Visibility of Shafarevich-Tate Groups of Abelian Varieties

Amod Agashe
University of Texas
Austin, TX
agashe@math.utexas.edu

and

William Stein
Harvard University
Cambridge, MA
was@math.harvard.edu

Version: February 27, 2002

We investigate Mazur's notion of visibility of elements of Shafarevich-Tate groups of abelian varieties. We give a proof that every cohomology class is visible in a suitable abelian variety, discuss the visibility dimension, and describe a construction of visible elements of certain Shafarevich-Tate groups. This construction can be used to give some of the first evidence for the Birch and Swinnerton-Dyer Conjecture for abelian varieties of large dimension. We then give examples of visible and invisible Shafarevich-Tate groups.

Key Words: Visibility, Shafarevich-Tate Group, Birch and Swinnerton-Dyer Conjecture, Modular Abelian Variety

INTRODUCTION

If a genus 0 curve X over $\mathbf{Q}$ has a point in every local field $\mathbf{Q}_p$ and in $\mathbf{R}$, then it has a global point over $\mathbf{Q}$. For genus 1 curves, this "local-to-global principle" frequently fails. For example, the nonsingular projective curve defined by the equation $3x^3 + 4y^3 + 5z^3 = 0$ has a point over each local field and $\mathbf{R}$, but has no $\mathbf{Q}$-point. The Shafarevich-Tate group of an elliptic curve E, denoted $Ш(E)$, is a group that measures the extent to which a local-to-global principle fails for the genus one curves with Jacobian E. More generally, if A is an abelian variety over a number field K, then the elements of the Shafarevich-Tate group $Ш(A)$ of A correspond to the torsors for A that have a point everywhere locally, but not globally. In this paper, we study a geometric way of realizing (or "visualizing") torsors corresponding to elements of $Ш(A)$.

Let A be an abelian variety over a field K. If $\iota : A \hookrightarrow J$ is a closed immersion of abelian varieties, then the subgroup of $H^1(K, A)$ *visible in* J (with respect to ι) is $\ker(H^1(K, A) \to H^1(K, J))$. We prove that every element of $H^1(K, A)$ is visible in some abelian variety, and give bounds on the smallest size of an abelian variety in which an element of $H^1(K, A)$ is visible. Next assume that K is a number field. We give a construction of visible elements of $Ш(A)$, which we demonstrate by giving evidence for the Birch and Swinnerton-Dyer conjecture for a certain 20-dimensional abelian variety. We also give an example of an elliptic curve E over $\mathbf{Q}$ of conductor N whose Shafarevich-Tate group is not visible in $J_0(N)$ but is visible in $J_0(Np)$ for some prime p.

This paper is organized as follows. Section 1 contains the definition of visibility for cohomology classes and elements of Shafarevich-Tate groups. Then in Section 1.3, we use a restriction of scalars construction to prove that every cohomology class is visible in some abelian variety. Next, in Section 2, we investigate the visibility dimension of cohomology classes. Section 3 contains a theorem that can be used to construct visible elements of Shafarevich-Tate groups. The final section, Section 4, contains examples and applications of our visibility results in the context of modular abelian varieties.

ACKNOWLEDGMENTS

We thank Barry Mazur for his generous guidance, Brian Conrad for his extensive assistance, Ralph Greenberg for suggesting the use of restriction of scalars in Section 1.3, Fabrizio Andreatta for suggesting that a semistability hypothesis was unnecessary in Theorem 3.1, and Loic Merel, Bjorn Poonen, and Ken Ribet for helpful conversations. The first author would like to thank the Mathematical Sciences Research Institute in Berkeley and the Institut des Hautes Études Scientifiques in France, and the second author the Max Planck Institute in Bonn, for their generous hospitality.

1. VISIBILITY

In Section 1.1 we introduce visible cohomology classes, then in Section 1.2 we discuss visible elements of Shafarevich-Tate groups. In Section 1.3, we use restriction of scalars to deduce that every cohomology class is visible somewhere.

For a field K and a smooth commutative K-group scheme G, we write $H^i(K, G)$ to denote the group cohomology $H^i(\mathrm{Gal}(K_s/K), G(K_s))$ where K_s is a fixed separable closure of K; equivalently, $H^i(K, G)$ denotes the ith étale cohomology of G viewed as an étale sheaf on $\mathrm{Spec}(K)_{\text{ét}}$.

1.1. Visible Elements of $H^1(K, A)$

In [Maz99], Mazur introduced the following definition. Let A be an abelian variety over an arbitrary field K.

DEFINITION 1.1. Let $\iota : A \hookrightarrow J$ be an embedding of A into an abelian variety J over K. Then the *visible subgroup of $H^1(K, A)$ with respect to the embedding ι* is

$$\mathrm{Vis}_J(H^1(K, A)) = \mathrm{Ker}(H^1(K, A) \to H^1(K, J)).$$

The visible subgroup $\mathrm{Vis}_J(H^1(K, A))$ depends on the choice of embedding ι, but we do not include ι in the notation, as it is usually clear from context.

