William A. Stein *Project Description*

(206) 419-0925 wstein@uw.edu http://wstein.org

Explicit Approaches to Elliptic Curves and Modular Abelian Varieties

1 Introduction

Intellectual Merit: The projects in this proposal would generalize the highly influential tables of Cremona to the next (ordered by discriminant) totally real number field and to higher dimensional modular abelian varieties. This would improve on algorithms available for computing with elliptic curves and abelian varieties, and provide useful data and tools for number theory researchers. The proposed research would also advance techniques for constructing points and cohomology classes on elliptic curves, and for understanding the arithmetic of elliptic curves over number fields. This project would have as a concrete deliverable new publicly available tables and software that will be of use to many number theorists.

Broader Impact: The PI is co-authoring a popular expository book with Barry Mazur on the Riemann Hypothesis, co-authoring a graduate level book with Kenneth Ribet on modular forms and Hecke operators, and intends to release a new edition of his modular forms book [Ste07b]. The PI has tables of data that are freely available online, and whose creation has been supported by NSF FRG grant DMS-0757627, and the proposed research would expand these tables further. He will also continue to organize the development of the free open source NSF-funded Sage mathematical software project that he started (see [S$^+$11]). The PI organizes dozens of "Sage Days" workshops that involve many undergraduate and graduate students, and touch on number theory, algebraic topology, combinatorics, special functions, numerical computation, and other areas. The PI is also a co-PI on the UTMOST NSF grant (DUE-1020378), whose goal is to make Sage more accessible to high school and college teachers and students.

Overview: Section 2 is about generalizing many existing tables of elliptic curves over $\mathbf{Q}$ to the next totally real field, which is $\mathbf{Q}(\sqrt{5})$. Section 3 discusses creation of tables of Chow-Heegner points, numerical computation of triple product L-functions, and applications of such computations. Section 4 is about the problem of systematically enumerating all simple modular abelian varieties over $\mathbf{Q}$, problems about computing invariants of modular abelian varieties, computation of p-adic L-functions, and generalization of some of this to $\mathbf{Q}(\sqrt{5})$. Section 5 discusses determining the set of prime orders of torsion points on elliptic curves over all number fields of bounded degree. Section 6 involves application of congruences to studying visibility of Shafarevich-Tate groups and the use of Heegner points and congruences to construct cohomology classes on elliptic curves of rank at least 2.

(206) 419-0925 wstein@uw.edu http://wstein.org

1.1 Results from Prior NSF Support

The PI was partly supported by an NSF postdoctoral fellowship during 2000–2004 (DMS-0071576) in the amount of $90,000. The PI was awarded NSF grant DMS-0555776 (and DMS-0400386) from the ANTC program for the period 2004–2007. The PI has received a SCREMS grant (DMS-0821725) that supported purchasing computer hardware, an FRG (DMS-0757627), and two COMPMATH (DMS-0713225 and DMS-1015114) grants that support Sage development. He is currently a co-PI on a CCLI type 2 grant (DUE-1020378).

The PI was mainly supported by ANTC (DMS-0653968) for the period 2007–2010, and this is the award most closely related to this proposal, so we report in more detail about this award. It resulted in numerous published papers on the arithmetic of elliptic curves, modular forms and abelian varieties, including [JS07, BMSW07, KSW08, JLS09, SP10, Ste10, BS11], and one undergraduate number theory book [Ste09]. It also resulted in the submitted papers [SW10, Ste11, SW11] and the graduate level textbook [Ste07a] on the Birch and Swinnerton-Dyer conjecture.

2 Elliptic Curves over $\mathbf{Q}(\sqrt{5})$

Tables of Birch et al. from the 1970s [BK75], the book of Cremona [Cre97] and associated tables [Cre], and the Stein-Watkins tables of elliptic curves [SW02, BMSW07] have together had a profound impact on number theory. We propose to create comprehensive and easy-to-use tables, but over the field $\mathbf{Q}(\sqrt{5})$. Elliptic curves over totally real fields such as $\mathbf{Q}(\sqrt{5})$ are of particular current interest due to the plethora of extra structure (Heegner points, Zhang's formula, modularity results of Taylor, Kisin, Gee, Fujiwara, etc.) arising from Hilbert modular forms and Shimura curves. There are challenges over $\mathbf{Q}(\sqrt{5})$ that do not occur over $\mathbf{Q}$, for example: we do not know modularity in general; the complete list of degrees of isogenies is not yet known; there appears to be no good analogue of modular symbols in the case of even degree fields (see [GV10]); and canonical definitions, e.g., of global minimal models when they exist, are more subtle due to units.

