Visibility of Mordell-Weil Groups

William A. Stein[1]

Received: March 8, 2005
Revised: August 21, 2007

Communicated by Stephen Lichtenbaum

Abstract. We introduce a notion of visibility for Mordell-Weil groups, make a conjecture about visibility, and support it with theoretical evidence and data. These results shed new light on relations between Mordell-Weil and Shafarevich-Tate groups.

11G05, 11G10, 11G18, 11Y40
Keywords and Phrases: Elliptic Curves, Abelian Varieties, Mordell-Weil Groups, Shafarevich-Tate Groups, Visibility

1 Introduction

Consider an exact sequence $0 \to C \to B \to A \to 0$ of abelian varieties over a number field K. We say that the covering $B \to A$ is *optimal* since its kernel C is connected. As introduced in [LT58], there is a corresponding long exact sequence of Galois cohomology

$$0 \to C(K) \to B(K) \to A(K) \xrightarrow{\delta} \mathrm{H}^1(K, C) \to \mathrm{H}^1(K, B) \to \mathrm{H}^1(K, A) \to \cdots$$

The study of the Mordell-Weil group $A(K)$ is central in arithmetic geometry. For example, the Birch and Swinnerton-Dyer conjecture (BSD conjecture) of [Bir71, Tat66]), which is one of the Clay Math Problems [Wil00], asserts that the rank r of $A(K)$ equals the ordering vanishing of $L(A, s)$ at $s = 1$, and also gives a conjectural formula for $L^{(r)}(A, 1)$ in terms of the invariants of A.

The group $\mathrm{H}^1(K, A)$ is also of interest in connection with the BSD conjecture, because it contains the Shafarevich-Tate group

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

which is the most mysterious object appearing in the BSD conjecture.

[1]This material is based upon work supported by the National Science Foundation under Grant No. 0555776.

Definition 1.0.1 (Visibility). The *visible subgroup* of $\mathrm{H}^1(K, C)$ relative to the embedding $C \hookrightarrow B$ is

$$\begin{aligned}\mathrm{Vis}_B \mathrm{H}^1(K, C) &= \mathrm{Ker}(\mathrm{H}^1(K, C) \to \mathrm{H}^1(K, B)) \\ &\cong \mathrm{Coker}(B(K) \to A(K)).\end{aligned}$$

The *visible quotient* of $A(K)$ relative to the optimal covering $B \to A$ is

$$\begin{aligned}\mathrm{Vis}^B(A(K)) &= \mathrm{Coker}(B(K) \to A(K)) \\ &\cong \mathrm{Vis}_B \mathrm{H}^1(K, C).\end{aligned}$$

We say an abelian variety over $\mathbb{Q}$ is *modular* if it is a quotient of the modular Jacobian $J_1(N) = \mathrm{Jac}(X_1(N))$, for some N. For example, every elliptic curve over $\mathbb{Q}$ is modular [BCDT01].

This paper gives evidence toward the following conjecture that Mordell-Weil groups should give rise to many visible Shafarevich-Tate groups.

Conjecture 1.0.2. *Let A be an abelian variety over a number field K. For every integer m, there is an exact sequence $0 \to C \to B \to A \to 0$ such that:*

1. *The image of $B(K)$ in $A(K)$ is contained in $mA(K)$, so $A(K)/mA(K)$ is a quotient of $\mathrm{Vis}^B(A(K))$.*

2. *If $K = \mathbb{Q}$ and A is modular, then B is modular.*

3. *The rank of C is zero.*

4. *We have $\mathrm{Coker}(B(K) \to A(K)) \subset Ш(C/K)$, via the connecting homomorphism.*

In [Ste04] we give the following computational evidence for this conjecture.

Theorem 1.0.3. *Let E be the rank 1 elliptic curve $y^2+y = x^3-x$ of conductor 37. Then Conjecture 1.0.2 is true for all* primes $m = p < 25000$ *with* $p \neq 2, 37$.

Let $f = \sum a_n q^n$ be the newform associated to the elliptic curve E of Theorem 1.0.3. Suppose p is one of the primes in the theorem. Then there is an $\ell \equiv 1 \pmod p$ and a surjective Dirichlet character $\chi : (\mathbb{Z}/\ell\mathbb{Z})^* \to \mu_p$ such that $L(f \otimes \chi, 1) \neq 0$. The C of the theorem belongs to the isogeny class of abelian varieties associated to f^χ and C has dimension $p - 1$.

In general, we expect the construction of [Ste04] to work for any elliptic curve and any odd prime p of good reduction. The main obstruction to proving that it does work is proving a nonvanishing result for the special values $L(f^\chi, 1)$. In [Ste04], we verified this hypothesis using modular symbols for $p < 25000$.

A surprising observation that comes out of the construction of [Ste04] is that $\#Ш(C) = p \cdot n^2$, where n^2 is an integer square. We thus obtained the first ever examples of abelian varieties whose Shafarevich-Tate groups have order neither a square nor twice a square.

1.1 Contents

In Section 2, we give a brief review of results about visibility of Shafarevich-Tate groups. In Section 3, we give evidence for Conjecture 1.0.2 using results of Kato, Lichtenbaum and Mazur. Section 4 is about bounding the dimension of the abelian varieties in which Mordell-Weil groups are visible. We prove that every Mordell-Weil group is 2-visible relative to an abelian surface. In Section 5, we describe how to construct visible quotients of Mordell-Weil groups, and carry out a computational study of relations between Mordell-Weil groups of elliptic curves and the arithmetic of rank 0 factors of $J_0(N)$.

1.2 Acknowledgement

The author had extremely helpful conversations with Barry Mazur and Grigor Grigorov. Proposition 3.0.3 was proved jointly with Ken Ribet. The author was supported by NSF grant DMS-0400386. He used Magma [BCP97] and SAGE [Sage07] for computing the data in Section 5.

2 Review of Visibility of Galois Cohomology

In this section, we briefly review visibility of elements of $\mathrm{H}^1(K, A)$, as first introduced by Mazur in [CM00, Maz99], and later developed by Agashe and Stein in [Aga99a, AS05, AS02]. We describe two basic results about visibility, and in Section 2.2 we discuss modularity of elements of $\mathrm{H}^1(K, A)$.

