# *William A. Stein* *Research Statement*

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

My research 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.*

This research statement is divided into three parts. The first is about computing with modular forms and abelian varieties. The second discusses techniques for understanding the arithmetic of elliptic curves and their higher-dimensional analogues, motivated by the Birch and Swinnerton-Dyer conjecture. The third is about making computations and tools available to the mathematical community.

## 1 Computing with Modular Forms

For several years I have developed algorithms and made available tools for computing with modular forms, modular abelian varieties, and motives attached to modular forms. I have written several packages that are included with MAGMA [BCP97] for computing with modular forms and abelian varieties and created the Modular Forms Database [Ste04a]. In this section I describe the current thrust of my research in this direction for a general audience of mathematicians. In Section 2, I will describe some more technical aspects of my research.

### 1.1 Background

An *elliptic curve* $E$ is a smooth projective curve of genus one with a distinguished point. Every such curve is naturally endowed with an abelian group structure, and moreover $E$ can even be defined by an equation of the form $y^2 = x^3 + ax + b$, where $x^3 + ax + b$ has distinct roots. When $a$ and $b$ are complex numbers, there is a lattice $L$ in the complex plane such that $E$ is isomorphic to the quotient group $\mathbf{C}/L$. This uniformization of $E$ is useful, but there is sometimes another uniformization that is extremely useful in number theory.

The $2 \times 2$ real matrices with determinant 1 act by linear fractional transformations on the *extended upper half plane* $\mathfrak{h} = \{z \in \mathbf{C} : \mathrm{Im}(z) > 0\} \cup \mathbf{Q} \cup \{i\infty\}$. Especially important for number theory is the action by the (noncommutative) group $\Gamma_1(N)$ of $2 \times 2$ matrices with integer entries and determinant 1 that are of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ modulo $N$. A celebrated theorem of Andrew Wiles et al. (see [BCDT01]), which implies Fermat'qs last theorem, is that if $E$ is an elliptic curve defined over $\mathbf{Q}$, then there is a surjective map of curves

$$\Gamma_1(N)\backslash\mathfrak{h} \to E,$$

where $\Gamma_1(N)\backslash\mathfrak{h}$ is the orbit space of $\mathfrak{h}$ under $\Gamma_1(N)$, viewed as a compact Riemann surface. Using differential forms on Riemann surfaces, we can produce a holomorphic function $f(z)$ on $\mathfrak{h}$ called a *weight* 2 *cuspidal modular eigenform.* The function $f(z)$ has a representation of the form

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \qquad q = e^{2\pi i z},$$

where the coefficients $a_n$ hold deep arithmetic information about the elliptic curve. In particular, $a_p = p + 1 - \#E(\mathbf{F}_p)$ for all but finitely many $p$. Thus modular forms arise as functions whose coefficients hold deep arithmetic significance.

For example, the curve $E$ defined by $y^2 + y = x^3 - x^2$ has associated form

$$f = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + q^5 + \cdots .$$

Note that $y^2 + y = x^3 - x^2$ can be transformed into the form $y^2 = x^3 + ax + b$ by completing the square. Notice that when $p = 2$,

$$p + 1 - \#E(\mathbf{F}_2) = 2 + 1 - 5 = -2$$

is the coefficient of $q^2$.

A few decades before Wiles's theorem, Goro Shimura gave a converse construction (see, e.g, [Shi73]) passing from certain modular forms $f$ to elliptic curves $E_f$. More generally, his construction associates to a larger class of modular forms certain more general objects than elliptic curves, which are abelian varieties.

**Definition 1 (Abelian Variety).** An *abelian variety* is a projective variety equipped with a group structure.

The group law on an abelian variety is necessarily abelian. Also, abelian varieties of dimension one are simply the elliptic curves.

Shimura's construction associates an abelian variety $A_f$ to certain modular cuspforms $f = \sum a_n q^n$ (they must be eigenvectors for certain operators called Hecke operators). The abelian variety $A_f$ is defined over $\mathbf{Q}$ and has dimension equal to the degree of the field $\mathbf{Q}(a_1, a_2, a_3, \ldots)$ generated by the coefficients of $f$. In particular, if $f$ has rational coefficients, then $A_f$ is an elliptic curve.

