William A. Stein ***Project Description***

(617) 308-0144 was@math.harvard.edu http://modular.fas.harvard.edu

1 Background

The proposed project reflects the interplay of abstract theory with explicit machine computation, as illustrated by the following quote of Bryan Birch [Bir71]:

> I want to describe some computations undertaken by myself and Swinnerton-Dyer on EDSAC by which we have calculated the zeta-functions of certain elliptic curves. As a result of these computations we have found an analogue for an elliptic curve of the Tamagawa number of an algebraic group; and conjectures (due to ourselves, due to Tate, and due to others) have proliferated.

The PI is primarily interested in abelian varieties attached to modular forms via Shimura's construction [Shi73], which we now recall. Let $f = \sum a_n q^n$ be a weight 2 newform on $\Gamma_1(N)$. Then f corresponds to a differential on the modular curve $X_1(N)$, which is a curve whose affine points over $\mathbf{C}$ correspond to isomorphism classes of pairs (E, P), where E is an elliptic curve and $P \in E$ is a point of order N. We view the Hecke algebra

$$\mathbf{T} = \mathbf{Z}[T_1, T_2, T_3, \ldots]$$

as a subring of the endomorphism ring of the Jacobian $J_1(N)$ of $X_1(N)$. Let I_f be the kernel of the homomorphism $\mathbf{T} \to \mathbf{Z}[a_1, a_2, a_3]$ that sends T_n to a_n, and attach to f the quotient

$$A_f = J_1(N)/I_f J_1(N).$$

Then A_f is a simple abelian variety over $\mathbf{Q}$ of dimension equal to the degree of the field $\mathbf{Q}(a_1, a_2, a_3, \ldots)$ generated by the coefficients of f. We also sometimes consider a similar construction with $J_1(N)$ replaced by the Jacobian $J_0(N)$ of the modular curve $X_0(N)$ that parametrizes isomorphism classes of pairs (E, C), where C is a cyclic subgroup of E of order N.

Definition 1 (Modular abelian variety). A *newform abelian variety* is an abelian variety over $\mathbf{Q}$ of the form A_f. An abelian variety over a number field is a *modular abelian varieties* if it is a quotient of $J_1(N)$ for some N.

Over $\mathbf{Q}$, newform abelian varieties are simple and every modular abelian variety is isogenous to a product of copies of newform abelian varieties. Newform abelian varieties are typically not absolutely simple.

Newform abelian varieties A_f are important. For example,the celebrated modularity theorem of C. Breuil, B. Conrad, F. Diamond, R. Taylor, and A. Wiles [BCDT01] asserts that every elliptic curve over $\mathbf{Q}$ is isogenous to some A_f. Also, J-P. Serre conjectures that, up to twist, every two-dimensional odd irreducible mod p Galois representation appears in the torsion points on some A_f.

Much of this research proposal is inspired by the following special case of the Birch and Swinnerton-Dyer conjecture:

(617) 308-0144 was@math.harvard.edu http://modular.fas.harvard.edu

Conjecture 2 (BSD Conjecture (special case)). *Let A be a modular abelian variety over $\mathbf{Q}$.*

1. *$L(A,1) = 0$ if and only if $A(\mathbf{Q})$ is infinite.*
2. *If $L(A,1) \neq 0$, then*

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

where the objects and notation in this formula are discussed below.

Here $L(A,s)$ is the L-series attached to A, which is entire because A is modular, so $L(A,1)$ makes sense. The real volume Ω_A is the measure of $A(\mathbf{R})$ with respect to a basis of differentials for the Néron model of A. For each prime $p \mid N$, the integer $c_p = \#\Phi_{A,p}(\mathbf{F}_p)$ is the *Tamagawa number* of A at p, where $\Phi_{A,p}$ denotes the component group of the Néron model of A at p. The dual of A is denoted $A^\vee$, and in the conjecture $A(\mathbf{Q})_{\mathrm{tor}}$ and $A^\vee(\mathbf{Q})_{\mathrm{tor}}$ are the torsion subgroups. The *Shafarevich-Tate group* of A is

$$Ш(A) = \mathrm{Ker}\left(\mathrm{H}^1(\mathbf{Q}, A) \to \bigoplus_{p \leq \infty} \mathrm{H}^1(\mathbf{Q}_p, A)\right),$$

which is a group that measures the failure of a local-to-global principle. When $L(A,1) \neq 0$, Kato proved in [Kat] that $Ш(A)$ and $A(\mathbf{Q})$ are finite, so $\#Ш(A)$ makes sense and one implication of part 1 of the conjecture is known.