Consider an exact sequence of abelian varieties

$$0 \to A \to B \to C \to 0$$

over a number field K. Elements of $\mathrm{H}^0(K, C)$ are points, so they are relatively easy to "visualize", but elements of $\mathrm{H}^1(K, A)$ are mysterious.

There is a geometric way to view elements of $\mathrm{H}^1(K, A)$. The Weil-Chatalet group $\mathrm{WC}(A/K)$ of A over K is the group of isomorphism classes of principal homogeneous spaces for A, where a principal homogeneous space is a variety X and a simply-transitive action $A \times X \to X$. Thus X is a twist of A as a variety, but $X(K) = \emptyset$, unless X is isomorphic to A. Also, the elements of $\text{Ш}(A)$ correspond to the classes of X that have a K_v-rational point for all places v. By [LT58, Prop. 4], there is an isomorphism between $\mathrm{H}^1(K, A)$ and $\mathrm{WC}(A/K)$.

In [CM00], Mazur introduced the visible subgroup of H^1 as in Definition 1.0.1 in order to help unify diverse constructions of principal homogeneous spaces. Many papers were subsequently written about visibility, including [Aga99b, Maz99, Kle01, AS02, MO03, DWS03, AS05, Dum01].

Remark 2.0.1. Note that $\mathrm{Vis}_B\, \mathrm{H}^1(K, A)$ depends on the embedding of A into B. For example, if $B = B_1 \times A$, then there could be nonzero visible elements if A is embedded into the first factor, but there will be no nonzero visible elements if A is embedded into the second factor.

A connection between visibility and $\mathrm{WC}(A/K)$ is as follows. Suppose

$$0 \to A \to B \xrightarrow{\pi} C \to 0$$

is an exact sequence of abelian varieties and that $c \in \mathrm{H}^1(K, A)$ is visible in B. Thus there exists $x \in C(K)$ such that $\delta(x) = c$, where $\delta : C(K) \to \mathrm{H}^1(K, A)$ is the connecting homomorphism. Then $X = \pi^{-1}(x) \subset B$ is a translate of A in B, so the group law on B gives X the structure of principal homogeneous space for A, and this homogeneous space in $\mathrm{WC}(A/K)$ corresponds to c.

2.1 Basic Facts

Two basic facts about visibility are that the visible subgroup of $\mathrm{H}^1(K, A)$ in B is finite, and that each element of $\mathrm{H}^1(K, A)$ is visible in some B.

Lemma 2.1.1. *The group* $\mathrm{Vis}_B \mathrm{H}^1(K, A)$ *is finite.*

Proof. Let $C = B/A$. By the Mordell-Weil theorem $C(K)$ is finitely generated. The group $\mathrm{Vis}_B \mathrm{H}^1(K, A)$ is a homomorphic image of $C(K)$ so it is finitely generated. On the other hand, it is a subgroup of $\mathrm{H}^1(K, A)$, so it is a torsion group. But a finitely generated torsion abelian group is finite. $\square$

Proposition 2.1.2. *Let* $c \in \mathrm{H}^1(K, A)$*. Then there exists an abelian variety* B *and an embedding* $A \hookrightarrow B$ *such that* c *is visible in* B*. Moreover,* B *can be chosen to be a twist of a power of* A*.*

Proof. See [AS02, Prop. 1.3] for a cohomological proof or [JS05, §5] for an equivalent geometric proof. Johan de Jong also proved that everything is visible somewhere in the special case $\dim(A) = 1$ using Azumaya algebras, Néron models, and étale cohomology, as explained in [CM00, pg. 17–18], but his proof gives no (obvious) specific information about the structure of B. $\square$

2.2 Modularity

Usually one focuses on visibility of elements in $\text{Ш}(A) \subset \mathrm{H}^1(K, A)$. The papers [CM00, AS02, AS05] contain a number of results about visibility in various special cases, and tables involving elliptic curves and modular abelian varieties.

For example, if $A \subset J_0(389)$ is the 20-dimensional simple newform abelian variety, then we show that

$$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong E(\mathbb{Q})/5E(\mathbb{Q}) \subset \text{Ш}(A),$$

where E is the elliptic curve of conductor 389. The divisibility $5^2 \mid \#\text{Ш}(A)$ is as predicted by the BSD conjecture. The paper [AS05] contains a few dozen other examples like this; in most cases, explicit computational construction of the Shafarevich-Tate group seems hopeless using any other known techniques.

The author has conjectured that if A is a modular abelian variety, then every element of $\text{Ш}(A)$ is modular, i.e., visible in a modular abelian variety. It is a theorem that if $c \in \text{Ш}(A)$ has order either 2 or 3 and A is an elliptic curve, then c is modular (see [JS05]).

3 Results Toward Conjecture 1.0.2

The main result of this section is a proof of parts 1 and 2 of Conjecture 1.0.2 for elliptic curves over $\mathbb{Q}$. We prove more generally that Mazur's conjecture on finite generatedness of Mordell-Weil groups over cyclotomic $\mathbb{Z}_p$-extensions implies part 1 of Conjecture 1.0.2. Then we observe that for elliptic curves over $\mathbb{Q}$, Mazur's conjecture is known, and prove that the abelian varieties that appear in our visibility construction are modular, so parts 1 and 2 of Conjecture 1.0.2 are true for elliptic curves over $\mathbb{Q}$.

