This proof explains how visible cohomology classes arise from rational points in terms of the geometry of the restriction of scalars variety and of the torsor corresponding to the cohomology class.

Acknowledgement: Both authors had many helpful conversations with David Helm, Barry Mazur, Bjorn Poonen and Ken Ribet.

1.4 Notation

Let A be an abelian variety over a field K , and let $G_K = \text{Gal}(K^{\text{sep}}/K)$. If $\varphi : A \rightarrow B$ is an isogeny of degree n , we denote the *complementary isogeny* by φ' ; this is the isogeny such that $\varphi \circ \varphi' = \varphi' \circ \varphi = [n]$. We denote Néron models using caligraphic letters, e.g., \mathcal{A} denotes the Néron model of A .

For any non-archimedean place v of K , the *component group* of A at v is $\Phi_{A,v} = \mathcal{A}_{k_v}/\mathcal{A}_{k_v}^0$, the *Tamagawa number* of A at v is $c_{A,v} = \#\Phi_{A,v}(\mathbb{F}_v)$, and the *order of the component group* of A at v is $\bar{c}_{A,v} = \#\Phi_{A,v}(\overline{\mathbb{F}_v})$.

If M is a module over a commutative ring R and I is a subset of R , let

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

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

$$\mathbb{T}(N) = \mathbb{Z}[\dots, T_n, \dots] \subset \text{End}(J_0(N))$$

be the Hecke algebra, and note that $\mathbb{T}(N)$ also acts on $S_2(\Gamma_0(N))$ and the integral homology $H_1(X_0(N), \mathbb{Z})$. If A is an abelian subvariety of $J_0(N)$, let $\theta : A \rightarrow J_0(N) \cong J_0(N)^\vee \rightarrow A^\vee$ be the induced polarization. The *modular degree* of A is

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

(See [AS02] for why m_A is an integer.)

2 Visibility and Modular Abelian Varieties

A good source of abelian varieties over \mathbb{Q} about which much is known are the abelian varieties attached to modular forms. In this section all abelian varieties and all morphisms between abelian varieties are considered as defined over \mathbb{Q} unless otherwise stated.

Definition 2.1 (Modular Abelian Variety). A *modular abelian variety* is an abelian variety A such that for some N there is a surjective morphism $J_1(N) \rightarrow A$.

For example, all elliptic curves over \mathbb{Q} are modular (see [BCDT01]). In general, the modular abelian varieties over \mathbb{Q} are conjectured to be the abelian varieties over \mathbb{Q} of GL_2 -type (see [Rib92, §4]).

For a newform $f = \sum a_n q^n \in S_2(\Gamma_0(N))$ let $I_f = \mathrm{Ann}_{\mathbb{T}(N)}(f)$. Recall the following construction of Shimura (see [Shi94, Thm. 7.14]).

Definition 2.2 (Newform Abelian Variety). The *newform abelian variety* attached to a newform $f \in S_2(\Gamma_0(N))$ is the connected component of the intersection of the kernels of all elements of I_f , so

$$A_f = J_0(N)[I_f]^0 \subset J_0(N).$$

The abelian variety $A = A_f$ is simple over \mathbb{Q} of dimension $[\mathbb{Q}(a_2, a_3, \dots) : \mathbb{Q}]$ and $\mathbb{Z}[\dots, a_n, \dots] \subset \mathrm{End}(A/\mathbb{Q})$. Also $L(A, s) = \prod L(f_i, s)$, where the f_i are the $G_{\mathbb{Q}}$ -conjugates of f .

Remark 2.3. In this paper A_f always denotes an abelian subvariety of $J_0(N)$. Shimura [Shi73] and other authors also sometimes denote by A_f the dual of our A_f , which is a quotient of $J_0(N)$.

2.1 Conjectures

We state and give evidence for the following conjectures about modularity of the elements of the Shafarevich-Tate group.

Conjecture 2.4. *Suppose that A/\mathbb{Q} is a quotient of $J_1(N)$ and $c \in \mathrm{III}(A/\mathbb{Q})$. Then there is a modular abelian variety C and a closed immersion $i : A \hookrightarrow C$ such that $c \in \mathrm{Vis}_C \mathrm{III}(A/\mathbb{Q})$.*

Conjecture 2.5. *Suppose that A is a quotient of $J_0(N)$ and $c \in \mathrm{III}(A/\mathbb{Q})$. Then there is a positive integer M , a quotient C of $J_0(NM)$, and a closed immersion $i : A \hookrightarrow C$ such that $c \in \mathrm{Vis}_C \mathrm{III}(A/\mathbb{Q})$.*

Conjecture 2.6. *Suppose that A is an abelian subvariety $J_0(N)$ and $c \in \mathrm{III}(A/\mathbb{Q})$. Then there is a positive integer M , and a homomorphism $i : A \rightarrow C = J_0(NM)$ of finite degree coprime to the order of c such that $i_*(c) = 0$.*

Mazur first asked whether elements of $\mathrm{III}(A/\mathbb{Q})$ are visible in $J_0(N)$, where A is an elliptic curve of conductor N . Mazur and Cremona [CM00] found examples for which there are nonzero elements of $\mathrm{III}(A/\mathbb{Q})$ of odd order that are not visible in $J_0(N)$. Such examples are also known for higher dimensional modular abelian varieties (see [AS05]).

Mazur (personal communication) has argued that the group $\mathrm{Vis}_{J_0(N)}(\mathrm{III}(A/\mathbb{Q}))$ is asymptotically a small subgroup of $\mathrm{III}(A/\mathbb{Q})$, which suggests that visibility might

not be very useful when studying $\text{III}(A/\mathbb{Q})$. However, for any prime ℓ , the Jacobian $J_0(N)$ comes with two morphisms $\alpha^*, \beta^* : J_0(N) \rightarrow J_0(N\ell)$ induced from the two degeneracy maps $\alpha, \beta : X_0(\ell N) \rightarrow X_0(N)$ between the modular curves of levels ℓN and N , and it is natural to instead consider visibility of $\text{III}(A/\mathbb{Q})$ in $J_0(N\ell)$.