Remark 3. The general Birch and Swinnerton-Dyer conjecture (see [Tat66, Lan91]) is a conjecture about any abelian variety A over a global field K. It asserts that the order of vanishing of $L(A,s)$ at $s=1$ equals the free rank of $A(K)$, and gives a formula for the leading coefficient of the Taylor expansion of $L(A,s)$ about $s=1$.

The rest of this proposal is divided into two parts. The first is about computing with modular forms and abelian varieties, and making the results of these computations available to the mathematical community. The second is about visibility of Mordell-Weil and Shafarevich-Tate groups, the ultimate goal being to obtain relationships between parts 1 and 2 of Conjecture 2.

2 Computing with modular forms

The PI proposes to continue developing algorithms and making available tools for computing with modular forms, modular abelian varieties, and motives attached to modular forms. This includes finishing a major new Magma [BCP97] package for computing directly with modular abelian varieties over number fields, extending the Modular Forms Database [Ste03a], and searching for algorithms for computing the quantities appearing in Conjecture 2 and in the Bloch-Kato conjecture for modular motives.

(617) 308-0144 was@math.harvard.edu http://modular.fas.harvard.edu

2.1 The Modular Forms Database

The Modular Forms Database [Ste03a] is a freely-available collection of data about objects attached to cuspidal modular forms. It is analogous to Sloane's tables of integer sequences, and extends Cremona's tables [Cre] to dimension bigger than one and weight bigger than two. Cremona's tables contain more refined data about elliptic curves than [Ste03a], but the PI intends to work with Cremona to make the modular forms database a superset of [Cre].

The database is used world-wide by prominent number theorists, including Noam Elkies, Matthias Flach, Dorian Goldfeld, Benedict Gross, Ken Ono, and Don Zagier.

The PI proposes to greatly expand the database. A major challenge is that data about modular abelian varieties of large dimension takes a huge amount of space to store. For example, the database currently occupies 40GB disk space. He proposes to find and implement a better method for storing information about modular abelian varieties so that the database will be more useful. He has found a method whereby a certain eigenvector is computed by the database server, which may (or may not!) enable storing coefficients of modular forms far more efficiently; however, he has not yet tried to implement it and study its properties.

The PI proposes to improve the usability of the database. It is currently implemented using a PostgreSQL database coupled with a Python web interface. To speed access and improve efficiency, he is considering rewriting key portions of the database using MySQL and PHP. He hopes to rewrite key portions of the database in response to user feedback that he has received. The database currently runs on a three-year-old 933Mhz Pentium III, which has unduly limited disk space and no offsite backup, so the PI is requesting a powerful modern computer with a large hard drive array and external hard drives for offsite backups.

2.1.1 MAGMA package for modular abelian varieties

The PI's software is published as part of the non-commercial Magma computer algebra system. The core of Magma is developed by a group of academics at the University of Sydney, who are supported mostly by grant money. Magma is considered by many to be the most comprehensive tool for research in number theory, finite group theory, and cryptography, and is widely distributed. The PI has already written over 400 pages (26000 lines) of modular forms code and extensive documentation that is distributed with Magma, and intends to "publish" future work in Magma.

As mentioned above, an abelian variety A over a number field K is *modular* if it is a quotient of $J_1(N)$ for some N. Modular abelian varieties were studied intensively by Ken Ribet, Barry Mazur, and others during recent decades, and studying them is popular because results about them often yield surprising insight into number theoretic questions. Computation with modular abelian varieties is

(617) 308-0144 was@math.harvard.edu http://modular.fas.harvard.edu

attractive because they are much easier to describe than arbitrary abelian varieties, and their L-functions are reasonably well understood when K is an abelian extension of $\mathbf{Q}$.