For a prime p, the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ is an extension $\mathbb{Q}_{p^\infty}$ of $\mathbb{Q}$ with Galois group $\mathbb{Z}_p$; also $\mathbb{Q}_{p^\infty}$ is contained in the cyclotomic field $\mathbb{Q}(\mu_{p^\infty})$. We let $\mathbb{Q}_{p^n}$ denote the unique subfield of $\mathbb{Q}_{p^\infty}$ of degree p^n over $\mathbb{Q}$. If K is an arbitrary number field, the cyclotomic $\mathbb{Z}_p$-extension of K is $K_{p^\infty} = K\cdot\mathbb{Q}_{p^\infty}$. We denote by K_{p^n} the unique subfield of K_{p^∞} of degree p^n over K. The extension K_{p^∞} of K decomposes as a tower

$$K = K_{p^0} \subset K_{p^1} \subset \cdots \subset K_{p^n} \subset \cdots \subset K_{p^\infty} = \bigcup_{n=0}^{\infty} K_{p^n}.$$

Mazur hints at the following conjecture in [Maz78] and [RM05, §3]:

Conjecture 3.0.1 (Mazur). *If A is an abelian variety over a number field K and p is a prime, then $A(K_{p^\infty})$ is a finitely generated abelian group.*

Let L/K be a finite extension of number fields and A an abelian variety over K. In much of the rest of this paper we will use the *restriction of scalars* $R = \mathrm{Res}_{L/K}(A_L)$ of A viewed as an abelian variety over L. Thus R is an abelian variety over K of dimension $[L : K]$, and R represents the following functor on the category of K-schemes:

$$S \mapsto E_L(S_L).$$

If L/K is Galois, then we have an isomorphism of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$-modules

$$R(\overline{\mathbb{Q}}) = A(\overline{\mathbb{Q}}) \otimes_{\mathbb{Z}} \mathbb{Z}[\mathrm{Gal}(L/K)],$$

where $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acts on $\sum P_\sigma \otimes \sigma$ by

$$\tau\left(\sum P_\sigma \otimes \sigma\right) = \sum \tau(P_\sigma) \otimes \tau_{|L} \cdot \sigma,$$

where $\tau_{|L}$ is the image of τ in $\mathrm{Gal}(L/K)$.

Theorem 3.0.2. *Conjecture 3.0.1 implies part 1 of Conjecture 1.0.2. More precisely, if A/K is an abelian variety, m is a positive integer, and $A(K_{p^\infty})$ is finitely generated for each $p \mid m$, then there is an optimal covering of the form $B = \mathrm{Res}_{L/K}(A_L) \to A$ such that L is abelian over K and the image of $B(K)$ in $A(K)$ is contained in $mA(K)$.*

Proof. Fix a prime $p \mid m$. Let $M = K_{p^\infty}$. Because $A(M)$ is finitely generated, some finite set of generators must be in a single sufficiently large $A(K_{p^n})$, and for this n we have $A(M) = A(K_{p^n})$. For any integer $j > 0$ let

$$R_j = \mathrm{Res}_{K_{p^j}/K}(A_{K_{p^j}}).$$

Then, as explained in [Ste04], the trace map induces an exact sequence

$$0 \to B_j \to R_j \xrightarrow{\pi_j} A \to 0,$$

with B_j an abelian variety. Then for any $j \geq n$, $A(K_{p^j}) = A(K_{p^n})$, so

$$\begin{aligned}
\mathrm{Vis}^{B_j}(A(K)) &\cong A(K)/\pi_j(R_j(K)) \\
&= A(K)/\operatorname{Tr}_{K_{p^j}/K}(A(K_{p^j})) \\
&= A(K)/\operatorname{Tr}_{K_{p^n}/K}(\operatorname{Tr}_{K_{p^j}/K_{p^n}}(A(K_{p^j}))) \\
&= A(K)/\operatorname{Tr}_{K_{p^n}/K}(\operatorname{Tr}_{K_{p^j}/K_{p^n}}(A(K_{p^n}))) \\
&= A(K)/\operatorname{Tr}_{K_{p^n}/K}(p^{j-n}A(K_{p^n})) \\
&= A(K)/p^{j-n}\operatorname{Tr}_{K_{p^n}/K}(A(K_{p^n})) \\
&\to A(K)/p^{j-n}A(K),
\end{aligned}$$

where the last map is surjective since

$$\operatorname{Tr}_{K_{p^n}/K}(A(K_{p^n})) \subset A(K).$$

Arguing as above, for each prime $p \mid m$, we find an extension L_p of K of degree a power of p such that $\operatorname{Tr}_{L_p/K}(A(L_p)) \subset p^{\nu_p}A(K)$, where $\nu_p = \mathrm{ord}_p(m)$. Let L be the compositum of the fields L_p. Then for each $p \mid m$,

$$\operatorname{Tr}_{L/K}(A(L)) = \operatorname{Tr}_{L_p/K}(\operatorname{Tr}_{L/L_p}(A(L))) \subset \operatorname{Tr}_{L_p/K}(A(L_p)) \subset p^{\nu_p}A(K).$$

Thus

$$\operatorname{Tr}_{L/K}(A(L)) \subset \bigcap_{p \mid m} p^{\nu_p}A(K) = mA(K), \tag{1}$$

where for the last equality we view $A(K)$ as a finite direct sum of cyclic groups.

Let $R = \mathrm{Res}_{L/K}(A_L)$. Then trace induces an optimal cover $R \to A$, and (1) implies that we have the required surjective map

$$\mathrm{Vis}^R(A(K)) = A(K)/\operatorname{Tr}_{L/K}(A(L)) \to A(K)/mA(K).$$

□

We will next prove parts 1 and 2 of Conjecture 1.0.2 for elliptic curves over $\mathbb{Q}$ by observing that Conjecture 3.0.1 is a theorem of Kato in this case. We first prove a modularity property for restriction of scalars. Recall that a modular abelian variety is a quotient of $J_1(N)$.

Proposition 3.0.3. *If A is a modular abelian variety over $\mathbb{Q}$ and K is an abelian extension of $\mathbb{Q}$, then $\mathrm{Res}_{K/\mathbb{Q}}(A_K)$ is also a modular abelian variety.*

Proof. Since A is modular, A is isogenous to a product of abelian varieties A_f attached to newforms in $S_2(\Gamma_1(N))$, for various N. Since the formation of restriction of scalars commutes with products, it suffices to prove the proposition under the hypothesis that $A = A_f$ for some newform f. Let $R = \mathrm{Res}_{K/\mathbb{Q}}(A_f)$. As discussed in [Mil72, pg. 178], for any prime p there is an isomorphism of $\mathbb{Q}_p$-adic Tate modules

$$V_p(R) \cong \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} V_p(A_K).$$

The induced representation on the right is the direct sum of twists of $V_p(A_K)$ by characters of $\mathrm{Gal}(K/\mathbb{Q})$. This is isomorphic to the $\mathbb{Q}_p$-adic Tate module of some abelian variety $P = \prod_\chi A_{g^\chi}$, where χ runs through certain Dirichlet characters corresponding to the abelian extension $K/\mathbb{Q}$, and g runs through certain $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates of f, and g^χ denotes the twist of g by χ. Falting's theorem (see e.g., [Fal86, §5]) then gives us the desired isogeny $R \to P$.