**Definition 2 (Modular Abelian Variety).** We say that an abelian variety $A$ over a number field $K$ is *modular* if there is a homomorphism (over $K$) with finite kernel from $A$ to a product of abelian varieties $A_f$.

There is a conjectural generalization of Wiles's theorem about modularity of elliptic curves to abelian varieties [Rib92, Thm. 4.4].

### 1.2 MAGMA: Packages for Modular Forms and Abelian Varieties

Much of my software is published as part of the non-commercial (but non-free) 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. I have already written over 25000 lines of modular forms code and extensive documentation that is distributed with MAGMA, and intend to "publish" future work in MAGMA. In addition to incremental improvements to the packages I've already written, I next hope to develop a satisfactory package for computing with modular abelian varieties over number fields.

As mentioned above, an abelian variety $A$ over a number field $K$ is modular if it admits a finite-degree map to a product of abelian varieties $A_f$. Modular abelian varieties were studied intensively by Ribet, 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 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 $\mathbf{Q}$.

I recently designed and implemented a general package for computing with modular abelian varieties over number fields. This package was made available as part of MAGMA version 2.11, but it is currently very limited at computations over fields other than $\mathbf{Q}$. I hope to develop and refine several crucial components of the system. For example, when computing with modular abelian varieties over number fields, three major problems arise, which I've enumerated below, and I hope to resolve them in order to have a completely satisfactory system for computing with modular abelian varieties. When the base field is $\mathbf{Q}$, I have solved (1) and (2) completely, and (3) in many cases.

1. *Given a modular abelian variety $A$ over a number field, efficiently compute the endomorphism ring* $\mathrm{End}(A)$ *as a ring of matrices acting on* $\mathrm{H}_1(A, \mathbf{Z})$. I have 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 Heilbronn matrices and Manin symbols to give efficient algorithms for computing with Hecke operators. I intend to carry over Merel's method to give an efficient algorithm to compute $\mathrm{End}(A)$.

2. *Let $K$ be a number field. Given an explicit description of* $\mathrm{End}(A/K) \otimes \mathbf{Q}$, *decompose $A$ as a product of simple abelian varieties over $K$.* The problem is to find a set of simple subvarieties $B_i$ over $K$ of abelian varieties $A_f$, such that there is a surjective finite-degree map from $A$ to the product of the $B_i$. This is likely a 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. Such an enumeration would be a major step towards the ultimate possible extension 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.

Once these foundations for computing with modular abelian varieties are in place, I hope to find an algorithm to enumerate all elements of the $\mathbf{Q}$-isogeny class of a modular abelian variety. This is something that can be done for elliptic curves, but the algorithms for elliptic curves use explicit equations like $y^2 = x^3 + ax + b$ and do not generalize to abelian varieties. However other techniques are available (e.g., drawing on David Helm's Ph.D. thesis), which might make enumeration of isogeny classes of abelian varieties possible.

### 1.3 A Snapshot of Other Current Projects

Here is a snapshot of some other projects I'm currently involved in:

1. Barry Mazur, John Tate, and I are *creating a package for computing cyclotomic $p$-adic height pairings* on elliptic curves over $\mathbf{Q}$ with good ordinary reduction at $p$, motivated by investigations into $p$-adic analogues of the BSD conjecture. The main obstruction to quickly computing $p$-adic cyclotomic heights to large precision is evaluating the $p$-adic modular form $E_2$ at an elliptic curve with good ordinary reduction. Nick Katz has pointed out that one might compute $E_2$ using explicit computations with Monsky-Washnitzer cohomology (following, e.g., [Ked03]). I have tried this idea and it worked fabulously, thus open many doors for other investigations.

2. Michael Stoll, Stephen Donnelly, Andrei Jorza, and Stefan Patrikis (a Harvard undergraduate), and I are attempting to *verify the full BSD conjecture for every elliptic curve of conductor at most* 25000 *and rank at most* 1. This involves refinement of Kolyvagin's Euler system with a view towards computational applications, and explicit computations on elliptic curves using MAGMA, and computational tools and tables of Cremona and others. I am responsible for general organization and programming.