The PI recently designed and partially implemented a general system for computing with modular abelian varieties over number fields. He hopes to develop and refine several crucial components of the system. For example, three major problems arose, and the PI intends to resolve them in order to have a completely satisfactory system for computing with modular abelian varieties.

1. *Given a modular abelian variety A, efficiently compute the endomorphism ring* $\mathrm{End}(A)$ *as a ring of matrices acting on* $\mathrm{H}_1(A, \mathbf{Z})$. The PI has found a modular symbols solution that draws on work of Ribet [Rib80] and Shimura [Shi73], but it is too slow to be really useful in practice. In [Mer94], Merel uses Herbrand matrices and Manin symbols to give efficient algorithms for computing with Hecke operators. The PI intends to carry over Merel's method to give an efficient algorithm to compute $\mathrm{End}(A)$.

2. *Given* $\mathrm{End}(A) \otimes \mathbf{Q}$*, compute an isogeny decomposition of A as a product of simple abelian varieties.* This is a standard and difficult problem in general, but it might be possible to combine work of Allan Steel on his "characteristic 0 Meataxe" with special features of modular abelian varieties to solve it in practice. It is absolutely *essential* to solve this problem in order to explicitly enumerate all modular abelian varieties over $\overline{\mathbf{Q}}$ of given level N. Such an enumeration would be a major step towards the ultimate possible generalization of Cremona's tables [Cre] to modular abelian varieties. Computation of a decomposition is also crucial to other algorithms, e.g., computing complements and duals of abelian subvarieties.

3. *Given two modular abelian varieties over a number field K, decide whether there is an isomorphism between them.* When the endomorphism ring of each abelian variety is known and both are simple, it is possible to reduce this problem to the solution of a norm equation, which has been studied extensively in many cases. This problem is analogous to the problem of testing isomorphism for modules over a fixed ring, which has been solved with much effort for many classes of rings. One application is to proving that specific abelian varieties can not be principally polarized.

2.2 An Example: The Arithmetic of $J_1(p)$

We finish be describing recent work of the PI on the modular Jacobian $J_1(p)$, where p is a prime, that was partly inspired by computation. The following conjecture generalizes a conjecture of Ogg, which asserts that $J_0(p)(\mathbf{Q})_{\mathrm{tor}}$ is cyclic of order the numerator of $(p-1)/12$, a fact that Mazur proved in [Maz77].

(617) 308-0144 was@math.harvard.edu http://modular.fas.harvard.edu

Conjecture 4 (Stein). *Let p be a prime. The torsion subgroup of $J_1(p)(\mathbf{Q})$ is the group generated by the cusps on $X_1(p)$ that lie over $\infty \in X_0(p)$.*

The PI gives significant numerical evidence for this conjecture in [CES03], and cuspidal subgroups of $J_1(p)$ are considered in detail in [KL81], where, e.g., they compute orders of such groups in terms of Bernoulli numbers.

Mazur's proof of Ogg's conjecture for $J_0(p)$ is deep, though the proof for the odd part of $J_0(p)(\mathbf{Q})_{\text{tor}}$ is much easier. The PI intends to explore whether or not it is possible to build on Mazur's method and prove results towards Conjecture 4. The PI also intends to develop his computational methods for computing torsion subgroups in order to answer, at least conjecturally, the following question.

Question 5. If A_f is a quotient of $J_1(p)$ attached to a newform, is the natural map $J_1(p)(\mathbf{Q})_{\text{tor}} \to A_f(\mathbf{Q})_{\text{tor}}$ surjective? Is the product of the orders of all $A_f(\mathbf{Q})_{\text{tor}}$ over all classes of newforms f equal to $\#J_1(p)(\mathbf{Q})_{\text{tor}}$?

The PI conjectured that the analogous questions for $J_0(p)$ should have "yes" answers, and in [Eme01] M. Emerton proved this conjecture. There he also proved that the natural map from the component group of $J_0(p)$ to that of A_f is surjective. By [CES03], the component group of $J_1(p)$ is trivial, which suggests the following question.

Question 6. If A_f is a quotient of $J_1(p)$ attached to a newform, is the component group of A_f trivial?