It is not necessary to use the full power of Falting's theorem to prove this proposition, since Ribet [Rib80] gave a more elementary proof of Falting's theorem in the case of modular abelian varieties. However, we must work some to apply Ribet's theorem, since we do not know yet that R is modular.

Let R and P be as above. Over $\overline{\mathbb{Q}}$, the abelian variety A is isogenous to a power of a simple abelian variety B, since if more than one non-isogenous simple occurred in the decomposition of $A/\overline{\mathbb{Q}}$, then $\mathrm{End}(A/\overline{\mathbb{Q}})$ would not be a matrix ring over a (possibly skew) field (see [Rib92, §5]). For any character χ, by the (3) $\implies$ (2) assertion of [Rib80, Thm. 4.7], the abelian varieties A_f and A_{f^χ} are isogenous over $\overline{\mathbb{Q}}$ to powers of the same abelian variety A', hence to powers of the simple B. A basic property of restriction of scalars is that R_K is isomorphic to a power of $(A_f)_K$, hence R_K is isogenous over $\overline{\mathbb{Q}}$ to a power of B. Thus R and P are both isogenous over $\overline{\mathbb{Q}}$ to a power of B, so R is isogenous to P over $\overline{\mathbb{Q}}$, since they have the same dimension, as their Tate modules are isomorphic. Let L be a Galois number field over which such an isogeny is defined. Consider the natural $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant inclusion

$$\mathrm{Hom}(R_{\overline{\mathbb{Q}}}, P_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}_p \hookrightarrow \mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}(V_p(R), V_p(P)). \tag{2}$$

By Ribet's proof of the Tate conjecture for modular abelian varieties [Rib80], the inclusion

$$\mathrm{Hom}(R_L, P_L) \otimes \mathbb{Q}_p \hookrightarrow \mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{Q}}/L)}(V_p(R), V_p(P)) \tag{3}$$

is an isomorphism, since there is an isogeny $P_L \to R_L$ and P is modular. But then (2) must also be an isomorphism, since (2) is the result of taking $\mathrm{Gal}(L/\mathbb{Q})$-invariants of both sides of (3).

By construction of P, there is an isomorphism $V_p(R) \cong V_p(P)$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules, so by (2) there is an isomorphism in $\mathrm{Hom}(R_{\mathbb{Q}}, P_{\mathbb{Q}}) \otimes \mathbb{Q}_p$. Thus there is a $\mathbb{Q}_p$-linear combination of elements of $\mathrm{Hom}(R_{\mathbb{Q}}, P_{\mathbb{Q}})$ that has nonzero determinant. However, if a $\mathbb{Q}_p$-linear combination of matrices has nonzero determinant, then some $\mathbb{Q}$-linear combination does, since the determinant is a polynomial function of the coefficients and $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Thus there is an isogeny $R \to P$ defined over $\mathbb{Q}$, so R is modular. □

Corollary 3.0.4. *Parts 1 and 2 of Conjecture 1.0.2 are true for every elliptic curve E over $\mathbb{Q}$.*

Proof. Suppose p is a prime, and let $\mathbb{Q}_{p^\infty}$ be the cyclotomic $\mathbb{Z}_p$ extension of $\mathbb{Q}$. By [BCDT01], E is a modular elliptic curve, so work of Rohrlich [Roh84], Kato [Kat04, Sch98], and Serre [Ser72] implies that $E(\mathbb{Q}_{p^\infty})$ is finitely generated (see [Rub98, Cor. 8.2]). Theorem 3.0.2 implies that if $x \in E(\mathbb{Q})$ and $m \mid \mathrm{order}(x)$, then x is m-visible relative to an optimal cover of E by a restriction of scalars B from an abelian extension. Then Proposition 3.0.3 implies that B is modular. □

4 The Visibility Dimension

The visibility dimension is analogous to the visibility dimension for elements of $\mathrm{H}^1(K, A)$ introduced in [AS02, §2]. We prove below that elements of order 2 in Mordell-Weil groups of elliptic curves over $\mathbb{Q}$ are 2-visible relative to an abelian surface. Along the way, we make a general conjecture about stability of rank and show that it implies a general bound on the visibility dimension.

Definition 4.0.5 (Visibility Dimension). Let A be an abelian variety over a number field K and suppose m is an integer. Then A has *m-visibility dimension n* if there is an optimal cover $B \to A$ with $n = \dim(B)$ and the image of $B(K)$ in $A(K)$ is contained in $mA(K)$, so $A(K)/mA(K)$ is a quotient of $\mathrm{Vis}^B(A(K))$.

The following rank-stability conjecture is motivated by its usefulness for proving a result about m-visibility.

Conjecture 4.0.6. *Suppose A is an abelian variety over a number field K, that L is a finite extension of K, and $m > 0$ is an integer. Then there is an extension M of K of degree m such that $\mathrm{rank}(A(K)) = \mathrm{rank}(A(M))$ and $M \cap L = K$.*

The following proposition describes how Conjecture 4.0.6 can be used to find an extension where the index of $A(K)$ in $A(M)$ is coprime to m.

Proposition 4.0.7. *Let A be an abelian variety over a number field K and suppose m is a positive integer. If Conjecture 4.0.6 is true for A and m, then there is an extension M of K of degree m such that $A(M)/A(K)$ is of order coprime to m.*

Proof. Choose a finite set $P_1, \dots, P_n$ of generators for $A(K)$. Let

$$L = K\left(\frac{1}{m}P_1, \dots, \frac{1}{m}P_n\right)$$

be the extension of K generated by *all* mth roots of each P_i. Since the set of mth roots of a point is closed under the action of $\mathrm{Gal}(\overline{K}/K)$, the extension L/K is Galois. Note also that the m torsion of A is defined over L, since the differences of conjugates of a given $\frac{1}{m}P_i$ are exactly the elements of $A[m]$. Let S be the set of primes of K that ramify in L.