The Galois cohomology group $H^1(K, A)$ has a geometric interpretation as the group of classes of torsors X for A (see [LT58]). To a cohomology class $c \in H^1(K, A)$, there is a corresponding variety X over K and a map $A \times X \to X$ that satisfies axioms similar to those for a simply transitive group action. The set of equivalence classes of such X forms a group, the Weil-Chatelet group of A, which is canonically isomorphic to $H^1(K, A)$.

There is a close relationship between visibility and the geometric interpretation of Galois cohomology. Suppose $\iota : A \to J$ is an embedding and $c \in \mathrm{Vis}_J(H^1(K, A))$. We have an exact sequence of abelian varieties $0 \to A \to J \to C \to 0$, where $C = J/A$. A piece of the associated long exact sequence of Galois cohomology is

$$0 \to A(K) \to J(K) \to C(K) \to H^1(K, A) \to H^1(K, J) \to \cdots,$$

so there is an exact sequence

$$0 \to J(K)/A(K) \to C(K) \to \mathrm{Vis}_J(H^1(K, A)) \to 0. \tag{1.1}$$

Thus there is a point $x \in C(K)$ that maps to c. The fiber X over x is a subvariety of J, which, when equipped with its natural action of A, lies in the class of torsors corresponding to c. This is the origin of the terminology "visible". Also, we remark that when K is a number field, $\mathrm{Vis}_J(H^1(K, A))$ is finite because it is torsion and is the surjective image of the finitely generated group $C(K)$.

1.2. Visible Elements of $\text{Ш}(A)$

Let A be an abelian variety over a number field K. The Shafarevich-Tate group of A, which is defined below, measures the failure of the local-to-global principle for certain torsors. The *Shafarevich-Tate group* of A is

$$\text{Ш}(A) := \mathrm{Ker}\left(H^1(K, A) \to \prod_v H^1(K_v, A)\right),$$

where the product is over all places of K.

DEFINITION 1.2. If $\iota : A \hookrightarrow J$ is an embedding, then the *visible subgroup of* $\text{Ш}(A)$ *with respect to* ι is

$$\text{Vis}_J(\text{Ш}(A)) := \text{Ш}(A) \cap \text{Vis}_J(H^1(K, A)) = \text{Ker}(\text{Ш}(A) \to \text{Ш}(J)).$$

1.3. Every Element is Visible Somewhere

PROPOSITION 1.3. *Every element of* $H^1(K, A)$ *is visible in some abelian variety* J.

Proof. Fix $c \in H^1(K, A)$. There is a finite separable extension L of K such that $\text{res}_L(c) = 0 \in H^1(L, A)$. Let $J = \text{Res}_{L/K}(A_L)$ be the Weil restriction of scalars from L to K of the abelian variety A_L (see [BLR90, §7.6]). Thus J is an abelian variety over K of dimension $[L : K] \cdot \dim(A)$, and for any scheme S over K, we have a natural (functorial) group isomorphism $A_L(S_L) \cong J(S)$. The functorial injection $A(S) \hookrightarrow A_L(S_L) \cong J(S)$ corresponds via Yoneda's Lemma to a natural K-group scheme map $\iota : A \to J$, and by construction ι is a monomorphism. But ι is proper and thus is a closed immersion (see [Gro66, §8.11.5]). Using the Shapiro lemma one finds, after a tedious computation, that there is a canonical isomorphism $H^1(K, J) \cong H^1(L, A)$ which identifies $\iota_*(c)$ with $\text{res}_L(c) = 0$. ∎

Remark 1.4.

1. In [CM00], de Jong gave a totally different proof of the above proposition in the case when A is an elliptic curve over a number field. His argument actually displays A as visible inside the Jacobian of a curve.

2. L. Clozel has remarked that the method of proof above is a standard technique in the theory of algebraic groups.

2. THE VISIBILITY DIMENSION

Let A be an abelian variety over a field K and fix $c \in H^1(K, A)$.

DEFINITION 2.1. The *visibility dimension* of c is the minimum of the dimensions of the abelian varieties J such that c is visible in J.

In Section 2.1 we prove an elementary lemma which, when combined with the proof of Proposition 1.3, gives an upper bound on the visibility dimension of c in terms of the order of c and the dimension of A. Then, in Section 2.2, we consider the visibility dimension in the case when $A = E$ is an elliptic curve. After summarizing the results of Mazur and Klenke on the visibility dimension, we apply a theorem of Cassels to deduce that the visibility dimension of $c \in \text{Ш}(E)$ is at most the order of c.

2.1. A Simple Bound

The following elementary lemma, which the second author learned from Hendrik Lenstra, will be used to give a bound on the visibility dimension in terms of the order of c and the dimension of A.