Even assuming the full BSD conjecture (and a conjecture about a Manin constant), the PI has not yet produced enough data to give a conjectural answer to this question. He has many examples in which the conjecture predicts that either $Ш(A_f)$ is nontrivial or the component group of A_f is nontrivial. He and B. Poonen formulated, and hope to carry out, a strategy to decide which of these two is nontrivial by using an explicit description of $\text{End}(A_f/\overline{\mathbf{Q}})$ to obtain a curve whose Jacobian is A_f. Note that computing $\text{End}(A_f/\overline{\mathbf{Q}})$ in general is the second problem in Section 2.1.1 above.

3 Visibility

The underlying motivation for this part of the proposal is to prove implications between the two parts of Conjecture 2, in examples and eventually in some generality. That is, we link information about the first part of the BSD conjecture for an abelian variety B to information about the second part of the conjecture for a related abelian variety A. Visibility provides a conceptual framework in which to organize our ideas.

(617) 308-0144 was@math.harvard.edu http://modular.fas.harvard.edu

3.1 Computational problems

Barry Mazur introduced visibility in order to unify various constructions of Shafarevich-Tate groups.

Definition 7 (Visibility of Shafarevich-Tate Groups). Suppose that

$$\iota : A \hookrightarrow J$$

is an inclusion of abelian varieties over $\mathbf{Q}$. The *visible subgroup* of $\mathrm{H}^1(\mathbf{Q}, A)$ with respect to J is

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

The *visible subgroup* of $Ш(A)$ in J is the intersection of $Ш(A)$ with $\mathrm{Vis}_J\, \mathrm{H}^1(\mathbf{Q}, A)$; equivalently,

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

The terminology "visible" arises from the fact that if $x \in Ш(A)$ is visible in J, then a principal homogenous space X corresponding to x can be realized as a subvariety of J.

Before discussing theoretical questions about visibility, we describe computational evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties (and motives) that the PI and A. Agashe obtained using theorems inspired by the definition of visibility. In [AS02], the PI and Agashe prove a theorem that makes it possible to use abelian varieties of positive rank to explicitly construct subgroups of Shafarevich-Tate groups of other abelian varieties. The main theorem is that if A and B are abelian subvarieties of an abelian variety J, and $B[p] \subset A$, then, under certain hypothesis, there is an injection

$$B(\mathbf{Q})/pB(\mathbf{Q}) \hookrightarrow \mathrm{Vis}_J\, Ш(A).$$

The paper concludes with the first ever example of an abelian variety A_f attached to a newform, of large dimension (20), whose Shafarevich-Tate group has order that is provably divisible by an odd prime (5).

The PI has used the result described above to give evidence for the BSD conjecture for many $A \subset J_0(N)$, where A is attached to a newform of level $N \leq 2333$. The PI proposes to give similar evidence using visibility in $J_0(NM)$ for small M. More precisely, [AS] describes the computation of an odd divisor of the BSD conjectural order of $Ш(A)$ for over ten thousand $A \subset J_0(N)$ with $L(A, 1) \neq 0$ (these are *all* simple A with $N \leq 2333$ and $L(A, 1) \neq 0$). For over a hundred of these, the divisor of the conjectural order of $Ш(A)$ is divisible by an odd prime; for a quarter of these the PI and Agashe prove that if n is the conjectural divisor of the order of $Ш(A)$, then there are at least n elements of $Ш(A)$ that are visible in $J_0(N)$.

(617) 308-0144 was@math.harvard.edu http://modular.fas.harvard.edu

The PI intends to investigate the remaining 75% of the A with $n > 1$ by considering the image of A in $J_0(NM)$ for small integers M. Information about which M to choose can be extracted from Ribet's level raising theorem (see [Rib90]). As a test, the PI recently tried the first example with conjectural odd $Ш(A)$ that is not visible in $J_0(N)$ (this is an 18 dimensional abelian variety A of level 551 such that $9 \mid \#Ш(A)$). He showed in [Ste03b] that there are elements of order 3 in $Ш(A)$ that are visible in $J_0(551 \cdot 2)$. Since the dimension of $J_0(NM)$ grows very quickly, a huge amount of computer memory will be required to investigate visibility at higher level. Fortunately, the PI recently received a grant from Sun Microsystems for a $67,000 computer that contains 22GB of contiguously addressable RAM (the processors are relatively slow and the hard drive is small, making this computer less suitable as a platform for the modular forms database, which requires a large hard drive but not so much RAM).