By our hypothesis that Conjecture 4.0.6 is true for A and m, there is an extension M of K of degree m such that

$$\mathrm{rank}(A(K)) = \mathrm{rank}(A(M))$$

and $M \cap L = K$. In particular, $C = A(M)/A(K)$ is a finite group. Suppose, for the sake of contradiction, that $\gcd(m, \#C) \neq 1$, so there is some prime divisor $p \mid m$ and an element $[Q] \in C$ of exact order p. Here $Q \in A(M)$ is such that $pQ \in A(K)$ but $Q \notin A(K)$. Because $P_1, \dots, P_n$ generate $A(K)$ and $pQ \in A(K)$, there are integers $a_1, \dots a_n$ such that

$$pQ = \sum_{i=1}^{n} a_i P_i.$$

Then for any fixed choice of the $\frac{1}{p}P_i$, we have

$$Q - \sum_{i=1}^{n} a_i \cdot \frac{1}{p}P_i \in A[p],$$

since

$$p\left(Q - \sum_{i=1}^{n} a_i \cdot \frac{1}{p}P_i\right) = pQ - \sum_{i=1}^{n} a_i \cdot P_i = 0.$$

Thus $Q \in A(L)$. But then since $L \cap M = K$, so we obtain a contradiction from

$$Q \in A(L) \cap A(M) = A(K).$$

□

With Proposition 4.0.7 in hand, we show that Conjecture 4.0.6 bounds the visibility dimension of Mordell-Weil groups. In particular, we see that Conjecture 4.0.6 implies that for any abelian variety A over a number field K, and any m, there is an embedding $A(K)/mA(K) \hookrightarrow \mathrm{H}^1(K, C)$ coming from a δ map, where C is an abelian variety over K of rank 0.

Theorem 4.0.8. *Let A be an abelian variety over a number field K and suppose m is a positive integer. If Conjecture 4.0.6 is true for A and m, then there is an optimal covering $B \to A$ with B of dimension m such that*

$$\mathrm{Vis}^B(A(K)) \cong A(K)/mA(K).$$

Proof. By Proposition 4.0.7, there is an extension M of K of degree m such that the quotient $A(M)/A(K)$ is finite of order coprime to m. Then, as in [Ste04], the restriction of scalars $B = \mathrm{Res}_{M/K}(A_M)$ is an optimal cover of A and

$$\mathrm{Vis}^B(A(K)) \cong A(K)/\mathrm{Tr}(A(M)).$$

However, there is also an inclusion $A \hookrightarrow B$ from which one sees that

$$mA(K) \subset \mathrm{Tr}(A(M)),$$

so $\mathrm{Vis}^B(A(K))$ is an m-torsion group.

We have

$$[\mathrm{Tr}(A(M)) : \mathrm{Tr}(A(K))] \;\Big|\; [A(M) : A(K)].$$

We showed above that $\gcd([A(M) : A(K)], m) = 1$, so since

$$\mathrm{Tr}(A(M))/\mathrm{Tr}(A(K))$$

is killed by m, it follows that $\mathrm{Tr}(A(M)) = \mathrm{Tr}(A(K))$. We conclude that

$$\mathrm{Vis}^B(A(K)) = A(K)/mA(K).$$

□

Proposition 4.0.9. *If E is an elliptic curve over $\mathbb{Q}$ and $m = 2$, then Conjecture 4.0.6 is true for E and m.*

Proof. Let L be as in Conjecture 4.0.6, so L is an extension of $\mathbb{Q}$ of possibly large degree. Let D be the discriminant of L. By [MM97, BFH90] there are infinitely many quadratic imaginary extensions M of $\mathbb{Q}$ such that $L(E^M, 1) \neq 0$, where E^M is the quadratic twist of E by M. By [Kol91, Kol88] all these curves have rank 0. Since there are only finitely many quadratic fields ramified only at the primes that divide D, there must be some field M that is ramified at a prime $p \nmid D$. If M is contained in L, then all the primes that ramify in M divide D, so M is not contained in L. Since M is quadratic, it follows that $M \cap L = \mathbb{Q}$, as required. Since the image of $E(\mathbb{Q}) + E^M(\mathbb{Q})$ in $E(M)$ has finite index, it follows that $E(M)/E(\mathbb{Q})$ is finite. □

Corollary 4.0.10. *If E is an elliptic curve over $\mathbb{Q}$, then there is an optimal cover $B \to E$, with B a 2-dimension modular abelian variety, such that*

$$\mathrm{Vis}^B(E(\mathbb{Q})) \cong E(\mathbb{Q})/2E(\mathbb{Q}).$$

Proof. Combine Proposition 4.0.9 with Theorem 4.0.8. Also B is modular since it is isogenous to $E \times E'$, where E' is a quadratic twist of E. □

Note that the B of Corollary 4.0.10 is isomorphic to $(E \times E^D)/\Phi$, where E^D is a rank 0 quadratic imaginary twist of E and $\Phi \cong E[2]$ is embedded antidiagonally in $E \times E^D$. Note that E^D also has analytic rank 0, since it was constructed using the theorems of [Kol91, Kol88] and [MM97, BFH90]. Thus our construction is compatible with the one of Proposition 5.1.1 below.

5 Some Data About Visibility and Modularity

This section contains a computational investigation of modularity of Mordell-Weil groups of elliptic curves relative to abelian varieties that are quotients of $J_0(N)$. One reason that we restrict to $J_0(N)$ is so that computations are more tractable. Also, for $m > 2$, the twisting constructions that we have given in previous sections are no longer allowed since they take place in $J_1(N)$. Furthermore, the work of [KL89] suggests that we understand the arithmetic of $J_0(N)$ better than that of $J_1(N)$.