The main challenges to generalizing tables to $\mathbf{Q}(\sqrt{5})$ are: (1) finding equations for all curves of given conductor, since unlike the case of elliptic curves over $\mathbf{Q}$, there is no known algorithm to do this in general; and (2) many algorithms for elliptic curves over number fields (such as $\mathbf{Q}(\sqrt{5})$) have only been incompletely implemented anywhere, and the existing implementations are sometimes orders of magnitude slower than the implementations over $\mathbf{Q}$.

(206) 419-0925 wstein@uw.edu http://wstein.org

Specific Goals:

1. Compute data about all elliptic curves over $\mathbf{Q}(\sqrt{5})$ of norm conductor up to 26,569 (smallest known norm conductor of a curve of rank 3), where the *norm conductor* is the absolute norm to $\mathbf{Q}$ of the conductor.
2. Create a Stein-Watkins style table of over a hundred million elliptic curves over $\mathbf{Q}(\sqrt{5})$ with norm conductor up to 10^8 and bounded discriminant.
3. Prove that every elliptic curve over $\mathbf{Q}(\sqrt{5})$ is modular, or at least carry out relevant computations that may be needed for this.

2.1 Enumeration and Creation of Tables

We give an outline of the main techniques for computing elliptic curves over $\mathbf{Q}(\sqrt{5})$. Many of these techniques were refined during a successful NSF-funded REU (DMS-0757627) that the PI ran during Summer 2011 at University of Washington, which resulted in a complete table of curves over $\mathbf{Q}(\sqrt{5})$ of norm conductor up to 1831. (The PI hopes to organize another REU on this topic during Summer 2012.)

Goal 1 is to create tables similar to Cremona's, but for all elliptic curves over $\mathbf{Q}(\sqrt{5})$ with conductor a given nonzero ideal $\mathcal{N}$ of the ring R of integers of $\mathbf{Q}(\sqrt{5})$.

1. **Enumerate Hilbert Modular Newforms:** Using arithmetic in the Hamilton quaternion algebra over $\mathbf{Q}(\sqrt{5})$, we compute a complete list of the Hilbert modular newforms of level $\mathcal{N}$ and weight $(2,2)$ with eigenvalues in $\mathbf{Q}$. The PI spent substantial time implementing a highly optimized algorithm for doing this, based on ideas from [Dem04] and J. Voight, but with many refinements. Nonetheless, there is still much room for improvement, especially in the sparse linear algebra part of the computation. Also, the PI is not satisfied with current algorithms for computing Hecke operators at bad primes yet in this setting. The PI estimates that it will be feasible to run this computation for all $\mathcal{N}$ with norm up to 200,000. Moreover, the implementation is efficient enough that it can compute the Hecke eigenvalues $a_{\mathfrak{p}}(f)$, for all $\mathfrak{p}$ with norm up to 50,000, in a few hours. The PI also proposes to enumerate non-rational newforms, which should correspond to certain abelian varieties over $\mathbf{Q}(\sqrt{5})$, and the PI intends to consider problems like those in Section 4 for these abelian varieties. Together with the "wide" tables of S. Donnelly and Voight of Hilbert modular forms over many fields, this data should provide a good resource for the community.
2. **Enumerate Weierstrass Equations:** To each rational Hilbert newform f found above, there should be an associated isogeny class of elliptic curves over $\mathbf{Q}(\sqrt{5})$ with L-series equal to $L(f,s)$. Though the PI knows of no algorithm in general that is guaranteed to compute some elliptic curve E in

(206) 419-0925 wstein@uw.edu http://wstein.org

this isogeny class, there are many *techniques* for finding E. The PI with his students and postdocs intends to fully implement and optimize the following techniques as part of this project:

- *Generalize Stein-Watkins:* efficiently enumerate Weierstrass equations of a certain form. This requires generalizing algorithms (see [SW02]) for computing minimal twists, conductors, and traces of Frobenius, and taking account of extra units (ongoing thesis work of Aly Deines).
- *Torsion families:* We can tell from several $a_{\mathfrak{p}}(f)$ whether some curve in the isogeny class is likely to have a torsion point of some order $n > 1$. If so, searching through curves with a torsion point of that order may yield the sought for curve. With input from Noam Elkies, one of the 2011 REU students (Ben LeVeque) wrote code to do this for many n.
- *Traces of Frobenius:* Fix some $a_{\mathfrak{p}}(f)$, and use the Chinese remainder theorem to search through curves with those $a_{\mathfrak{p}}(f)$, checking further when one is found with the right factors dividing its discriminant. The REU students (mainly R. Andrew Ohana) wrote highly optimized code to do this. We can modify this implementation to search for hundreds of curves at once with the same $a_{\mathfrak{p}}(f)$.
- *Special values:* Use Dembele's strategy (see [Dem05]), which involves computing mixed periods by computing special values of twists $L(f, \chi, s)$, where χ is a character of $\mathbf{Q}(\sqrt{5})$. During the summer 2011 REU, the postdoc Jon Bober explored and implemented this approach, and used it to find several new curves that had stumped all other methods.
- *Bad reduction:* Use the method of Cremona-Lingham (see [CL07]) to find many curves with good reduction outside the set of primes dividing $\mathcal{N}$. This relies on finding S-integral points on many auxiliary curves, and works well for certain $\mathcal{N}$, but less well for other $\mathcal{N}$. Also, use a similar (unpublished and less developed) effective method that Elkies came up with at Sage Days 22 that uses the λ-invariant and finding solutions to S-unit equations in number fields.
- *Congruences:* When f is congruent modulo 7 to a newform corresponding to a known elliptic curve of lower level, use [Fis11].