LEMMA 2.2. *Let G be a group, M be a finite (discrete) G-module, and $c \in H^1(G, M)$. Then there is a subgroup H of G such that $\mathrm{res}_H(c) = 0$ and $\#(G/H) \leq \#M$.*

Proof. Let $f : G \to M$ be a cocycle corresponding to c, so $f(\tau\sigma) = f(\tau) + \tau f(\sigma)$ for all $\tau, \sigma \in G$. Let $H = \ker(f) = \{\sigma \in G : f(\sigma) = 0\}$. The map $\tau H \mapsto f(\tau)$ is a well-defined injection from the coset space G/H to M. ∎

The following is a general bound on the visibility dimension.

PROPOSITION 2.3. *The visibility dimension of any $c \in H^1(K, A)$ is at most $d \cdot n^{2d}$ where n is the order of c and d is the dimension of A.*

Proof. The map $H^1(K, A[n]) \to H^1(K, A)[n]$ is surjective and $A[n]$ has order n^{2d}, so Lemma 2.2 implies that there is an extension L of K of degree at most n^{2d} such that $\mathrm{res}_L(c) = 0$. The proof of Proposition 1.3 implies that c is visible in an abelian variety of dimension $[L : K] \cdot \dim A \leq dn^{2d}$. ∎

2.2. The Visibility Dimension for Elliptic Curves

We now consider the case when $A = E$ is an elliptic curve over a number field K. Mazur proved in [Maz99] that every nonzero $c \in Ш(E)[3]$ has visibility dimension 2 (note that Proposition 2.3 only implies that the visibility dimension is ≤ 3). Mazur's result is particularly nice because it shows that c is visible in an abelian variety that is isogenous to the product of two elliptic curves. Using similar techniques, T. Klenke proved in [Kle01] that every nonzero $c \in H^1(K, E)[2]$ has visibility dimension 2 (note that Proposition 2.3 only implies that the visibility dimension of any $c \in H^1(K, E)[2]$ is ≤ 4). It is unknown whether the visibility dimension of every nonzero element of $H^1(K, E)[3]$ is 2, and it is not known whether elements of $Ш(E)[5]$ must have visibility dimension 2.

When c lies in $Ш(E)$ we use a classical result of Cassels to strengthen the conclusion of Proposition 2.3.

PROPOSITION 2.4. *Let E be an elliptic curve over a number field K and let $c \in Ш(E)$. Then the visibility dimension of c is at most the order of c.*

Proof. Let n be the order of c. In view of the restriction of scalars construction in the proof of Proposition 1.3, it suffices to show that there is an extension L of K of degree n such that $\mathrm{res}_L(c) = 0$. Without the hypothesis that c lies in $Ш(E)$, such an extension L might not exist, as Cassels observed in [Cas63]. However, in that same paper, Cassels proved that such an L exists when $c \in Ш(E)$ (see also [O'N01] for another proof). ∎

Remark 2.5. In contrast to the case of dimension 1, it seems to be an open problem to determine whether or not elements of $Ш(A)[n]$ split over an extension of degree n.

3. CONSTRUCTION OF VISIBLE ELEMENTS

The goal of this section is to state and prove the main result of this paper, which we use to construct visible elements of Shafarevich-Tate groups and sometimes give a nontrivial lower bound for the order of the Shafarevich-Tate group of an abelian variety, thus providing new evidence for the conjecture of Birch and Swinnerton-Dyer (see Section 4.1 and [AS02]). The Tamagawa numbers $c_{A,v}$ and $c_{B,v}$ will be defined in Section 3.1 below.

THEOREM 3.1. *Let A and B be abelian subvarieties of an abelian variety J over a number field K such that $A \cap B$ is finite. Let N be an integer divisible by the residue characteristics of primes of bad reduction for B. Suppose n is an integer such that for each prime $p \mid n$, we have $e_p < p-1$ where e_p is the largest ramification of any prime of K lying over p, and that*

$$\gcd\left(n,\ N \cdot \#(J/B)(K)_{\mathrm{tor}} \cdot \#B(K)_{\mathrm{tor}} \cdot \prod_{\text{all places } v} (c_{A,v} \cdot c_{B,v})\right) = 1,$$

where $c_{A,v} = \#\Phi_{A,v}(\mathbf{F}_\ell)$ (resp., $c_{B,\ell}$) is the Tamagawa number of A (resp., B) at v (see Section 3.1 for the definition of $\Phi_{A,v}$). Suppose furthermore that $B[n] \subset A$ as subgroup schemes of J. Then there is a natural map

$$\varphi : B(K)/nB(K) \to \mathrm{Vis}_J(Ш(A)),$$

such that $\ker(\varphi) \subset J(K)/(B(K) + A(K))$. If $A(K)$ has rank 0, then $\ker(\varphi) = 0$ (more generally, $\ker(\varphi)$ has order at most n^r where r is the rank of $A(K)$).

Remark 3.2. Mazur has proved similar results for elliptic curves using flat cohomology (unpublished), and discussions with him motivated this theorem.