3. Baur Bektemirov (a Harvard undergraduate) and I are computing surprising statistics about the massive (about 200 million curves) Stein-Watkins database of elliptic curves, which we intend to publish in *Experimental Mathematics*. We are also making the database easily available online.

4. Jennifer Balakrishnan (a Harvard undergraduate) and I are working on *developing methods for the sort of linear algebra over cyclotomic fields that arises in modular forms computations*. We hope to understand the paper [Abb89] on $p$-adic reconstruction of algebraic numbers, and apply it to computing rational canonical forms of matrices over cyclotomic fields.

5. I am working with Joan-Carlos Lario to create a *table of CM elliptic curves* over number fields. My primary input to the project is to use modular symbols to compute explicit Weierstrass equations attached to appropriate linear combinations of CM cuspforms.

## 2 Arithmetic of Elliptic Curves and Abelian Varieties

The underlying motivation for this part of my research is to prove implications between the two parts of the Birch and Swinnerton-Dyer Conjecture (see Conjecture 3 below), 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 $A$. The concept of visibility provides a conceptual framework in which to organize our ideas.

### 2.1 The Birch and Swinnerton-Dyer Conjecture

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

**Conjecture 3 (BSD Conjecture (special case)).** *Let $A$ be a modular abelian variety over $\mathbf{Q}$ (see Section 1.1), and let $L(A,s)$ be its L-function, which is an entire function of $s \in \mathbf{C}$.*

1. *$L(A,1) = 0$ if and only if the group $A(\mathbf{Q})$ is infinite.*

2. *If $L(A,1) \neq 0$, then*

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

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

This conjecture is striking because it asserts that the arithmetic behavior of an abelian variety is governed by properties of an analytic function near 1!

In the conjecture, $L(A,s)$ is the $L$-series attached to $A$, which is entire because $A$ is modular, so $L(A,1)$ makes sense. The real volume $\Omega_A$ 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. It is a major open problem to prove finiteness of this group in general. 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* 4. The general Birch and Swinnerton-Dyer conjecture (see [Tat66, Lan91]) is a conjecture about any abelian variety $A$ over a number field $K$ (or a function field of a curve over a finite field). 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 $L(A,s)$ at $s = 1$. Note that without the hypothesis that $A$ is modular and defined over $\mathbf{Q}$, we do not yet know in general that $L(A,s)$ makes sense near $s = 1$, though this is expected to be the case. Finally, in the case $\dim(A) = 1$ and $K = \mathbf{Q}$, the Clay Math Institute has announced a million dollar prize for a proof that the free rank of $A(\mathbf{Q})$ equals the order of vanishing of $L(A,s)$ at $s = 1$.

### 2.2 Visibility of Shafarevich-Tate Groups

Mazur introduced visibility in order to unify various constructions of Ш.

**Definition 5 (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 $Ш(A)$ 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 homogeneous 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 A. Agashe and I obtained by proving theorems inspired by the definition of visibility. In [AS02], Agashe and I 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.

**Theorem 6 (Agashe, Stein).** *If $A$ and $B$ are abelian subvarieties of an abelian variety $J$, and $B[p] \subset A$, then, under certain technical 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).

I have used the result described above to give evidence for the BSD conjecture for many modular abelian varieties $A$, attached to modular forms of level $N \leq 2333$. These modular forms have "trivial nebentypus", so the $A$ we consider sit naturally as subvarieties of the Jacobian $J_0(N)$ of a certain modular curve $X_0(N)$, which classifies pairs $(E, C)$, where $E$ is an elliptic curve and $C$ is a cyclic subgroup of $E$ of order $N$. More precisely, in [AS] Agashe and I describe the computation of an odd divisor of the BSD conjectural order of $Ш(A)$ for over ten thousand $A$ 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 Agashe and I 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 $J_0(N)$.

Dimitar Jetchev and I have been investigating 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, I 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 $9 \mid \#Ш(A)$). I showed in [Ste04c] 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 may be required to investigate visibility at higher level. (Fortunately, I received a grant from Sun Microsystems for a \$70K computer that contains 22GB of physical 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 I 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 me to do computations in this direction, and I intend 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 me and others to develop new algorithms for computing with modular abelian varieties. For example, in [CS01], B. Conrad and I use Grothendieck's monodromy pairing to give an algorithm for computing orders of component groups of certain purely toric abelian varieties. Computing these component groups is a crucial step in computing the Tamagawa numbers $c_p$ in the BSD Conjecture. Our 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.