5.1 A Visibility Construction for Mordell-Weil Groups

The following proposition is an analogue of [AS02, Thm. 3.1] but for visibility of Mordell-Weil groups (compare also [CM00, pg. 19]).

Proposition 5.1.1. *Let E be an elliptic curve over a number field K, and let $\Phi = E[m]$ as a $\mathrm{Gal}(\overline{K}/K)$-module. Suppose A is an abelian variety over K such that $\Phi \subset A$, as $G_{\mathbb{Q}}$-modules. Let $B = (A \times E)/\Phi$, where Φ is embedded anti-diagonally. Then there is an exact sequence*

$$0 \to B(K)/(A(K) + E(K)) \to E(K)/mE(K) \to \mathrm{Vis}^B(E(K)) \to 0.$$

Moreover, if $(A/E[m])(K)$ is finite of order coprime to m, then the first term of the sequence is 0, so

$$\mathrm{Vis}^B(E(K)) \cong E(K)/mE(K).$$

Proof. Using the definition of B and multiplication by m on E, we obtain the following commutative diagram, whose rows and columns are exact:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & E[m] \arrow[r] \arrow[d] & E \arrow[r, "m"] \arrow[d] & E \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & E \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A/E[m] \arrow[r, "\cong"] \arrow[d] & B/E \arrow[r] \arrow[d] & 0 & \\
 & 0 & 0 & &
\end{tikzcd}$$

Taking K-rational points we arrive at the following diagram with exact rows and columns:

$$
\begin{tikzcd}
0 \arrow[r] & E(K)/E(K)[m] \arrow[r, "m"] \arrow[d] & E(K) \arrow[r] \arrow[d, "\cong"] & E(K)/mE(K) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & B(K)/A(K) \arrow[r] \arrow[d] & E(K) \arrow[r] \arrow[d] & \mathrm{Vis}^B(E(K)) \arrow[r] & 0 \\
& B(K)/(A(K)+E(K)) & 0 & &
\end{tikzcd}
$$

The snake lemma and the fact that the middle vertical map is an isomorphism implies that the right vertical map is a surjection with kernel isomorphic to $B(K)/(A(K)+E(K))$. Thus we obtain an exact sequence

$$0 \to B(K)/(A(K)+E(K)) \to E(K)/mE(K) \to \mathrm{Vis}^B(E(K)) \to 0.$$

This proves the first statement of the proposition. For the second, note that we have an exact sequence $0 \to E \to B \to A/E[m] \to 0$. Taking Galois cohomology yields an exact sequence

$$0 \to E(K) \to B(K) \to (A/E[m])(K) \to \cdots,$$

so $\#(B(K)/E(K)) \mid \#(A/E[m])(K)$. If $(A/E[m])(K)$ is finite of order coprime to m, then $B(K)/(A(K)+E(K))$ has order dividing $\#(A/E[m])(K)$, so the quotient $B(K)/(A(K)+E(K))$ is trivial, since it injects into $E(K)/mE(K)$. □

5.2 Tables

The data in this section suggests the following conjecture.

CONJECTURE 5.2.1. *Suppose E is an elliptic curve over $\mathbb{Q}$ and p is a prime such that $E[p]$ is irreducible. Then there exists infinitely many newforms $g \in S_2(\Gamma_0(N))$, for various integers N, such that $L(g,1) \neq 0$ and $E[p] \subset A_g$ and $\mathrm{Vis}^B(E(\mathbb{Q})) = E(\mathbb{Q})/pE(\mathbb{Q})$, where $B = (A_g \times E)/E[p]$.*

Let E be the elliptic curve $y^2 + y = x^3 - x$. This curve has conductor 37 and Mordell-Weil group free of rank 1. According to [Cre97], E is isolated in its isogeny class, so each $E[p]$ is irreducible.

Table 1 gives for each N the *odd* primes p such that there is a mod p congruence between f_E and some newform g in $S_2(\Gamma_0(37N))$ such that A_g has rank 0 and the isogeny class of A_g contains no abelian variety with rational p torsion. The first time a p occurs, it is in bold. We bound the torsion in the isogeny class using the algorithm from [AS05, §3.5] with primes up to 17. Thus by Proposition 5.1.1, the Mordell-Weil group of E is p-modular of level $37N$. A − means there are no such p. Table 2, which was derived directly from Table 1, gives for a prime p, all integers N such that $E(\mathbb{Q})$ is p-modular of level $37N$.

Table 1: Visibility of Mordell-Weil for $y^2 + y = x^3 - x$

N	$p's$	N	$p's$	N	$p's$	N	$p's$	N	$p's$	N	$p's$	N	$p's$
2	**5**	19	5	36	–	53	**53**	70	–	87	–	104	–
3	**7**	20	–	37	–	54	–	71	3, 7	88	–	105	–
4	–	21	7	38	5	55	–	72	–	89	**43**	106	5
5	–	22	–	39	–	56	–	73	3, 5	90	–	107	3, 5
6	–	23	**11**	40	–	57	–	74	–	91	3	108	–
7	**3**	24	–	41	3, 17	58	–	75	–	92	–	109	3, 7
8	–	25	–	42	–	59	**13**	76	–	93	7	110	–
9	–	26	–	43	7	60	–	77	–	94	–	111	–
10	–	27	3	44	–	61	5, 7	78	–	95	–	112	–
11	**17**	28	–	45	–	62	–	79	–	96	–	113	3, 11
12	–	29	3	46	–	63	3	80	–	97	**47**	114	–
13	–	30	–	47	3	64	–	81	3	98	–	115	–
14	–	31	3	48	–	65	–	82	–	99	–	116	–
15	–	32	–	49	–	66	–	83	3, 11	100	–	117	–
16	–	33	7	50	5	67	3, 5	84	–	101	3, 11	118	–
17	3	34	–	51	–	68	–	85	–	102	–	119	3
18	–	35	–	52	–	69	–	86	–	103	43	120	–