In Section 3.1 we recall a definition of the Tamagawa numbers of an abelian variety. In Section 3.2 we prove a lemma, which gives a condition under which there is an unramified nth root of an unramified point. In Section 3.3, we use the snake lemma to produce a map

$$B(K)/nB(K) \hookrightarrow \mathrm{Vis}_J(H^1(K, A))$$

with bounded kernel. Finally, in Section 3.4, we use a local analysis at each place of K to show that the image of the above map lies in Ш(A).

3.1. Tamagawa Numbers

Let A be an abelian variety over a local field K with residue class field k, and let $\mathcal{A}$ be the Néron model of A over the ring of integers of K. The closed fiber $\mathcal{A}_k$ of $\mathcal{A}$ need not be connected. Let $\mathcal{A}_k^0$ denote the geometric component of $\mathcal{A}$ that contains the identity. The group $\Phi_{\mathcal{A}} = \mathcal{A}_k/\mathcal{A}_k^0$ of connected components is a finite group scheme over k. This group scheme is called the *component group* of $\mathcal{A}$, and the *Tamagawa number* of A is $c_A = \#\Phi_{\mathcal{A}}(k)$.

Now suppose that A is an abelian variety over a global field K. For every place v of K, the *Tamagawa number* of A at v, denoted $c_{A,v}$ or just c_v, is the Tamagawa number of A_{K_v}, where K_v is the completion of K at v.

3.2. Smoothness and Surjectivity

In this section, we recall some well-known lemmas that we will use in Section 3.4 to produce unramified cohomology classes. The authors are grateful to B. Conrad for explaining the proofs of these lemmas.

LEMMA 3.3. *If G is a finite-type smooth commutative group scheme over a strictly henselian local ring R and the fibers of G over R are (geometrically) connected, then the multiplication map*

$$n_G : G(R) \to G(R)$$

is surjective *when $n \in R^\times$.*

Proof. Pick an element $g \in G(R)$ and form the cartesian diagram

$$\begin{array}{ccc} Y_g & \xrightarrow{\ \psi\ } & \mathrm{Spec}(R) \\ \downarrow & & \downarrow g \\ G & \xrightarrow{\ n_G\ } & G \end{array}$$

We want to prove that ψ has a section. Since R is strictly henselian, by [Gro67, 18.8.1] it suffices to show that Y_g is étale over R with non-empty closed fiber, or more generally that n_G is étale and surjective.

By Lemma 2(b) of [BLR90, §7.3], n_G is étale. The image of the étale n_G must be an open subgroup scheme, and on fibers over Spec(R) we get surjectivity since an open subgroup scheme of a smooth connected (hence irreducible) group scheme over a field must fill up the whole space [Gro70, $\mathrm{VI_A}$, 0.5]. ∎

Lemma 3.4. *Let A be an abelian variety over the fraction field K of a strictly henselian dvr (e.g., K could be the maximal unramified extension a local field). Let n be an integer not divisible by the residue characteristic of K. Suppose that x is a point of $A(K)$ whose reduction lands in the identity component of the closed fiber of the Néron model of A. Then there exists $z \in A(K)$ such that $nz = x$.*

Proof. Let $\mathcal{A}$ denote the Néron model of A over the valuation ring R of K, and let $\mathcal{A}^0$ denote the "identity component" (i.e., the open subgroup scheme obtained by removing the non-identity components of the closed fiber of $\mathcal{A}$). The hypothesis on the reduction of $x \in A(K) = \mathcal{A}(R)$ says exactly that $x \in \mathcal{A}^0(R)$. Since connected schemes over a field are geometrically connected when there is a rational point [Gro65, Prop. 4.5.13], the fibers of $\mathcal{A}^0$ over $\mathrm{Spec}(R)$ are geometrically connected. The lemma now follows from Lemma 3.3 with $G = \mathcal{A}^0$. ∎

Remark 3.5. M. Baker noted that this argument can also be formulated in terms of formal groups when R is the strict henselization of a *complete* dvr.

Lemma 3.6. *Let $\mathcal{J} \xrightarrow{\phi} \mathcal{C}$ be a smooth surjective morphism of schemes over a strictly Henselian local ring R. Then the induced map $\mathcal{J}(R) \to \mathcal{C}(R)$ is surjective.*

Proof. The argument is similar to that of the proof of Lemma 3.3. Pick an element $g \in \mathcal{C}(R)$ and form the cartesian diagram

$$\begin{array}{ccc} Y_g & \xrightarrow{\quad\psi\quad} & \mathrm{Spec}(R) \\ \big\downarrow & & \big\downarrow{\scriptstyle g} \\ \mathcal{J} & \xrightarrow{\quad\phi\quad} & \mathcal{C} \end{array}$$

We want to prove that ψ has a section. Since ϕ is smooth, ψ is also smooth. By [Gro67, 18.5.17], to show that ψ has a section, we just need to show that the closed fiber of ψ has a section (i.e., a rational point). But this closed fiber is smooth and non-empty (since ϕ is surjective); also its base field is separably closed since R is strictly Henselian. Hence by [BLR90, Cor. 2.2.13], the closed fiber has an R-rational point. ∎

3.3. Visible Elements of $H^1(K, A)$

In this section, we produce a map $B(K)/nB(K) \to \mathrm{Vis}_J(H^1(K, A))$ with bounded kernel.