There is one example of visibility at higher level in the literature (see the example at end of [AS02]). In this paper we develop theoretical and computational tools and apply them to gathering evidence in support of these conjectures.

2.2 Theoretical Evidence for the Conjectures

Proposition 2.7. *If $c \in H^1(K, A)$, then c is visible in some abelian variety C .*

Proof. See [AS02, Prop. 1.3] or Theorem 5.1 for a more geometric proof. \square

Proposition 2.8. *Suppose E is an elliptic curve over \mathbb{Q} . Then Conjecture 2.5 is true for the elements of order 2 and 3 in $\text{III}(E/\mathbb{Q})$.*

Proof. We first show that there is an abelian variety C of dimension 2 and a closed immersion $i : E \hookrightarrow C$ such that $c \in \text{Vis}_C(\text{III}(E/\mathbb{Q}))$. If c has order 2, this follows from [AS02, Prop. 2.4] or [Kle01], and if c has order 3, this follows from [Maz99b, 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 . \square

Proposition 2.9. *Suppose A is a modular abelian variety over \mathbb{Q} and $c \in \text{III}(A/\mathbb{Q})$ splits over an abelian extension of \mathbb{Q} . Then Conjecture 2.4 is true for c .*

Proof. Suppose K is an abelian extension such that $\text{res}_K(c) = 0$, and let $C = \text{Res}_{K/\mathbb{Q}}(A_K)$. Then c is visible in C (see Section 5).

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

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

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

2.3 Questions For Future Investigation

Our conjectures and computations suggest the following concrete questions, which the authors intend to investigate in future work.

Question 2.10. Suppose that E is an elliptic curve and $c \in \text{III}(E/\mathbb{Q})$. Is there an abelian extension K of \mathbb{Q} such that $\text{res}_K(c) = 0$?

It is a well-known conjecture that c splits over a solvable extension; this is closely related to work of Richard Taylor on Serre’s conjecture on modularity of mod p Galois representation.

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

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

where A is an abelian variety with $L(A, s) = \prod L(f_i, s)$, where the f_i 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 investigate Question 2.10 by investigating whether or not $L(f_E, \chi, 1) = 0$, which one could do using modular symbols. The authors expect that L -functions of twists of degree $p > 2$ are very unlikely to vanish at 1, which suggests that Question 2.10 has a negative answer when the cohomology class has order bigger than 2.

It would also be interesting to prove something about visibility of Kolyvagin cohomology classes. The following is a first “test question” in this direction.

Question 2.11. Suppose $E \subset J_0(N)$ is an elliptic curve with conductor N , and fix a prime ℓ such that $\rho_{E, \ell}$ 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 $c_p \in H^1(\mathbb{Q}, E)[\ell]$ be the corresponding Kolyvagin cohomology class. There are two natural homomorphisms $\delta_1^*, \delta_p^* : E \rightarrow J_0(Np)$. When is

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

When is

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

The authors intend to investigate this and related questions in a future paper.

3 Equivariant Visibility

Let K be a number field and suppose A and B are abelian subvarieties of an abelian variety C , all defined over K , and that $C = A + B$ and $A \cap B$ is finite. Let N is an integer divisible by all primes of bad reduction for C .

Suppose ℓ is a prime such that $B[\ell] \subset A$ and that $e < \ell - 1$, where e is the largest ramification of any prime of K lying over ℓ . In this section we establish certain condition under which we obtain an injection $B(K)/\ell B(K) \hookrightarrow \text{III}(A/K)[\ell]$. The following result is [AS02, Thm. 3.1].

Theorem 3.1. *Let A, B, C, K, N , and ℓ be as above, and that*

$$\ell \nmid N \cdot \#(C/B)(K)_{\text{tor}} \cdot \#B(K)_{\text{tor}} \cdot \prod_v c_{A,v} \cdot c_{B,v}.$$

Then there is a homomorphism

$$\varphi : B(K)/\ell B(K) \rightarrow \text{Vis}_C(\text{III}(A/K))$$

such that $\dim_{\mathbb{F}_\ell} \text{Ker}(\varphi) \leq \dim_K A(K) \otimes K$.

In this section we refine the above theorem by taking into account additional algebraic structure coming from $\text{End}(C)$. The reason we need this refinement is that many of the examples in [AS05] of abelian varieties $A_f \subset J_0(N)$ for which $\text{III}(A_f)$ is not visible in $J_0(N)$ also do not satisfy some of the hypothesis of Theorem 3.1. For example, as we explain in Proposition 4.15 below, we have $\ell = 3$ for the example of level 767; unfortunately, 3 also divides $\#(C/B)(\mathbb{Q})_{\text{tor}}$ and $c_{A,13}$. This failure occurs frequently with the examples in [AS05].

Let A and B be as above. Suppose R is a commutative subring of $\text{End}(C)$, and that \mathfrak{m} be a maximal ideal of R of residue characteristic ℓ . For example, we could take $R = \mathbb{Z}$ and recover the above theorem, or if C is modular take R to be the ring generated by the Hecke operators that leave C invariant.

Theorem 3.2 (Equivariant Visibility Theorem). *Suppose A, B, C, K, N, ℓ , and \mathfrak{m} are as above, that $A(K)$ is finite as a set and that*

$$\#(C/B)(K)[\mathfrak{m}] = \#B(K)[\mathfrak{m}] = \#\Phi_{A,v}(k_v)[\mathfrak{m}] = \#\Phi_{B,v}(k_v)[\ell] = 1,$$

for all nonarchimedean places v . Then there is an injective homomorphism of R/\mathfrak{m} -vector spaces

$$(B(K)/\ell B(K))[\mathfrak{m}] \hookrightarrow \text{Vis}_C(\text{III}(A/K))[\mathfrak{m}].$$

Remark 3.3. We could probably relax the hypothesis that $A(K)$ is finite and instead give a bound on the dimension of the kernel of φ in terms of the rank of A . We will not need this stronger result in this paper.