### 2.3 Visibility at Higher Level

Suppose $A_f$ is a quotient of $J_0(N)$ attached to a newform and let $A = A_f^\vee \subset J_0(N)$ be its dual. One expects that most of $Ш(A)$ is *not* visible in $J_0(N)$. Data of Jetchev and I provides evidence for the following conjecture:

**Conjecture 7 (Stein).** *For each $x \in Ш(A)$, there is an integer $M$ and a morphism $f : A \to J_0(NM)$, of finite degree and coprime to the order of $x$, such that the image of $x$ in $Ш(f(A))$ is visible in $J_0(NM)$.*

A possible approach to Conjecture 7 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 has lead me to hope for a refinement of Ribet's level raising theorem [Rib90] that includes a statement about the behavior of the value at 1 of the $L$-function attached to the form at higher level. I intend to do further computations in the hopes of finding a satisfactory conjectural refinement of Ribet's theorem, which I hope to subsequently prove.

I also intend 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

$J_0(NM)$. This is well worth looking into, since the payoffs could be huge—the existence of such an $M$ would imply finiteness of $\text{Ш}(A)$, since $\mathrm{Vis}_J(\text{Ш}(A))$ is always finite. Finiteness of $\text{Ш}(A)$ is a mysterious open problem when $L(A,1)=0$ and $A$ is not a quotient of $J_0(N)$ with $\mathrm{ord}_{s=1} L(A,s) = \dim A$. Finiteness of $\text{Ш}(A)$ may be a key obstruction to finding a proof of the BSD Conjecture.

### 2.3.1 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". I introduced the following definition, in hopes of eventually creating a framework for giving a conjectural explanation.

**Definition 8 (Visibility of Mordell-Weil Groups).** Suppose that $\pi : J \to A$ is a surjective morphism of abelian varieties with connected kernel. The *visible quotient of* $A(\mathbf{Q})$ with respect to $J$ (and $\pi$) 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 $\pi$ and $\delta : A(\mathbf{Q}) \to \mathrm{H}^1(\mathbf{Q}, C)$ is the connecting homomorphism of Galois cohomology, then $\delta$ 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

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

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

**Theorem 9 (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 $d \mid n$, there is a surjective morphism $J \to A$, with connected kernel, such that the image of $x$ in $\mathrm{Vis}^J(A(\mathbf{Q}))$ has order $d$.*

**Conjecture 10 (Stein).** *Suppose $A$ is a modular abelian variety and $x \in A(\mathbf{Q})$ has order $n$. For every $d \mid n$ 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 $\mathrm{Vis}^J_{\text{Ш}}(A(\mathbf{Q}))$ and has order $d$.*

We now describe partial results about this conjecture that I proved in [Ste04b]. 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 11 (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. I have verified this conjecture for the elliptic curve of rank 1 and conductor 37 and all $p \leq 25000$. In most 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. I proved the following theorem in [Ste04b].

**Theorem 12 (Stein).** *Let $E$ be an elliptic curve over $\mathbf{Q}$ and suppose $p$ and $\chi$ are as in Conjecture 11 above. Then there is an exact sequence $0 \to A \to J \to E \to 0$ that induces an exact sequence*

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

*In particular,*

$$E(\mathbf{Q})/pE(\mathbf{Q}) \cong \mathrm{Vis}^J_{\text{Ш}}(E(\mathbf{Q})) \cong \mathrm{Vis}_J(\text{Ш}(A)).$$

We finish by explaining how Theorem 12 may lead to a link between the two parts of the BSD Conjecture (Conjecture 3). Suppose $E$ is an elliptic curve over $\mathbf{Q}$ and $L(E, 1) = 0$. Then part 1 of Conjecture 3 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 12. If part 2 of Conjecture 3 were true, there would be an element $x \in \text{Ш}(A)$ of order $p$ (the proof of Theorem 12 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 3 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 3 would yield some insight into whether or not $x$ is visible. Alternatively, one could try to replace the isomorphism $E(\mathbf{Q})/pE(\mathbf{Q}) \cong \mathrm{Vis}_J(\text{Ш}(A))$ by an isomorphism

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

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 3 might imply that $\text{Ш}(A)[I]$ contains an element of order $p$, which would imply that either $E(\mathbf{Q})$ is infinite or $\text{Ш}(E/\mathbf{Q})[p]$ is nonzero.