Lemma 3.7. *Let A and B be abelian subvarieties of an abelian variety J over a number field K such that $A \cap B$ is finite. Suppose n is a natural* *number such that*

$$\gcd\left(n,\ \#(J/B)(K)_{\mathrm{tor}} \cdot \#B(K)_{\mathrm{tor}}\right) = 1$$

and $B[n] \subset A$ *as subgroup schemes of* J. *Then there is a natural map*

$$\varphi : B(K)/nB(K) \to \mathrm{Vis}_J(H^1(K, A))$$

such that $\ker(\varphi) \subset J(K)/(B(K) + A(K))$. *If* $A(K)$ *has rank* 0, *then* $\ker(\varphi) = 0$ *(more generally,* $\ker(\varphi)$ *has order at most* n^r *where* r *is the rank of* $A(K)$*).*

Proof. First we produce a map $\varphi : B(K)/nB(K) \to \mathrm{Vis}(H^1(K, A))$ by using that $B[n] \subset A$ hence a certain map factors through multiplication by n. Then we use the snake lemma and our hypothesis that n does not divide the orders of certain torsion groups to bound the dimension of the kernel of φ.

The quotient J/A is an abelian variety C over K. The long exact sequence of Galois cohomology associated to the short exact sequence

$$0 \to A \to J \to C \to 0$$

begins

$$0 \to A(K) \to J(K) \to C(K) \xrightarrow{\delta} H^1(K, A) \to \cdots . \tag{3.1}$$

Let ψ be map $B \to C$ obtained by composing the inclusion $B \hookrightarrow J$ with the quotient map $J \to C$. Since $B[n] \subset A$, we see that ψ factors through multiplication by n, so the following diagram commutes:

$$\begin{array}{ccccc} & & B & \xrightarrow{\ n\ } & B \\ & & \downarrow & \searrow^{\psi} & \downarrow \\ A & \longrightarrow & J & \longrightarrow & C. \end{array}$$

Using that $B[n](K) = \{0\}$, we obtain the following commutative diagram, all of whose rows and columns are exact:

$$\begin{array}{ccccccccc} & & K_0 & & K_1 & & K_2 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & B(K) & \xrightarrow{\ n\ } & B(K) & \longrightarrow & B(K)/nB(K) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & \searrow^{\pi} & \downarrow{\scriptstyle \varphi} & & \\ 0 & \longrightarrow & J(K)/A(K) & \longrightarrow & C(K) & \longrightarrow & \delta(C(K)) & \longrightarrow & 0 \\ & & \downarrow & & & & & & \\ & & K_3, & & & & & & \end{array} \tag{3.2}$$

where K_0, K_1 and K_2 are the indicated kernels and K_3 is the indicated cokernel. Exactness of the top row expresses the fact that $B[n](K) = \{0\}$, and the bottom exact row arises from the exact sequence (3.1) above. The first vertical map $B(K) \to J(K)/A(K)$ is induced by the inclusion $B(K) \hookrightarrow J(K)$ composed with the quotient map $J(K) \to J(K)/A(K)$. The second vertical map $B(K) \to C(K)$ exists because the composition $B \hookrightarrow J \to C$ has kernel $B \cap A$, which contains $B[n]$, by assumption. The third vertical map exists because π contains $nB(K)$ in its kernel, so that π factors through $B(K)/nB(K)$.

The sequence (1.1) on page 3 implies that the image of φ is contained in $\mathrm{Vis}_J(H^1(K, A))$. The snake lemma gives an exact sequence

$$K_0 \to K_1 \to K_2 \to K_3.$$

Because $B \to C$ has finite kernel, $K_1 \subset B(K)_{\mathrm{tor}}$. Since $B[n](K) = \{0\}$ and K_2 is an n-torsion group, the map $K_1 \to K_2$ is the 0 map. Thus $K_2 = \ker(\varphi)$ is isomorphic to a subgroup of $K_3 = J(K)/(A(K) + B(K))$, as claimed.

Any torsion in the quotient $J(K)/B(K)$ is of order coprime to n because $J(K)/B(K)$ is a subgroup of $(J/B)(K)$, and $\gcd(n, \#(J/B)(K)_{\mathrm{tor}}) = 1$, by assumption. Thus if $A(K)$ is a torsion group, $K_3 = (J(K)/B(K))/A(K)$ has no nontrivial torsion of order dividing n, so when $A(K)$ has rank zero, $\ker(\varphi) = 0$.