We will prove Theorem 3.2 in Section 3.3. The proof closely follows the proof of [AS02, Thm. 3.1]. In Section 3.1 we prove a few algebraic results that we will use in the proof of Theorem 3.2.

3.1 Some Facts From Algebra

In this section we recall some very well known lemmas from commutative algebra. Let R be a commutative ring and suppose \mathfrak{m} is a finitely generated prime ideal of R .

Lemma 3.4. *If M is an R -module and $M_{\mathfrak{m}}$ is Artinian, then*

$$M_{\mathfrak{m}} \neq 0 \iff M[\mathfrak{m}] \neq 0. \tag{3.1}$$

¹Ken says: Lemma 3.4 is very well known. I wonder if you can find a reference and not have to give a proof. Did you look in Bourbaki *Algebre Commutative* I and II?

Proof. (\Leftarrow) 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 $I = \text{Ann}_R(x)$. 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 $\text{Ann}_R(x) = \mathfrak{m}$.

(\Rightarrow) 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 $I = \text{Ann}_{R_{\mathfrak{m}}}(x)$. 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 $\mathfrak{m} = (\alpha_1, \dots, \alpha_n)$ and for each α_i we get corresponding elements t_1, \dots, 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. \square

Lemma 3.5. *Suppose*

$$0 \rightarrow M_1 \rightarrow N \rightarrow M_2 \rightarrow 0 \tag{3.2}$$

is an exact sequence of R -modules each of whose localization at \mathfrak{m} is Artinian, and that \mathfrak{m} is finitely generated. Then

$$N[\mathfrak{m}] \neq 0 \iff (M_1 \oplus M_2)[\mathfrak{m}] \neq 0.$$

Proof. By Lemma 3.4 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

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

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 3.4, 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 $(M_1 \oplus M_2)[\mathfrak{m}] \neq 0$. \square

Remark 3.6. One could also prove the lemmas using the isomorphism $M[\mathfrak{m}] \cong \text{Hom}_R(R/\mathfrak{m}, M)$ and exactness properties of Hom , but even with this approach many of the details in Lemma 3.4 still have to be checked.

Remark 3.7. In the context of the proof of Theorem 3.2 below, the ring R is contained in the ring of endomorphism of an abelian variety, hence finitely generated as a \mathbb{Z} -module. Thus any ideal of R is also finitely generated as a \mathbb{Z} -module, hence finitely generated as an ideal.

2

2

Lemma 3.8. *Suppose G is a finite cyclic group, M is 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. This argument was inspired by the proof of [Ser79, Prop. VIII.4.8]. Let s be a generator for G , and let $D = s - 1$. There is an exact sequence

$$0 \rightarrow M^G \rightarrow M \xrightarrow{D} M \rightarrow M_G \rightarrow 0, \quad (3.3)$$

and each map is a homomorphism of R -modules. By [AM69, Prop. 3.3], the localization

$$0 \rightarrow (M^G)_{\mathfrak{p}} \rightarrow M_{\mathfrak{p}} \xrightarrow{D} M_{\mathfrak{p}} \rightarrow (M_G)_{\mathfrak{p}} \rightarrow 0$$

of (3.3) is exact. By hypothesis $H^0(G, M)[\mathfrak{p}] = 0$, and by definition $M^G = H^0(G, M)$, so by Lemma 3.4, $(M^G)_{\mathfrak{p}} = 0$, and the following sequence is exact:

$$0 \rightarrow M_{\mathfrak{p}} \xrightarrow{D} M_{\mathfrak{p}} \rightarrow (M_G)_{\mathfrak{p}} \rightarrow 0.$$

But $D : M_{\mathfrak{p}} \rightarrow M_{\mathfrak{p}}$ is an injective map of finite sets, so it is a bijection, hence $(M_G)_{\mathfrak{p}} = 0$. Again using Lemma 3.4 it follows that $M_G[\mathfrak{p}] = 0$.

It follows from [Ser79, Ch. VIII, §4] that

$$H^1(G, M) \cong M[N]/DM \quad (\text{as functors in } M),$$

where $M[N]$ is the kernel of the map $M \xrightarrow{N} M$, and $N = \sum_{g \in G} g$. Since $M_G = M/DM$, we have an R -module inclusion $H^1(G, M) \hookrightarrow M_G$. We showed above that $M_G[\mathfrak{p}] = 0$, so the lemma follows. \square

Remark 3.9. If \mathfrak{p} were replaced by a prime number $p \in \mathbb{Z}$ then the result would be immediate since using Herbrand quotients one shows that $\#H^0(G, M) = \#H^1(G, M)$ (see [Ser79, Prop. VIII.4.8]). It is unclear to the authors if the result is true in general, i.e., if G is replaced by an arbitrary group.

²Ribet's remark about this lemma: I find Lemma 3.10 very strangely stated. Why not say simply that a certain group is divisible by every integer n prime to the residue characteristic; the group might be denoted $A^0(K)$. I imagine that this lemma is in SGA 7I Expose IX (by Grothendieck). Is it really true that x can be divided by n only in $A(K)$ (and not in $A^0(K)$)?

3.2 A Lemma About Divisible Points

The following lemma will be necessary for proving that certain cohomology classes are locally trivial. For proofs of this result, see [AS02, §3.2].