# 3 Infrastructure Development

## 3.1 MANIN: A Free Package for Computing with Modular Forms

I have been working intensely for several months to create a free and open program called MANIN for computing with modular forms and modular abelian varieties. MANIN is implemented in a hybrid of the object-oriented languages Python and C++. Python is easy to write and even easier to read, compiled C++ runs quickly and gives access to the number theory libraries NTL, LiDIA, and PARI, and interfacing Python with C++ is easy.

One reason I am creating MANIN is that MAGMA is expensive, hence many mathematicians are unable to use the software I write in MAGMA. A second reason is that most of MAGMA is closed source, so basic code that my modular forms computations rely on are (perhaps) not extensively documented and only available to a limited audience. For example, few people know in detail exactly how MAGMA computes the echelon form of a matrix with entries in the rationals. Finally MAGMA is complex, consisting of extensive package code that sits on top of over 2.3 million lines of C code.

I intend to write a book, *Algorithms for Computing With Modular Forms*, similar in spirit to Henri Cohen's book *Algorithms for Algebraic Number Theory.* This book will be based on my experiences implemented MANIN; as a starting point, I am now teaching a graduate course on computing with modular forms.

## 3.2 The Modular Forms Database

The Modular Forms Database [Ste04a] 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 abelian varieties of dimension bigger than one and modular forms of weight bigger than two. The database is used world-wide by prominent number theorists, including N. Elkies, M. Flach, D. Goldfeld, B. Gross, K. Ono, B. Poonen, and D. Zagier.

I intend 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 is currently a PostgreSQL/Python system that occupies 40GB of disk space. I intend to find and implement a better method for storing information about modular abelian varieties so that the database will be more useful. Fortunately, in July 2004 I received a $21,000 grant from NSF for computational equipment to store and make available the modular forms database.

I would like to improve the usability of the database. As a first step, I read about how Google works and created a much faster database [Ste04d] that uses Python, ZOPE, and ZODB and custom indexing code. I hope to greatly extend the current very-limited query facilities of this database in response to user feedback.

## References

[Abb89] J. Abbott, *Recovery of algebraic numbers from their p-adic approximations*, Proceedings of the ACM-SIGSAM 1989 international symposium on Symbolic and algebraic computation (1989), 112–120.

[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* **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* **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.

[Cre] J. E. Cremona, *Elliptic curves of conductor* $\leq 25000$,
`http://www.maths.nott.ac.uk/personal/jec/ftp/data/`.

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

[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.

[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.

[Ked03] K. S. Kedlaya, *Errata for: "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology" [J. Ramanujan Math. Soc.* **16**

*(2001), no. 4, 323–338*, J. Ramanujan Math. Soc. **18** (2003), no. 4, 417–418, Dedicated to Professor K. S. Padmanabhan. MR 2 043 934

[Lan91] S. Lang, *Number theory. III*, Springer-Verlag, Berlin, 1991, Diophantine geometry. MR 93a:11048

[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.

[Rib92] ______, *Abelian varieties over* **Q** *and modular forms*, Algebra and topology 1992 (Taejŏn), Korea Adv. Inst. Sci. Tech., Taejŏn, 1992, pp. 53–79. MR 94g:11042

[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.

[Ste04a] W. A. Stein, *The Modular Forms Database*, `http://modular.fas.harvard.edu/Tables` (2004).

[Ste04b] ______, *Shafarevich-Tate Groups of Nonsquare Order*, Modular Curves and Abelian Varieties, Progress of Mathematics (2004), 277–289.

[Ste04c] ______, *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 (2004).

[Ste04d] ______, *The ZOPE Modular Forms Database*, `http://modular.fas.harvard.edu/mfd` (2004).

[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.