Consider the map $\psi : A(K) \to J(K)/B(K)$. To show that $\ker(\phi)$ has order at most n^r, where r is the rank of $A(K)$, it suffices to show that $\mathrm{coker}(\psi)[n]$ has order at most n^r. To prove the latter statement, by the structure theorem for finite abelian groups, it suffices to prove it for the case when n is a power of a prime. Moreover, we may assume that $A(K)$ and $J(K)/B(K)$ have no prime-to-n torsion. Then $J(K)/B(K)$ is in fact torsion-free, and so we may also assume $A(K)$ is torsion-free. With these assumptions, the statement we want to prove follows easily by elementary group-theoretic arguments (in particular, by considering of the Smith normal form of the matrix representing ψ). ∎

3.4. Proof of Theorem 3.1

Proof of Theorem 3.1. The proof proceeds in two steps. The first step is to use the hypothesis that $B[n] \subset A$ to produce a map $B(K)/nB(K) \to \mathrm{Vis}_J(H^1(K, A))[n]$. This was done in Section 3.3. The second step is to perform a local analysis at each place v of K in order to prove that the image of this map consists of locally-trivial cohomology classes. We divide this local analysis into three cases:

1. When v is real archimedian, we use that $\gcd(2, n) = 1$. (We know that for any $p \mid n$ we have $p > 2$ because $1 \le e_p < p - 1$, by assumption.)

2. When $\gcd(\mathrm{char}(v), n) = 1$, we use the result of Section 3.2 and a relationship between unramified cohomology and the cohomology of a component group.

3. When $\gcd(\mathrm{char}(v), n) \neq 1$, for each prime $p \mid n$, the reduction of J is abelian and by hypothesis $e_p < p-1$, so we can apply an exactness theorem from [BLR90].

We now deduce that the image of $B(K)/nB(K)$ in $H^1(K, A)$ lies in $Ш(A)$. Fix an element $x \in B(K)$. To show that $\pi(x) \in Ш(A)$, it suffices to show that $\mathrm{res}_v(\pi(x)) = 0$ for all places v of K.

Case 1. v real archimedian: At a real archimedian place v, the restriction $\mathrm{res}_v(\pi(x))$ is killed by 2 and the odd n, hence $\mathrm{res}_v(\pi(x)) = 0$.

Case 2. $\gcd(\mathrm{char}(v), n) = 1$: Suppose that $\gcd(\mathrm{char}(v), n) = 1$. Let $m = c_{B,v} = \Phi_{B,v}(\mathbf{F}_v)$ be the Tamagawa number of B at v. The reduction of mx lies in the identity component of the closed fiber $\mathcal{B}_{\mathbf{F}_v}$ of the Néron model of B at v, so by Lemma 3.4, there exists $z \in B(K_v^{\mathrm{ur}})$ such that $nz = mx$. Thus the cohomology class $\mathrm{res}_v(\pi(mx))$ is defined by a cocycle that sends $\sigma \in \mathrm{Gal}(\overline{K_v}/K_v)$ to $\sigma(z) - z \in A(K_v^{\mathrm{ur}})$ (see diagram (3.2) for the definition of π). In particular, $\mathrm{res}_v(\pi(mx))$ is unramified at v. By [Mil86, Prop. 3.8],

$$H^1(K_v^{\mathrm{ur}}/K_v, A(K_v^{\mathrm{ur}})) = H^1(K_v^{\mathrm{ur}}/K_v, \Phi_{A,v}(\overline{\mathbf{F}}_v)),$$

where $\Phi_{A,v}$ is the component group of A at v. The Herbrand quotient of a finite module is 1 (see, e.g., [Ser79, VIII.4.8]), so

$$\#\Phi_{A,v}(\mathbf{F}_v) = \#H^1(K_v^{\mathrm{ur}}/K_v, \Phi_{A,v}(\overline{\mathbf{F}}_v)).$$

Thus the order of $\mathrm{res}_v(\pi(mx))$ divides both $\#\Phi_{A,v}(\mathbf{F}_v)$ and n. Since by assumption $\gcd(\#\Phi_{A,v}(\mathbf{F}_v), n) = 1$, it follows that $\mathrm{res}_v(\pi(mx)) = 0$, hence $m\,\mathrm{res}_v(\pi(x)) = 0$. Again, since the order of $\pi(x)$ divides n, and $\gcd(n, m) = 1$, we have $\mathrm{res}_v(\pi(x)) = 0$.