Lemma 3.10. *Let A be an abelian variety over the fraction field K of a strictly Henselian discrete valuation ring R (e.g. the maximal unramified extension of local field). Let n be an integer coprime to the residue characteristic of K . Let $x \in A(K)$ be a point whose reduction lands in the identity component of the closed fiber of the Néron model of A . Then $x \in nA(K)$.*

3.3 Proof of Theorem 3.2

Let Q be the quotient C/A which is an abelian variety over K . The construction of the map is similar to the one in the proof of Lemma 3.6 of [AS02]. One has the following commutative diagram

$$\begin{array}{ccccccc}
 0 & \longrightarrow & B[\ell] & \longrightarrow & B & \xrightarrow{[\ell]} & B & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & \searrow \psi & \downarrow \pi & & \\
 0 & \longrightarrow & A & \longrightarrow & C & \longrightarrow & Q & \longrightarrow & 0
 \end{array}$$

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

$$\begin{array}{ccccccc}
 & & M_0 & & M_1 & & M_2 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & B(K)/(B(K)[\ell]) & \xrightarrow{[\ell]} & B(K) & \longrightarrow & B(K)/\ell B(K) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & \searrow \pi & \downarrow \varphi & & \\
 0 & \longrightarrow & C(K)/A(K) & \longrightarrow & Q(K) & \longrightarrow & \text{Vis}_C(H^1(K, A)) & \longrightarrow & 0 \\
 & & \downarrow & & & & & & \\
 & & M_3 & & & & & &
 \end{array}$$

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

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

By hypothesis, $B(K)[\mathfrak{m}] = 0$, so $N_0 = \text{Ker}(B(K) \rightarrow C(K)/A(K))$ 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 3.5. 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 $(C/B)(K)$ and by hypothesis $(C/B)(K)[\mathfrak{m}] = 0$, so $(C(K)/B(K))[\mathfrak{m}] = 0$. Since C/B is isogenous to A and $A(K)$ is finite and $C(K)/B(K) \hookrightarrow (C/B)(K)$, 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 3.5 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

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

and both of M_1/M_0 and M_3 have trivial \mathfrak{m} -torsion. It follows by Lemma 3.5, that $M_2[\mathfrak{m}] = 0$. Therefore, we have an injective morphism of R/\mathfrak{m} -vector spaces

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

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

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

$$H^1(K_v^{\text{ur}}/K_v, A(K_v^{\text{ur}})) \cong H^1(\bar{k}_v/k_v, \Phi_{A,v}(\bar{k}_v)). \quad (3.4)$$

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 $\text{Vis}_C(\text{III}(A/K))[\mathfrak{m}]$. Let d denote the image of c in $H^1(\bar{k}_v/k_v, \Phi_{A,v}(\bar{k}_v))$. 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 (3.4) is induced from the exact sequence of $\text{Gal}(K_v^{\text{ur}}/K_v)$ -modules

$$0 \rightarrow \mathcal{A}^0(K_v^{\text{ur}}) \rightarrow \mathcal{A}(K_v^{\text{ur}}) \rightarrow \Phi_{A,v}(\bar{k}_v) \rightarrow 0,$$

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 $\varphi(x) \in H^1(K, A)[\mathfrak{m}]$, it follows that

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

Lemma 3.8, our hypothesis that $\Phi_{A,v}(k_v)[\mathfrak{m}] = 0$, and that

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

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

4 Strong Visibility at Higher Level

In this section we introduce a specific notion of visibility at higher level.

Suppose $A \subset J_0(N)$ is an abelian subvariety and $p \nmid N$ is a prime. Let

$$\varphi = \delta_1^* + \delta_p^* : J_0(N) \rightarrow J_0(pN) \quad (4.1)$$

be the homomorphism obtained by summing the two degeneracy maps. Let $H^1(\mathbb{Q}, A)'$ be the subgroup of $H^1(\mathbb{Q}, A)$ of elements of odd order.

Definition 4.1 (Strongly Visibility). Then the subgroup of $H^1(\mathbb{Q}, A)$ that is *strongly visible in $J_0(pN)$* is

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

Also,

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

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

Remark 4.2. In Definition 4.1 we could in addition consider $\delta_1^* - \delta_p^*$. This would allow for the possibility of more visible elements. Since the methods of this paper do not apply for this map, we will not consider it further.

For a positive integer N , let

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

Theorem 4.3. *Suppose $A = A_f \subset J_0(N)$ is a newform abelian variety with $L(A, 1) \neq 0$, that $p \nmid N$ is a prime, and that there is a maximal ideal $\lambda \subset \mathbb{T}(N)$ and an elliptic curve E over \mathbb{Q} of conductor pN such that the following properties are satisfied:*

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

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

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 . We have $a_p(E) = -1$,*

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

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

4. [Irreducibility] The mod ℓ representation $\rho_{E,\ell}$ is irreducible.

Then there is an injective homomorphism

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

Remark 4.4. In fact, we have

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

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

4.1 Some Lemmas

We will use the following lemmas in the proof of Theorem 4.3. The notation is as in the previous section.

Lemma 4.5. 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 $\ell \nmid 2pN$ of the ring \mathcal{O} generated by the Fourier coefficients of f and g such that for $q \leq \nu(pN)$,

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

Assume that $a_p(g) = -1$. Let $\lambda_f = i_f^{-1}(\lambda)$ and $\lambda_g = i_g^{-1}(\lambda)$, where

$$i_f : \mathbb{Z}[\dots, a_n(f), \dots] \hookrightarrow \mathcal{O}$$

and likewise for i_g . 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 $J_0(pN)$.

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

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

By [Rib90b, Lem. 1], the operator $U_p = T_p$ on $J_0(pN)$ acts as -1 on $\varphi(A_f[\lambda_f])$. With respect to the basis $f(q)$, $f(q^p)$, the matrix of U_p is

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

Thus neither $f(q)$ nor $f(q^p)$ 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

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

Thus we can choose $\alpha \in \overline{\mathbb{Z}}$ such that

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

is an eigenvector of U_p with eigenvalue congruent to -1 modulo λ . (It doesn't matter 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 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, the 2-dimensional $G_{\mathbb{Q}}$ -representations $\varphi(A_f[\lambda_f])$ and $A_g[\lambda_g]$ are isomorphic. If \mathfrak{m} is the annihilator in $\mathbb{T}(pN)$ of $A_g[\lambda_g]$, then multiplicity one [Edi92, Thm 9.2] implies that $A_g[\lambda_g]$ occurs with multiplicity one in $J_0(pN)$. Thus