3. **Data about each curve:** There are algorithms and code for most of the steps below, but substantial work remains to make them efficient and robust enough to succeed at the goals listed above.

   (a) Enumerate all the curves in the isogeny class of E using the (surprising) algorithm of [Bil11] to find a finite list of possible degrees of isogenies, then Velu's formulas to write down the actual isogenies. This approach was implemented by Ashwath Rabindranath as part of the 2011 REU.
   (b) Compute lower and upper bounds on the rank (which eventually hopefully agree) and search for generators using (Denis Simon's) 2-descent,

then use the Silverman bound and a further search to saturate.

(c) Compute the invariants in the Birch and Swinnerton-Dyer formula, solve for the conjectural order of $Ш(E/\mathbf{Q}(\sqrt{5}))$, and check that the number we obtain is close to a perfect square.

(d) It would also be of interest to compute the degree of each Shimura curve parametrization of E; the PI intends to investigate whether there is an analytic algorithm like [Wat02] in this setting.

(e) If E has analytic rank ≤ 1, one can often compute a nonzero Heegner point on E and obtain an explicit upper bound on $\#Ш(E/\mathbf{Q}(\sqrt{5}))$ from work of Zhang [Zha01, Zha04]. This was done by Ashwath Rabindranath as part of the summer 2011 REU; he worked with a curve of norm conductor 31 and used Zhang's height formula, which proved in this case that $\#Ш(E/\mathbf{Q}(\sqrt{5})) = 1$. This is an extension to $\mathbf{Q}(\sqrt{5})$ of [GJP+09, Mil10, MS11].

2.2 Modularity

The PI has written only published paper [BS02] on modularity of Galois representations. However, this elliptic curve enumeration project would greatly benefit if we knew modularity of elliptic curves over $\mathbf{Q}(\sqrt{5})$. The PI asked R. Taylor about this problem, and Taylor explained how current results likely prove modularity over any abelian (over $\mathbf{Q}$) totally real field in which 3 and 5 are not ramified.

> *Taylor, May 2011, personal communication:* "Suppose E is an elliptic curve over an abelian totally real field F. By [Kis09, Thm. 3.5.7], as extended by [Gee06], if $E[3]_{|_{G_{F(\zeta_3)}}}$ is absolutely irreducible then E is modular (by the usual argument using Langlands-Tunnell). Using the 3-5 trick this also tells us that E is modular if F does not contain $\sqrt{5}$ and $E[5]_{|_{G_{F(\zeta_5)}}}$ is absolutely irreducible. It may be possible to remove the condition that $\sqrt{5} \notin F$. If so, one is left to examine elliptic curves E/F with both $E[3]_{|_{G_{F(\zeta_3)}}}$ and $E[5]_{|_{G_{F(\zeta_5)}}}$ absolutely reducible. These all correspond to F-rational points on certain modular curves (see e.g., [CDT99, Lem. 7.2.3]). For $F = \mathbf{Q}$ there are finitely many such elliptic curves, but some of the modular curves are genus 1, so over a general totally real F might have infinitely many points. Also, F. Calegari has observed that one can make use of the prime 7 using an idea of Jayanta Manoharmayum's, which should allow for somewhat stronger results."

Thus the PI intends to consider the curves of [CDT99, Lem. 7.2.3] over $\mathbf{Q}(\sqrt{5})$.