Case 3. $\gcd(\mathrm{char}(v), n) = p \neq 1$: Suppose that $\mathrm{char}(v) = p \mid n$. Let R be the ring of integers of K_v^{ur}, and let $\mathcal{A}$, $\mathcal{J}$, and $\mathcal{C}$ be the Néron models of A, J, and C, respectively. Since $e_p < p-1$ and J has abelian reduction at v (since $p \nmid N$), by [BLR90, Thm. 7.5.4(iii)], the induced sequence $0 \to \mathcal{A} \to \mathcal{J} \xrightarrow{\phi} \mathcal{C} \to 0$ is exact, which means that ϕ is faithfully flat and surjective with scheme-theoretic kernel $\mathcal{A}$. Since ϕ is faithfully flat with smooth kernel, ϕ is smooth (see, e.g., [BLR90, 2.4.8]). By Lemma 3.6, $\mathcal{J}(R) \to \mathcal{C}(R)$ is a surjection; i.e., $J(K_v^{\mathrm{ur}}) \to C(K_v^{\mathrm{ur}})$ is a surjection.

So $\mathrm{res}_v(\pi(x))$ is unramified, and again by [Mil86, Prop. 3.8],

$$H^1(K_v^{\mathrm{ur}}/K_v, A) \cong H^1(K_v^{\mathrm{ur}}/K_v, \Phi_{A,v}(\overline{\mathbf{F}}_v)).$$

But $H^1(K_v^{\mathrm{ur}}/K_v, \Phi_{A,v}(\overline{\mathbf{F}}_v)) = \{0\}$, since $\Phi_{A,v}(\overline{\mathbf{F}}_v)$ is trivial, as A has good reduction at v (because $p \nmid N$). Thus $\mathrm{res}_v(\pi(x)) = 0$. ∎

4. SOME EXAMPLES

This section contains some examples of visible and invisible elements of Shafarevich-Tate groups. Section 4.1 uses Theorem 3.1 to produce nontrivial visible elements of $Ш(A)$, where A is a 20-dimensional modular abelian variety, thus giving evidence for the BSD conjecture. In Section 4.2 we show that an invisible Shafarevich-Tate group from [CM00] becomes visible at a higher level.

In [AS02], we describe the notation used below (which is standard) and the algorithms that we used to carry out the computations described below. We also report on a large number of similar computations, which were performed using the second author's modular symbols package, which is part of MAGMA (see [BCP97]).

4.1. Visibility in an Abelian Variety of Dimension 20

Using the methods described in [AS02], we find that $S_2(\Gamma_0(389))$ contains exactly five Galois-conjugacy classes of newforms, and these are defined over extensions of $\mathbf{Q}$ of degrees 1, 2, 3, 6, and 20. Thus $J = J_0(389)$ decomposes, up to isogeny, as a product $A_1 \times A_2 \times A_3 \times A_6 \times A_{20}$ of abelian varieties, where $d = \dim A_d$ and A_d is the quotient corresponding to the appropriate Galois-conjugacy class of newforms.

Next we consider the arithmetic of each A_d. Using [AS02], we find that

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

and

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

where $2^?$ is a power of 2. Using [AS02], we find that $\#A_{20}(\mathbf{Q}) = 97$ and the Tamagawa number of A_{20} at 389 is also 97. The BSD Conjecture then predicts that $\#Ш(A_{20}) = 5^2 \cdot 2^?$. The following proposition provides support for this conjecture.

PROPOSITION 4.1. *There is an inclusion*

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

Proof. Let $A = A_{20}^\vee$, $B = A_1^\vee = A_1$ and $J = A + B \subset J_0(389)$. Using algorithms in [AS02], we find that $A \cap B \cong (\mathbf{Z}/4)^2 \times (\mathbf{Z}/5\mathbf{Z})^2$, so $B[5] \subset A$. Since 5 does not divide the numerator of $(389-1)/12$, it does not divide the Tamagawa numbers or the orders of the torsion subgroups of A, B, J, and J/B (we also verified this using a modular symbols computations), so Theorem 3.1 implies that there is an injective map

$$A_1(\mathbf{Q})/5A_1(\mathbf{Q}) \hookrightarrow \mathrm{Vis}_J(Ш(A_{20}^\vee).$$

To finish, note that Cremona [Cre97] has verified that $A_1(\mathbf{Q}) \approx \mathbf{Z} \times \mathbf{Z}$. ∎

4.2. Invisible Elements that Becomes Visible at Higher Level

Consider the elliptic curve E of conductor $5389 = 17 \cdot 317$ defined by the equation

$$y^2 + xy + y = x^3 - 35590x - 2587197.$$

In [CM00], Cremona and Mazur observe that the BSD conjecture implies that $\#Ш(E) = 9$, but they find that $\mathrm{Vis}_{J_0(5389)}(Ш(E)[3]) = \{0\}$. We will now verify, without assuming any conjectures, that $9 \mid \#Ш(E)$ and that these 9 elements of $Ш(E)$ are visible in $J_0(5389 \cdot 7)$.

First note that the mod 3 representation $\rho_{E,3}$ attached to E is irreducible because E is semistable and admits no 3-isogeny (according to [Cre]). The newform attached to E is

$$f_E = q + q^2 - 2q^3 - q^4 + 2q^5 - 2q^6 - 2q^7 + \cdots,$$

and $a_7^2 = (-2)^2 \equiv (7+1)^2 \pmod 3$, so Ribet's level-raising theorem [Rib90] implies that there is a newform g of level $7 \cdot 5389$ that is congruent modulo 3 to f_E. This observation led us to the following proposition.