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

This completes the proof. (Note: One could avoid the use of Brauer-Nesbitt above.) \square

Remark 4.6. The bounds in [Stu87] are sometimes much better than $\nu(pN)$ when comparing eigenforms (see also [BS02]). In the proof of Lemma 4.5 we are comparing eigenforms, so these better bounds apply. They are more complicated to state so we do not include them here. ³

3

Lemma 4.7. *Suppose $\varphi : A \rightarrow B$ and $\psi : B \hookrightarrow C$ are homomorphisms of abelian varieties over a number field, with φ an isogeny and ψ injective. Suppose n is an integer that is relatively prime to the degree of φ . If $G = \text{Vis}_C(\text{III}(B))[n^\infty]$, then there is some injective homomorphism*

$$f : G \hookrightarrow \text{Ker}((\psi \circ \varphi)_* : \text{III}(A) \rightarrow \text{III}(C)),$$

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

Proof. Let m be the degree of the isogeny $\varphi : A \rightarrow B$. Consider the complementary isogeny $\varphi' : B \rightarrow A$, 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 $G \subset \text{III}(B)$, which in turn maps to 0 in $\text{III}(C)$. \square

³Should we just state them? Ribet says so.

Lemma 4.8. *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 $M = 2$.) \square

Lemma 4.9. *Suppose λ is a maximal ideal of $\mathbb{T}(N)$ with generators ℓ and $T_n - a_n$, 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 $T_n - a_n$ with $p \nmid n$. 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 4.8, $R = \mathbb{T}(N)$, so $\mathbb{T}(N)/\lambda_p = \mathbb{F}_\ell$, hence λ_p is a maximal ideal. \square

Lemma 4.10. *Suppose that A is an abelian variety over a field K . Let R be a commutative subring of $\text{End}(A)$ and λ an ideal of R . Then*

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

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

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

$$\varphi : (A/A[\lambda])[\lambda] \rightarrow A[\lambda^2]/A[\lambda].$$

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

4.2 Proof of Theorem 4.3

By [BCDT01] E is modular, so there is an elliptic curve $B \subset J_0(pN)$ attached to a newform of level pN , and an isogeny $E \rightarrow B$ defined over \mathbb{Q} , which by Hypothesis 4 can be chosen to have degree coprime to ℓ . (Every cyclic rational isogeny is a composition of rational isogenies of prime degree, and E admits no rational ℓ -isogeny since $\rho_{E,\ell}$ is irreducible.)

By Hypothesis 1, the Tamagawa numbers of E are coprime to ℓ , so since E and B are related by an isogeny of degree coprime to ℓ , the Tamagawa numbers of B are also not divisible by ℓ . Note also that $E(\mathbb{Q}) \otimes \mathbb{F}_\ell \cong B(\mathbb{Q}) \otimes \mathbb{F}_\ell$.

Let \mathfrak{m} be the ideal of $\mathbb{T}(pN)$ generated by ℓ and $T_n - a_n(E)$ for all integer n coprime to p .

Let φ be as in (4.1), and let $A = \varphi(A_f)$. Note that if $T_n \in \mathbb{T}(pN)$ then $T_n(B) \subset B$ since B 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. Proposition 4.5 implies that

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

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

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

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

Suppose for the moment that we have verified that the hypothesis of Theorem 3.2 are satisfied with A , B , C , and R as above and $K = \mathbb{Q}$. Then we obtain an injective homomorphism

$$E(\mathbb{Q})/\ell E(\mathbb{Q}) \cong B(\mathbb{Q})/\ell B(\mathbb{Q}) \hookrightarrow \text{Ker}(\text{III}(A) \rightarrow \text{III}(C))[\mathfrak{m}].$$

We then apply Lemma 4.7 with $n = \ell$, A_f , A , and C , respectively, to see that

$$B(\mathbb{Q})/\ell B(\mathbb{Q}) \subset \text{Ker}(\text{III}(A_f) \rightarrow \text{III}(C))[\lambda].$$

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

Finally, consider $A \times B \rightarrow J_0(pN)$ 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

$$\text{III}(A_f) \rightarrow \text{III}(C) \rightarrow \text{III}(J_0(pN)),$$

hence inclusions

$$B(\mathbb{Q})/\ell B(\mathbb{Q}) \subset \text{Ker}(\text{III}(A_f) \rightarrow \text{III}(C)) \subset \text{Ker}(\text{III}(A_f) \rightarrow \text{III}(J_0(pN))),$$

which gives the conclusion of the theorem.

It remains to verify the hypotheses of Theorem 3.2. That $C = A + B$ is clear from the definition of C . Also, $A \cap B = B[\ell]$, which is finite. We explained above when defining R that each of A and B 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 A_f has rank 0 (by [KL89]).

It remains is to verify that

$$(C/B)(\mathbb{Q})[\mathfrak{m}] = B(\mathbb{Q})[\mathfrak{m}] = \Psi_{A,q}(\mathbb{F}_q)[\mathfrak{m}] = \Psi_{B,q}(\mathbb{F}_q)[\ell] = 0,$$

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

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

We will now verify that $(C/B)(\mathbb{Q})[\mathfrak{m}] = 0$. From the definition of C and Ψ we have $C/B \cong A/\Psi$. Let λ_p be as in Lemma 4.9 with $a_n = a_n(E)$. The map φ induces an isogeny of 2-power degree

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

Thus there is λ_p -torsion in $(A_f/(A_f[\lambda]))(\mathbb{Q})$ if and only if there is \mathfrak{m} -torsion in $(A/\Psi)(\mathbb{Q})$. (Note that λ_p and \mathfrak{m} are both ideals generated by ℓ and $T_n - a_n$ for all n coprime to p , but for λ_p the $T_n \in \mathbb{T}(N)$, and for \mathfrak{m} they are in $\mathbb{T}(pN)$.) Thus it suffices to prove that $(A_f/A_f[\lambda])(\mathbb{Q})[\lambda_p] = 0$.