N	$p's$	N	$p's$	N	$p's$	N	$p's$	N	$p's$	N	$p's$
121	–	138	–	155	–	172	–	189	3	206	–
122	–	139	17	156	–	173	3, 5, 11	190	–	207	–
123	–	140	–	157	3, 5	174	–	191	7	208	–
124	–	141	–	158	–	175	–	192	–	209	–
125	5	142	–	159	–	176	–	193	5, 11		
126	–	143	–	160	–	177	–	194	–		
127	**127**	144	–	161	–	178	–	195	–		
128	–	145	–	162	–	179	3	196	–		
129	–	146	–	163	7, 13	180	–	197	3, 5, 13		
130	–	147	7	164	–	181	3, **59**	198	–		
131	3	148	–	165	–	182	–	199	3, 11		
132	–	149	5, **31**	166	–	183	–	200	–		
133	–	150	–	167	3, 5	184	–	201	–		
134	–	151	17	168	–	185	–	202	5		
135	–	152	–	169	–	186	–	203	3		
136	–	153	3	170	–	187	–	204	–		
137	3	154	–	171	–	188	–	205	–		

Table 2: Levels Where Mordell-Weil is p-Visible for $y^2 + y = x^3 - x$

p	N such that $37N$ is a level of p-modularity of $E(\mathbb{Q})$
3	7, 17, 27, 29, 31, 41, 47, 63, 67, 71, 73, 81, 83, 91, 101, 107, 109, 113, 119, 131, 137, 153, 157, 167, 173, 179, 181, 189, 197, 199, 203
5	2, 19, 38, 50, 61, 67, 73, 106, 107, 125, 149, 157, 167, 173, 193, 197, 202
7	3, 21, 33, 43, 61, 71, 93, 109, 147, 163, 191
11	23, 83, 101, 113, 173, 193, 199
13	59, 163, 197
17	11, 41, 139, 151
$19 - 29$	-
31	149
$37 - 41$	-
43	89, 103
47	97
53	53
59	181
$61 - 113$	-
127	127

Ribet's level raising theorem [Rib90] gives necessary and sufficient conditions on a prime N for there to be a newform g of level $37N$ that is congruent to f_E modulo p. Note that the form g is new rather than just p-new since 37 is prime and there are no modular forms of level 1 and weight 2. If, moreover, we impose the condition $L(g,1) \neq 0$, then Ribet's condition requires that p divides $N+1+\varepsilon a_N$, where ε is the root number of E. Since E has odd analytic rank, in this case $\varepsilon = -1$. For each primes $p \leq 127$ and each $N \leq 203$, we find the levels of such g. If f is a newform, the *torsion multiple* of f is a positive integer that is a multiple of the order of the rational torsion subgroup of any abelian variety attached to f, as computed by the algorithm in [AS05]. The *only* cases in which we don't already find a congruence level already listed in Table 2 corresponding to a newform with torsion multiple coprime to p are

$$p = 3, \quad N = 43 \qquad \text{and} \qquad p = 19, \quad N = 47, 79.$$

In all other cases in which Ribet's theorem produces a congruent g with $\mathrm{ord}_{s=1} L(g,s)$ even (hence possibly 0), we actually find a g with $L(g,1) \neq 0$ and can show that $\#A_g(\mathbb{Q})_{\mathrm{tor}}$ is coprime to p.

For $p = 3$ and $N = 43$ we find a unique newform $g \in S_2(\Gamma_0(1591))$ that is congruent to f_E modulo 3. This form is attached to the elliptic curve $y^2 + y = x^3 - 71x + 552$ of conductor 1591, which has Mordell-Weil groups $\mathbb{Z} \oplus \mathbb{Z}$. Thus this is an example of a congruence relating a rank 1 curve to a rank 2 curve. For $p = 19$ and $N = 47$, the newform g has degree 43, so A_g has dimension 43, we have $L(g,1) \neq 0$, but the torsion multiple is $76 = 19 \cdot 4$, which is divisible by 19. For $p = 19$ and $N = 79$, the A_g has dimension 57, we have $L(g,1) \neq 0$, but the torsion multiple is 76 again.

Tables 3–4 are the analogues of Tables 1–2 but for the elliptic curve $y^2+y = x^3 + x^2$ of conductor 43. This elliptic curve also has rank 1 and all mod p representations are irreducible. The primes p and N such that Ribet's theorem produces a congruent g with $\mathrm{ord}_{s=1} L(g,s)$ even, yet we do not find one with $L(g,1) \neq 0$ and the torsion multiple coprime to p are

$$p = 3, \quad N = 31, 61 \qquad \text{and} \qquad p = 11, \quad N = 19, 31, 47, 79.$$

The situation for $p = 11$ is interesting since in this case all the g with $\mathrm{ord}_{s=1} L(g,s)$ even fail to satisfy our hypothesis. At level $19 \cdot 43$ we find that g has degree 18 and $L(g,1) \neq 0$, but the torsion multiple is divisible by 11.

Let E be the elliptic curve $y^2 + y = x^3 + x^2 - 2x$ of conductor 389. This curve has Mordell-Weil group free of rank 2. Tables 5–6 are the analogues of Tables 1–2 but for E. The primes p and N such that Ribet's theorem produces a congruent g with $\mathrm{ord}_{s=1} L(g,s)$ even, yet we do not find one with $L(g,1) \neq 0$ and the torsion multiple coprime to p are

$$p = 3, \quad N = 17 \qquad \text{and} \qquad p = 5, \quad N = 19.$$

For $p = 3$, there is a unique g of level $6613 = 37 \cdot 17$ with $\mathrm{ord}_{s=1} L(g,s)$ even and $E[3] \subset A_g$. This form has degree 5 and $L(g,1) = 0$, so this is another