Some of these ideas generalize to the context of Grothendieck motives, which A. Scholl attached to newforms of weight greater than two. N. Dummigan, M. Watkins, and the PI did work in this direction in [DWS03]. There we prove a theorem that can sometimes be used to deduce the existence of visible Shafarevich-Tate groups in motives attached to modular forms, assuming a conjecture of Beilinson about ranks of Chow groups. However, we give several pages of tables that suggest that Shafarevich-Tate groups of modular motives of level N are rarely visible in the higher-weight motivic analogue of $J_0(N)$, much more rarely than for weight 2. Just as above, the question remains to decide whether one expects these groups to be visible in the analogue of $J_0(NM)$ for some integer M. It would be relatively straightforward for the PI to do computations in this direction, and he intends to do so.

Before moving on to theoretical questions about visibility, we pause to emphasize that the above computational investigations into the Birch and Swinnerton-Dyer conjecture motivated the PI and others to develop new algorithms for computing with modular abelian varieties. For example, in [CS01], B. Conrad and the PI use Grothendieck's monodromy pairing to give an algorithm for computing orders of component groups of certain purely toric abelian varieties. This algorithm makes it practical to compute component groups of quotients A_f of $J_0(N)$ at primes p that exactly divide N. Without such an algorithm it would probably be difficult to get very far in computational investigations into the Birch and Swinnerton-Dyer conjecture for abelian varieties; indeed, the only other paper in this direction is [FpS$^+$01], which restricts to the case of Jacobians of genus 2 curves.

(617) 308-0144 was@math.harvard.edu http://modular.fas.harvard.edu

3.2 Theoretical problems

3.2.1 Visibility at higher level

Suppose A_f is a quotient of $J_1(N)$ attached to a newform and let $A = A_f^\vee \subset J_1(N)$ be its dual. One expects that most of $Ш(A)$ is *not* visible in $J_1(N)$. The following conjecture then arises.

Conjecture 8 (Stein). *For each $x \in Ш(A)$, there is an integer M and a morphism $f : A \to J_1(NM)$, of finite degree and coprime to the order of x, such that the image of x in $Ш(f(A))$ is visible in $J_1(NM)$.*

In [AS02], the PI proved that if $x \in \mathrm{H}^1(\mathbf{Q}, A)$, then there is an abelian variety B and an inclusion $\iota : A \to B$ such that x is visible in B; moreover, B is a quotient of $J_1(NM)$ for some M. This theorem is the main reason why the PI makes Conjecture 8. The PI hopes to prove Conjecture 8 by understanding the precise relationship between A, B, and $J_1(NM)$. First he will investigate explicitly the example with $N = 551$ described in Section 3.1 above.

A more analytical, and possibly deeper, approach to Conjecture 8 is to assume the rank statement of the Birch and Swinnerton-Dyer conjecture and relate when elements of $Ш(A)$ becoming visible at level NM to when there is a congruence between f and a newform g of level NM with $L(g, 1) = 0$. Such an approach leads one to try to formulate a refinement of Ribet's level raising theorem that includes a statement about the behavior of the value at 1 of the L-function attached to the form at higher level. The PI intends to do further computations in the hopes of finding a satisfactory conjectural refinement of Ribet's theorem, which he then hopes to subsequently prove.

The PI also proposes to investigate whether there is an M that is minimal with respect to some property, such that every element of $Ш(A)$ is simultaneously visible in $J_1(NM)$. This is well worth looking into, since the payoffs could be huge—the existence of such an M would imply finiteness of $Ш(A)$, since $\mathrm{Vis}_J(Ш(A))$ is always finite. Finiteness of $Ш(A)$ is a mysterious open problem when $L(A, 1) = 0$ and A is not a quotient of $J_0(N)$ with $\mathrm{ord}_{s=1} L(A, s) = \dim A$.