By Lemma 4.9, we have $\lambda_p = \lambda$, and by Lemma 4.10,

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

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 $\Psi_{A_f,q}(\mathbb{F}_q)[\lambda] = 0$ for each prime divisor $q \mid N$, so $\Psi_{A_f,q}(\mathbb{F}_q)[\mathfrak{m}] = 0$. 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 on $\Psi_{B,p}(\overline{\mathbb{F}}_p)$ acts as -1 . Thus $\Psi_{B,p}(\mathbb{F}_p)[\ell] = 0$ since ℓ is odd. This completes the proof.

4.3 A Variant of Theorem 4.3 with Simpler Hypothesis

Proposition 4.11. *Suppose $A = A_f \subset J_0(N)$ is a newform abelian variety and $q \parallel N$ 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 [Rib19], so

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

By Lemma 3.5, 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 3.5 implies that $\Phi_{A^\vee,q}(\overline{\mathbb{F}}_q)[\mathfrak{m}] = 0$. Finally, the modular polarization $A \rightarrow A^\vee$ has degree coprime to ℓ , so the induced map $\Phi_{A,q}(\overline{\mathbb{F}}_q) \rightarrow \Phi_{A^\vee,q}(\overline{\mathbb{F}}_q)$ 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 $\bar{c}_p = \text{ord}_p(\Delta)$.

Theorem 4.12. *Suppose $A = A_f \subset J_0(N)$ is a newform abelian variety with $L(A, 1) \neq 0$ 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 algebraic rank of E is positive.
2. [Divisibility] We have $\ell \mid \bar{c}_{E,p}$ but $\ell \nmid 2 \cdot N \cdot p \cdot m_A \cdot c_{E,p} \cdot \prod_{q|N} \bar{c}_{E,q}$.
3. [Irreducibility] The mod ℓ representation $\bar{\rho}_{E,\ell}$ is irreducible.
4. [Noncongruence] The representation $\bar{\rho}_{E,\ell}$ is not isomorphic to any representation $\bar{\rho}_{g,\lambda}$ 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 $\text{III}(A_f)$ that is not visible in $J_0(N)$ but is strongly visible in $J_0(pN)$. More precisely, there is an inclusion

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

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

Proof. The divisibility assumptions of Hypothesis 2 on the $\bar{c}_{E,q}$ imply that the Serre level of $\rho_{E,\ell}$ is N and since $\ell \nmid N$, the Serre weight is 2 (see [RS01, Thm. 2.10]). We have $\bar{c}_{E,p} \neq c_{E,p}$ since one is divisible by ℓ and the other is not, so E has nonsplit multiplicative reduction, hence $a_p(E) = -1$. Since ℓ is odd, Ribet's level optimization 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 , and by adjusting λ we may assume $h = f$. 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 4.11 implies that $\Phi_{A,q}(\overline{\mathbb{F}}_q)[\lambda] = 0$ for each $q \mid N$.

The theorem now follows from Theorem 4.3. \square

Remark 4.13. The non-congruence hypothesis of Theorem 4.12 can be verified using modular symbols as follows. Let $W \subset H_1(X_0(N), \mathbb{Z})_{\text{new}}$ 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.

4.4 Examples

In this section we give examples that illustrate Theorem 4.12.

Hypothesis 4.14. *The statements in this section all make the hypothesis that certain MAGMA [BCP97] commands gave correct output when we used them.*

4.4.1 Level 767

Consider the modular Jacobian $J_0(767)$. We exhibit elements of the Shafarevich-Tate group of a newform subvariety of that Jacobian which are invisible, but can be visualized in a Jacobian of higher level.

We use MAGMA to decompose $J_0(767)$ into a product of its optimal newform quotients. The duals of those optimal quotients are subvarieties of $J_0(767)$. There are six subvarieties $A_2, A_3, A_4, A_{10}, A_{17}$ and A_{23} of dimensions 2, 3, 4, 10, 17 and 23, respectively. Consider the subvariety A_{23} of highest dimension. We first compute a divisor of the conjectural order of III for the subvariety A_{23} and the quotient A_{23}^\vee .

Proposition 4.15. *Assume Conjecture 1.2. We have*

$$3^2 \mid \#\text{III}(A_{23}) \quad \text{and} \quad 3^2 \mid \#\text{III}(A_{23}^\vee).$$

Proof. Let $A = A_{23}^\vee$ be the 23-dimensional newform optimal quotient of $J_0(767)$. We break the proof into the following steps:

1. *Compute a divisor and a multiple of the order of $A(\mathbb{Q})_{\text{tor}}$ and $A^\vee(\mathbb{Q})_{\text{tor}}$.*

To compute a multiple of the order of the torsion subgroup of $A(\mathbb{Q})_{\text{tor}}$ we use the algorithms from [AS05, §3.5 and §3.6] (see also [Kat81]), which are implemented in MAGMA. The upper bound 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. Since this bound is an isogeny invariant, one gets the same upper bound for $A^\vee(\mathbb{Q})_{\text{tor}}$. For producing a divisor, one uses the injection of the subgroup of rational cuspidal divisor classes of degree 0 into $A(\mathbb{Q})_{\text{tor}}$. In this particular case, we obtain

$$120 \mid \#A(\mathbb{Q})_{\text{tor}} \mid 240.$$

To get a divisor for the dual variety A^\vee , we compute the *modular degree* (i.e. the positive square root of the degree of the isogeny $A \rightarrow A^\vee$) by using the algorithm described in [AS05, §3.3]. The modular degree is 2^{34} and is not divisible by any odd primes, so $\#A^\vee(\mathbb{Q})_{\text{tor}}$ is divisible by 15. Therefore,

$$15 \mid \#A^\vee(\mathbb{Q})_{\text{tor}} \mid 240.$$

Alternatively, we can compute $A^\vee(\mathbb{Q}) \cap C$, where C is the subgroup of $J_0(767)$ generated by differences of rational cusps. This group is of order 15.