PROPOSITION 4.2. *Map E to $J_0(7 \cdot 5389)$ by the sum of the two maps on Jacobians induced by the two degeneracy maps $X_0(7 \cdot 5389) \to X_0(5389)$. The image E' of E in $J_0(7 \cdot 5389)$ is 2-isogenous to E and*

$$(\mathbf{Z}/3\mathbf{Z})^2 \subset \mathrm{Vis}_{J_0(7\cdot 5389)}(Ш(E')).$$

Proof. It is easy to see from the discussion in [Rib90] that the kernel of the sum of the two degeneracy maps $J_0(5389) \to J_0(7 \cdot 5389)$ is a group of 2-power order, so E' is isogenous to E via an isogeny of degree a power of 2.

Consider the elliptic curve F defined by $y^2 - y = x^3 + x^2 + 34x - 248$. Using Cremona's programs `tate` and `mwrank` we find that F has conductor $7 \cdot 5389$, and that $F(\mathbf{Q}) \cong \mathbf{Z} \times \mathbf{Z}$. The Tamagawa numbers of F at 7, 17, and 317 are 1, 2, and 1, respectively. The newform attached to F is

$$f_F = q - 2q^2 + q^3 + 2q^4 - q^5 - 2q^6 - q^7 + \cdots$$

and, by [Stu87], we prove that $f_E(q) + f_E(q^7) \equiv f_F \pmod 3$ by checking this congruence for the first $7632 = [\mathrm{SL}_2(\mathbf{Z}) : \Gamma_0(7 \cdot 5389)]/6$ terms. Since $2 \leq k < 3$ and $3 \nmid 7 \cdot 5389$, the first part of the multiplicity one theorem of [Edi92, §9] implies that $F[3] = E'[3]$.

Finally, we apply Theorem 3.1 with $A = E'$, $B = F$, $J = A + B \subset J_0(7 \cdot 5389)$, $N = 7 \cdot 5389$, and $n = 3$. It is routine to check the hypothesis. For example, the hypothesis that J/B has no $\mathbf{Q}$-rational 3-torsion can be checked as follows. Cremona's online tables imply that E admits no 3-isogeny, so $E[3]$ is irreducible. Since J/B is isogenous to E, the representation $(J/B)[3]$ is also irreducible, so $(J/B)(\mathbf{Q})[3] = \{0\}$. Thus, by

Theorem 3.1, we have $(\mathbf{Z}/3\mathbf{Z})^2 \subset \mathrm{Vis}_J(\text{Ш}(E'))$. To finish the proof, note that $\mathrm{Vis}_J(\text{Ш}(E')) \subset \mathrm{Vis}_{J_0(7\cdot 5389)}(\text{Ш}(E'))$. ∎

Since E' is 2-isogenous to E and $9 \mid \#\text{Ш}(E')$, it follows that $9 \mid \#\text{Ш}(E)$, as predicted by the BSD conjecture.

REFERENCES

[AS02] A. Agashe and W. A. Stein, *Visible Evidence for the Birch and Swinnerton-Dyer Conjecture for Rank 0 Modular Abelian Varieties*, Preprint.

[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).

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

[Cas63] J. W. S. Cassels, *Arithmetic on curves of genus 1. V. Two counterexamples*, J. London Math. Soc. **38** (1963), 244–248.

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

[Cre] J. E. Cremona, *Elliptic curves of conductor* ≤ 12000, `http://www.maths.nott.ac.uk/personal/jec/ftp/data/`.

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

[Edi92] B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594.

[Gro65] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II*, Inst. Hautes Études Sci. Publ. Math. (1965), no. 24, 231.

[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.

[Gro67] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV*, Inst. Hautes Études Sci. Publ. Math. (1967), no. 32, 361.

[Gro70] A. Grothendieck, *Schémas en groupes. I: Propriétés générales des schémas en groupes*, Springer-Verlag, Berlin, 1970.

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

[LT58] S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. Math. **80** (1958), 659–684.

[Maz99] B. Mazur, *Visualizing elements of order three in the Shafarevich-Tate group*, Asian J. Math. **3** (1999), no. 1, 221–232.

[Mil86] J. S. Milne, *Arithmetic duality theorems*, Academic Press Inc., Boston, Mass., 1986.

[O'N01] C. O'Neil, *The period-index obstruction for elliptic curves*, to appear in Journal of Number Theory.

[Rib90] K. A. Ribet, *Raising the levels of modular representations*, Séminaire de Théorie des Nombres, Paris 1987–88, Birkhäuser Boston, Boston, MA, 1990, pp. 259–271.

[Ser79] J-P. Serre, *Local fields*, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

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

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