3.2.2 Visibility of Mordell-Weil groups

The Gross-Zagier theorem asserts that points on elliptic curves of rank 1 come from Heegner points, and that points on curves of rank bigger than one do not. It seems difficult to describe where points on elliptic curves of rank bigger than 1 "come from". The PI introduced the following definition, in hopes of eventually creating a framework for giving a conjectural explanation.

Definition 9 (Visibility of Mordell-Weil Groups). Suppose that $\pi : J \to A$ is a surjective morphism of abelian varieties with connected kernel. The *visible*

(617) 308-0144 was@math.harvard.edu http://modular.fas.harvard.edu

quotient of $A(\mathbf{Q})$ with respect to J (and π) is

$$\mathrm{Vis}^J(A(\mathbf{Q})) := \mathrm{Coker}(J(\mathbf{Q}) \to A(\mathbf{Q})).$$

Visibility of Mordell-Weil groups is closely connected to visibility of Shafarevich-Tate groups. If C is the kernel of π and $\delta : A(\mathbf{Q}) \to \mathrm{H}^1(\mathbf{Q}, C)$ is the connecting homomorphism of Galois cohomology, then δ induces an isomorphism

$$\tilde{\delta} : \mathrm{Vis}^J(A(\mathbf{Q})) \cong \mathrm{Vis}_J(\mathrm{H}^1(\mathbf{Q}, C)).$$

Note that this implies $\mathrm{Vis}^J(A(\mathbf{Q}))$ is finite. Let

$$\mathrm{Vis}^J_{Ш}(A(\mathbf{Q})) := \tilde{\delta}^{-1}(\mathrm{Vis}_J(Ш(C))).$$

Though we have introduced nothing fundamentally new, this different point of view suggested questions that seemed unnatural before, which inspired the following theorem and conjecture (the proof of the theorem relies on [Kat, Rub98] and [Roh84]):

Theorem 10 (Stein). *Let A be an elliptic curve. If $x \in A(\mathbf{Q})$ has order n (set $n = 0$ if x has infinite order), then for every divisor d of n, there is surjective morphism $J \to A$, with connected kernel, such that the image of x in $\mathrm{Vis}^J(A(\mathbf{Q}))$ has order d.*

Conjecture 11 (Stein). *Suppose A is a modular abelian variety and $x \in A(\mathbf{Q})$ has order n. For every divisor d of n there is a surjective morphism $J \to A$, with connected kernel, such that the image of x in $\mathrm{Vis}^J(A(\mathbf{Q}))$ lies in $\mathrm{Vis}^J_{Ш}(A(\mathbf{Q}))$ and has order d.*

We now describe partial results about this conjecture that the PI proved in [Ste04]. Suppose E is an elliptic curve over $\mathbf{Q}$ with conductor N, and let f be the newform attached to E. Fix a prime $p \nmid 2N \prod c_p$ such that the Galois representation $\mathrm{Gal}(\overline{\mathbf{Q}}) \to \mathrm{Aut}(E[p])$ is surjective.

Conjecture 12 (Stein). *There is a prime $\ell \nmid N$ and a surjective Dirichlet character $\chi : (\mathbf{Z}/\ell\mathbf{Z})^* \to \mu_p$ such that*

$$L(E, \chi, 1) \neq 0 \qquad \textit{and} \qquad a_\ell(E) \not\equiv \ell + 1 \pmod{p}.$$

According to Sarnak and Kowalski, this conjecture does not seem amenable to standard analytic averaging arguments. The PI has verified this conjecture for the elliptic curve of rank 1 and conductor 37 and all $p \leq 25000$. In almost all cases, the smallest $\ell \nmid N$ such that $a_\ell(E) \not\equiv \ell + 1 \pmod{p}$ and $\ell \equiv 1 \pmod{p}$ satisfies the conjecture.

The PI proved the following theorem in [Ste04].