2. *Compute the L -ratio.*

We compute using the algorithm from [AS05, §4] the L -ratio

$$\frac{L(A, 1)}{\Omega_A} = c_A \cdot \frac{2^9 \cdot 3^1}{5},$$

where $c_A \in \mathbb{Z}$ is the Manin constant. Since $c_A \mid 2^{\dim(A)}$ by [ARS05] then

$$\frac{L(A, 1)}{\Omega_A} = \frac{2^{n+2} \cdot 3^2}{5},$$

for some $0 \leq n \leq 23$.

3. *Compute the Tamagawa numbers.*

Using the algorithms from [CS01, KS00] we compute the Tamagawa number

$$c_{A_{23},13} = 1920 = 2^3 \cdot 3 \cdot 5.$$

We also have that

$$2 \mid c_{A_{23},59} \mid 4.$$

Note that $c_{A_{23},59}$ is a power of 2 follows because W_{23} acts as 1 on A_{23} , and on the component group $\text{Frob} = -W_{23}$, so the fixed subgroup $\Phi_{A_{23},59}(\mathbb{F}_{59})$ of Frobenius is a 2-torsion group (for more details, see [Rib90a, Prop.3.7–8]).

4. *Compute a divisor of the conjectural order of $\text{III}(A^\vee/\mathbb{Q})$.*

Conjecture 1.2 asserts that

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

By substituting the results from the above steps, we obtain that $3^2 \mid \#\text{III}(A/\mathbb{Q})$. Since the L -function of A does not vanish at 0, [KL89] implies that $\text{III}(A/\mathbb{Q})$ is finite, so the properties of the Cassels-Tate pairing imply that $\#\text{III}(A/\mathbb{Q}) = \#\text{III}(A^\vee/\mathbb{Q})$. Thus, if the BSD conjecture is true, it must also predict that $3^2 \mid \#\text{III}(A^\vee/\mathbb{Q})$.

□

Lemma 4.16. *The modular degree of A_{24} is 2^{34} , so any element of $\text{III}(A_{23}/\mathbb{Q})$ that is visible in $J_0(767)$ has order a power of 2.*

Proof. Using MAGMA we find that the modular degree of A_{23} is 2^{34} . By [AS05, Prop. 3.15], any element of $\text{III}(A_{23}/\mathbb{Q})$ that is visible in $J_0(767)$ has order a power of 2. □

Proposition 4.17. *There is an element of order 3 in $\text{III}(A_{23}/\mathbb{Q})$ which is not visible in $J_0(767)$ but is strongly visible in $J_0(2 \cdot 767)$. (This proposition does not assume Conjecture 1.2.)*

Proof. Let $A = A_{23}$, and note that A has rank 0, since $L(A, 1) \neq 0$. Using MAGMA or [Cre] we find that the elliptic curve

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

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

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

We apply Theorem 4.12 with $\ell = 3$ and $p = 2$. Since E has no rational 3-isogenies (which we see using the modular polynomial $\Phi_3(X, Y)$ or Cremona's `allisog`),

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 that

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

which verifies the noncongruence hypothesis, and completes the proof. \square

4.4.2 Level 959

We do similar computations for a 24-dimensional abelian variety in $J_0(959)$. 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 4.18. *There is an element of order 3 in $\text{III}(A_f/\mathbb{Q})$ which is not visible in $J_0(959)$ but is strongly visible in $J_0(2 \cdot 959)$.*

Proof. Using MAGMA we find that the modular degree of A is $2^{32} \cdot 583673$, which is coprime to 3. Thus we apply Theorem 4.12 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

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

Using `allisog` we find that E has no rational 3-isogeny. The modular form attached to E is

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

and we have

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

which completes the verification. \square

4.5 Table of Strong Visibility at Higher Level

The following is a table that gives the known examples of A_f with square free conductor ≤ 1339 such that Conjecture 1.2 predicts an odd prime divisor ℓ of $\text{III}(A_f)$, 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 4.12, hence there really is a nonzero element in $\text{III}(A_f)$ 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 4.12, E is an elliptic curve, denoted using a Cremona label, and $q \neq p$ is a prime such that

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

A_f	dim	$\ell \mid \text{III}(A_f)?$	moddeg	(p, E, q) 's
551H	18	3	$2^7 \cdot 13^2$	(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)

5 Appendix: Geometric Proof of Visibility Somewhere

In this section, we give a proof that each element of $\text{III}(A/K)$ can be visualized somewhere.

Theorem 5.1. *Let $c \in H^1(K, A)$ be any cohomology class. Then there exists an abelian variety J and a closed immersion $i : A \hookrightarrow J$, such that $c \in \text{Vis}_J H^1(K, A)$.*

Proof. Choosing a finite extension L/K such that $\text{res}_{L/K}(c) = 0$, where $\text{res}_{L/K} : H^1(K, A) \rightarrow H^1(L, A)$ is the restriction map on Galois cohomology.

Let C/K be a principal homogeneous space (a torsor) for A/K , such that the class $[C] \in WC(A/K)$ corresponds to the element $c \in H^1(K, A)$. Let $A \times C \rightarrow C$ be the simple, transitive action of A on C . Let $P \in C(L)$ be the L -rational point. Define a morphism $\varphi : A_L \rightarrow C_L$ by $\varphi(a) = a \oplus P$. Since A acts simply transitively on C , then φ is an isomorphism. Let $\psi = \varphi^{-1}$.

The first important step of the proof is to recover the group law on A_L in terms of the morphisms φ and ψ . The main idea for proving this is to use rigidity theorem for abelian varieties. Define a morphism

$$\phi : A_L \times A_L \rightarrow A_L$$

by $\phi(a, a') = \psi(a \oplus \varphi(a'))$. We compute $\phi(a, 0) = \psi(a \oplus P) = a$. Also, $\phi(0, a) = \psi(0 \oplus \varphi(a)) = \psi(a \oplus P) = a$. Therefore, if $\mu_L : A_L \times A_L \rightarrow A_L$ is the multiplication map, then $\phi - \mu_L$ satisfies the hypothesis for the rigidity theorem, therefore $\phi = \mu_L$.