Table 3: Visibility of Mordell-Weil for $y^2 + y = x^3 + x^2$

N	$p's$	N	$p's$	N	$p's$	N	$p's$	N	$p's$	N	$p's$	N	$p's$
2	**5**	17	$3, \mathbf{7}$	32	–	47	–	62	–	77	–	92	–
3	**3**	18	–	33	3	48	–	63	–	78	–	93	–
4	–	19	–	34	5	49	–	64	–	79	–	94	–
5	5	20	–	35	–	50	5	65	–	80	–	95	–
6	–	21	–	36	–	51	3	66	–	81	3	96	–
7	–	22	5	37	19	52	–	67	**71**	82	–	97	$7, \mathbf{13}$
8	–	23	5	38	–	53	**59**	68	–	83	$3, \mathbf{23}$	98	–
9	–	24	–	39	3	54	–	69	–	84	–	99	3
10	–	25	–	40	–	55	5	70	–	85	5	100	–
11	3	26	–	41	**37**	56	–	71	$5, 7$	86	–		
12	–	27	3	42	–	57	3	72	–	87	3		
13	**19**	28	–	43	–	58	–	73	3	88	–		
14	–	29	3	44	–	59	3	74	–	89	**47**		
15	–	30	–	45	–	60	–	75	–	90	–		
16	–	31	–	46	–	61	5	76	–	91	–		

Table 4: Levels Where Mordell-Weil is p-Visible for $y^2 + y = x^3 + x^2$

p	N such that $43N$ is a level of p-modularity of $E(\mathbb{Q})$
3	3, 11, 17, 27, 29, 33, 39, 51, 57, 59, 73, 81, 83, 87, 99
5	2, 5, 22, 23, 34, 50, 55, 61, 71, 85
7	17, 71, 97
11	-
13	97
17	-
19	13, 37
23	83
$29, 31$	-
37	41
$41, 43$	-
47	89
53	-
59	53
$61, 67$	-
71	67

Table 5: Visibility of Mordell-Weil for $y^2 + y = x^3 + x^2 - 2x$

N	$p's$	N	$p's$	N	$p's$	N	$p's$	N	$p's$
1	**5**	7	3	13	**11**	19	–	25	–
2	–	8	–	14	–	20	–	26	–
3	–	9	3	15	3	21	–	27	3
4	–	10	–	16	–	22	–	28	–
5	**3**	11	–	17	–	23	5	29	3
6	–	12	–	18	–	24	–		

Table 6: Levels Where Mordell-Weil is p-Visible for $y^2 + y = x^3 + x^2 - 2x$

p	N such that $389N$ is a level of p-modularity of $E(\mathbb{Q})$
3	5, 7, 9, 15, 27, 29
5	1, 23
7	-
11	13

example where the rank 0 hypothesis of Proposition 5.1.1 is not satisfied. Note that the torsion multiple in this case is 1. For $p = 5$, there is a unique g of level $7391 = 37 \cdot 19$, with $\mathrm{ord}_{s=1} L(g, s)$ even and $E[5] \subset A_g$. This form has degree 4 and $L(g, 1) \neq 0$, but the torsion multiple is divisible by 5.

References

[Aga99a] A. Agashe, *On invisible elements of the Tate-Shafarevich group*, C. R. Acad. Sci. Paris Sér. I Math. 328 (1999), no. 5, 369–374. MR 1 678 131

[Aga99b] 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

[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* **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

[BFH90] D. Bump, S. Friedberg, and J. Hoffstein, *Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L-functions and their derivatives*, Ann. of Math. (2) 131 (1990), no. 1, 53–127.

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

[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

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997, `http://www.maths.nott.ac.uk/personal/jec/book/`.

[Dum01] N. Dummigan, *Congruences of modular forms and Selmer groups*, Math. Res. Lett. 8 (2001), no. 4, 479–494. MR MR1849264 (2002k:11064)

[DWS03] N. Dummigan, M. Watkins, and W. A. Stein, *Constructing Elements in Shafarevich-Tate Groups of Modular Motives*, Number theory and algebraic geometry, ed. by Miles Reid and Alexei Skorobogatov 303 (2003), 91–118.

[Fal86] G. Faltings, *Finiteness theorems for abelian varieties over number fields*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, Translated from the German original [Invent. Math. 73 (1983), no. 3, 349–366; ibid. 75 (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz, pp. 9–27. MR 861 971

[JS05] D. Jetchev and W. Stein, *Visibility of Shafarevich-Tate Groups at Higher Level*, in preparation.

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque (2004), no. 295, ix, 117–290, Cohomologies p-adiques et applications arithmétiques. III. MR MR2104361

[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).

[Kol88] V. A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and $Ш(E, \mathbf{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), no. 3, 522–540, 670–671. MR 89m:11056

[Kol91] V. A. Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990) (Tokyo), Math. Soc. Japan, 1991, pp. 429–436. MR 93c:11046

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

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

[Maz99] ______, *Visualizing elements of order three in the Shafarevich-Tate group*, Asian J. Math. 3 (1999), no. 1, 221–232, Sir Michael Atiyah: a great mathematician of the twentieth century. MR 2000g:11048

[Mil72] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. 17 (1972), 177–190. MR 48 #8512

[MM97] M. R. Murty and V. K. Murty, *Non-vanishing of L-functions and applications*, Birkhäuser Verlag, Basel, 1997.

[MO03] William J. McGraw and Ken Ono, *Modular form congruences and Selmer groups*, J. London Math. Soc. (2) 67 (2003), no. 2, 302–318. MR MR1956137 (2004d:11033)

[Rib80] K. A. Ribet, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. 253 (1980), no. 1, 43–62. MR 82e:10043

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

[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

[RM05] K. Rubin and B. Mazur, *Finding large selmer groups*, in preparation.

[Roh84] D. E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. 75 (1984), no. 3, 409–423. MR 86g:11038b

[Rub98] K. Rubin, *Euler systems and modular elliptic curves*, Galois representations in arithmetic algebraic geometry (Durham, 1996), Cambridge Univ. Press, Cambridge, 1998, pp. 351–367. MR 2001a:11106

[Sch98] A. J. Scholl, *An introduction to Kato's Euler systems*, Galois Representations in Arithmetic Algebraic Geometry, Cambridge University Press, 1998, pp. 379–460.

[Ser72] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), no. 4, 259–331.

[Sage07] W. Stein, *SAGE: Software for Algebra and Geometry Experimentation*, `http://www.sagemath.org/`.

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

[Tat66] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1965/66, pp. Exp. No. 306, 415–440.

[Wil00] A. J. Wiles, *The Birch and Swinnerton-Dyer Conjecture*, `http://www.claymath.org/prize_problems/birchsd.htm`.

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