(617) 308-0144 was@math.harvard.edu http://modular.fas.harvard.edu

Theorem 13 (Stein). *Let E be an elliptic curve over $\mathbf{Q}$ and suppose p and χ are as in Conjecture 12 above. Then there is an exact sequence $0 \to A \to J \to E \to 0$ that induces an exact sequence*

$$0 \to E(\mathbf{Q})/pE(\mathbf{Q}) \to Ш(A) \to Ш(J) \to Ш(E) \to 0.$$

In particular,

$$E(\mathbf{Q})/pE(\mathbf{Q}) \cong \mathrm{Vis}_{Ш}^{J}(E(\mathbf{Q})) \cong \mathrm{Vis}_{J}(Ш(A)).$$

We finish this research proposal by explaining how Theorem 13 may lead to a link between the two parts of the BSD Conjecture (Conjecture 2). Suppose E is an elliptic curve over $\mathbf{Q}$ and $L(E,1) = 0$. Then part 1 of Conjecture 2 asserts that $E(\mathbf{Q})$ is infinite. Under our hypothesis that $L(E,1) = 0$, a standard argument shows that

$$\frac{L(A,1)}{\Omega_A} \equiv 0 \pmod{p},$$

where A is as in Theorem 13. If part 2 of Conjecture 2 were true, there would be an element $x \in Ш(A)$ of order p (the proof of Theorem 13 rules out the possibility that p divides a Tamagawa number). If, in addition, x were visible in J, then $E(\mathbf{Q})$ would be infinite, since $E(\mathbf{Q})$ has no elements of order p. Part 2 of Conjecture 2 does not assert that x is visible in J, so one can only hope that a close examination of an eventual proof of part 2 of Conjecture 2 would yield some insight into whether or not x is visible. Alternatively, one could try to replace the isomorphism $E(\mathbf{Q})/pE(\mathbf{Q}) \cong \mathrm{Vis}_J(Ш(A))$ by an isomorphism

$$\mathrm{Sel}^{(p)}(E) \cong Ш(A)[I]$$

where I is an appropriate ideal in the ring $\mathbf{Z}[\mu_p]$ of endomorphism of A. Then an appropriate refinement of part 2 of Conjecture 2 might imply that $Ш(A)[I]$ contains an element of order p, which would imply that either $E(\mathbf{Q})$ is infinite or $Ш(E/\mathbf{Q})[p]$ is nonzero.

One can also work orthogonally to the above approach by investigating similar situations coming from level raising, where isomorphisms like the ones above may arise. The PI intends to investigate this cluster of ideas from various directions in hopes of finding a new perspective on where points on elliptic curves of rank bigger than one come from it.

(617) 308-0144 was@math.harvard.edu http://modular.fas.harvard.edu

References

[AS] A. Agashe and W. A. Stein, *Visible Evidence for the Birch and Swinnerton-Dyer Conjecture for Modular Abelian Varieties of Analytic Rank* 0, To appear in Math. of Computation.

[AS02] ———, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185. MR 2003h:11070

[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

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

[CES03] B. Conrad, S. Edixhoven, and W. A. Stein, $J_1(p)$ *Has Connected Fibers*, Documenta Mathematica **8** (2003), 331–408.

[Cre] J. E. Cremona, *Elliptic curves of conductor* ≤ 17000*,* `http://www.maths.nott.ac.uk/personal/jec/ftp/data/`.

[CS01] Brian Conrad and William A. Stein, *Component groups of purely toric quotients*, Math. Res. Lett. **8** (2001), no. 5-6, 745–766. MR 2003f:11087

[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.

[Eme01] M. Emerton, *Optimal Quotients of Modular Jacobians*, preprint (2001).

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

[Kat] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Preprint, 244 pages.

[KL81] D. S. Kubert and S. Lang, *Modular units*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science], vol. 244, Springer-Verlag, New York, 1981. MR 84h:12009

[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).

[Mer94] L. Merel, *Universal Fourier expansions of modular forms*, On Artin's conjecture for odd 2-dimensional representations, Springer, 1994, pp. 59–94.

[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.

[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

[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.

[Ste03a] W. A. Stein, *The Modular Forms Database*, `http://modular.fas.harvard.edu/Tables` (2003).

[Ste03b] ———, *Studying the Birch and Swinnerton-Dyer Conjecture for Modular Abelian Varieties Using MAGMA*, To appear in J. Cannon, ed., *Computational Experiments in Algebra and Geometry*, Springer-Verlag (2003).

[Ste04] ———, *Shafarevich-tate groups of nonsquare order*, Proceedings of MCAV 2002, 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.