Let $J = \text{Res}_{L/K}(A_L)$. The isomorphism $\psi : C_L \rightarrow A_L$ induces an inclusion $C(K) \hookrightarrow C(L) \cong A_L(L) \cong J(K)$ and the identity morphism $\text{id} : A_L \rightarrow A_L$ induces an inclusion $A(K) \hookrightarrow A_L(L) \cong J(K)$. These inclusions correspond via Yoneda's lemma to injective morphisms $A \rightarrow J$ and $C \rightarrow J$. Since these morphisms are proper, then [Gro66, §8.11.5] implies that they are closed immersions.

Since A is defined over K , we may view J_L as a product of n copies of A_L , i.e.

$$J_L \cong \prod_{i=1}^n A_L.$$

The closed immersion $C \hookrightarrow J$ base extended to L gives a morphism $C_L \rightarrow J_L$. This morphism is the map, sending

$$x \mapsto (\psi_1(x), \psi_2(x), \dots, \psi_n(x)),$$

where $\psi_i : C_L \rightarrow A_L$ are the conjugates of $\psi : C_L \rightarrow A_L$, obtained by applying the n different embedding $L \hookrightarrow \overline{K}$ to ψ , which fix the field K . Note that each of the ψ_i 's is a morphism $C_L \rightarrow A_L$, since both C and A are defined over K .

We claim that the image of C_L inside J_L is a translate of A_L . The morphism $A_L \hookrightarrow J_L \cong \prod_{i=1}^n A_L$ is precisely the diagonal embedding. To determine the image of C_L , we consider the morphism

$$A_L \xrightarrow{\phi} C_L \rightarrow \prod_{i=1}^n A_L,$$

which maps $a \mapsto (\psi_1(\varphi(a)), \psi_2(\varphi(a)), \dots, \psi_n(\varphi(a)))$. The image of $a \in A_L(\overline{K})$ is the unique b , such that $b \oplus \sigma_i(P) = a \oplus P$. But the action is transitive, so we get $(-b + a) \oplus P = \sigma_i(P)$, which means that $b = a - \psi(\sigma_i(P))$. This shows that the image of C_L in J_L is a translate of A_L by $(-\psi(\sigma_1(P)), -\psi(\sigma_2(P)), \dots, -\psi(\sigma_n(P)))$, so we are done. This point then gives us the visible element of $H^1(K, A)$. \square

References

- [Aga99] Amod Agashé, *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
- [AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR 39 #4129
- [ARS05] A. Agashe, K. A. Ribet, and W. A. Stein, *The Manin Constant, Congruence Primes, and the Modular Degree*, Preprint, <http://modular.fas.harvard.edu/papers/manin-agashe/> (2005).
- [AS02] A. Agashe and W. A. Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185. MR 2003h:11070
- [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. MR 2085902
- [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). MR 2002d:11058

- [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
- [BS02] K. Buzzard and W. A. Stein, *A mod five approach to modularity of icosahedral Galois representations*, Pacific J. Math. **203** (2002), no. 2, 265–282. MR 2003c:11052
- [CM00] 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
- [Cre] J. E. Cremona, *Tables of Elliptic Curves*, <http://www.maths.nott.ac.uk/personal/jec/ftp/data/>.
- [CS01] B. Conrad and W. A. Stein, *Component groups of purely toric quotients*, Math. Res. Lett. **8** (2001), no. 5-6, 745–766. MR 2003f:11087
- [CV92] R. F. Coleman and J. F. Voloch, *Companion forms and Kodaira-Spencer theory*, Invent. Math. **110** (1992), no. 2, 263–281.
- [Edi92] B. Edixhoven, *The weight in Serre’s conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594.
- [Gro66] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III*, Inst. Hautes Études Sci. Publ. Math. (1966), no. 28, 255. MR 36 #178
- [Gro91] B. H. Gross, *Kolyvagin’s work on modular elliptic curves, L-functions and arithmetic* (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.
- [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.
- [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 $J_0(N)$* , Proceedings of the 4th International Symposium (ANTS-IV), Leiden, Netherlands, July 2–7, 2000 (Berlin), Springer, 2000.
- [Lan91] S. Lang, *Number theory. III*, Springer-Verlag, Berlin, 1991, Diophantine geometry. MR 93a:11048

- [Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).
- [Maz99a] ———, *Visualizing elements of order three in the Shafarevich-Tate group*, Asian J. Math. **3** (1999), no. 1, 221–232. MR 2000g:11048
- [Maz99b] ———, *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. MR 2000g:11048
- [Mil72] J.S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190. MR 48 #8512
- [Mil86] ———, *Arithmetic duality theorems*, Academic Press Inc., Boston, Mass., 1986.
- [Rib19] Kenneth A. Ribet, *On the component groups and the Shimura subgroup of $J_0(N)$* , Séminaire de Théorie des Nombres, 1987–1988 (Talence, 1987–1988), Univ. Bordeaux I, Talence, 19??. pp. Exp. No. 6, 10. MR MR993107 (91b:11070)
- [Rib83] ———, *Congruence relations between modular forms*, Proc. International Congress of Mathematicians (1983), 503–514.
- [Rib90a] K. A. Ribet, *On modular representations of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ 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. MR 94g:11042
- [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., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 143–232. MR 2002h:11047
- [Rub89] K. Rubin, *The work of Kolyvagin on the arithmetic of elliptic curves*, Arithmetic of complex manifolds (Erlangen, 1988), Springer, Berlin, 1989, pp. 128–136.
- [Ser79] J-P. Serre, *Local fields*, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

- [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.
- [Shi94] ———, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.
- [Ste00] W. A. Stein, *Explicit approaches to modular abelian varieties*, Ph.D. thesis, University of California, Berkeley (2000).
- [Ste04] ———, *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, pp. 275–280.
- [Wil95] A. J. Wiles, *Modular elliptic curves and Fermat’s last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.