(206) 419-0925 wstein@uw.edu http://wstein.org

3 Chow-Heegner Points

Chow-Heegner points, as are being actively pursed by Darmon, Rotger, et al., are quite general. We consider a special case that has a simple concrete description due to Shouwu Zhang (see [Tao]). Fix an elliptic curve E over $\mathbf{Q}$. Suppose F is any other elliptic curve over $\mathbf{Q}$ that is not isogenous to E. Let N be the least common multiple of the conductors of E and F, and fix choices of minimal modular parameterization maps $\phi_E : X_0(N) \to E$ and $\phi_F : X_0(N) \to F$ that take the cusp ∞ to the zero point of each curve. Choose a point $t \in F(\mathbf{C})$ that is unramified for the map ϕ_F. Define a rational point $P \in E(\mathbf{Q})$ by $P = P_{E,F} = \sum_{z \in \phi_F^{-1}(t)} \phi_E(z)$, where the sum uses the group law on E. The point P does not depend on the choice of t, since there is no nonzero morphism $F \to E$.

Example 3.1. Let E be 37a and F be 37b. Then $P = (6, 14)$ and $[E(\mathbf{Q}) : \mathbf{Z}P] = 6$. This follows from [MSD74, Prop. 3, pg. 30]; in addition, they remark: *"It would be of the utmost interest to link this index to something else in the theory."*

There is an analogue of the Gross-Kudla triple product L-function formula [GK92]; this analogue gives the height of P in terms of other L-values. It is a generalization of the Gross-Zagier formula, but with the ring class character replaced by an elliptic curve. It implies that the above construction can only produce points of infinite order when $\mathrm{ord}_{s=1} L(E, s) = 1$.

Specific Goals:

1. Compute a table of Chow-Heegner points $P = P_{E,F} \in E(\mathbf{Q})$ for all pairs (E, F) of elliptic curves over $\mathbf{Q}$ of equal conductor less than 1000.
2. Compute the corresponding triple product L-functions for the pairs above. (The PI has extensive experience with Dokchitser's method [Dok04] for numerically computing L-functions.)
3. More generally, numerically compute the triple product L-functions for many pairs of newforms f, g that we can compute to sufficient precision.
4. Compute tables of Chow-Heegner points associated to (E, F), but with F varying in a family of quadratic twists.

3.1 Numerical Computation of Chow-Heegner Points

As a result of discussions with S. Zhang, X. Yuan, Darmon, and Rotger, the PI has refined and implemented a numerical method for computing the point $P = P_{E,F}$ defined above; a first report on this work will appear as an appendix to [DDLR11]. The primary goal of the proposed project is not provable correctness of results, but instead flexible and easy-to-understand code that efficiently produces a likely correct result, which will provide helpful data, e.g., to those generalizing

(206) 419-0925 wstein@uw.edu http://wstein.org

the Heegner-Gross-Zagier-Kolyvagin machinery to this setting. It also provides a double check on the afformentioned other work to compute Chow-Heegner points.

Assume for simplicity that E and F have the same conductor. Our numerical strategy is partly inspired by work of Delaunay [Del02].

1. Choose a random (probably) transcendental point $t \in \mathbf{R}/\Omega_F \subset F(\mathbf{R})$.
2. For some B, e.g., 2000, numerically compute all double precision complex solutions to the real polynomial equation $\sum_{n=1}^{B} \frac{a_n(F)}{n} q^n = t$ using balanced-QR reduction of the companion matrix (implemented in [GSL11]). As necessary, repeat this and the following steps with integer multiples of Ω_F added to t.
3. Using Newton-Raphson, and a much larger choice of B that depends on the imaginary part of each root, numerically refine the roots to large precision.
4. Divide the roots in the upper half plane into $\Gamma_0(N)$ orbits. If the number of orbits equals the modular degree of F, map representatives (with largest imaginary parts) to E using $\sum_{n=1}^{B'} \frac{a_n(E)}{n} q^n$, for B' sufficiently large. Then sum up the result and apply the elliptic exponential to obtain a numerical approximation to the point $P = P_{E,F} \in E(\mathbf{Q})$.
5. Simultaneously, as we find roots in Step 3, map them to $E(\mathbf{C})$, and if we find enough distinct images, add them up to obtain P. By "enough", we require that the number of images equals the generic cardinality $m_{E,F}$ of the map $R \mapsto \pi_E(\pi_F^{-1}(R))$. Of course, $m_{E,F}$ is bounded by the modular degree of F, but it will be strictly smaller in many cases, e.g., if some Atkin-Lehner involution fix both E and the fiber $\pi_F^{-1}(R)$. The PI intends to more fully understand the invariant $m_{E,F}$; initial numerical data shows that the "obvious guess" about how to compute it is right in many but not all cases.

There are numerous subtle parameters in the above strategy. Also, aspects of the strategy are useful for other investigations. For example, computing information about the points on $X_0(N)$ over points on higher rank curves (see [Del02]).

The PI's current implementation can do many examples with conductor up to a few hundred in a few seconds each, but there are cases, e.g., when the modular degree of F is large, where it can take many hours.

Similar results can be obtained, with different complexity, using (1) the iterated integral formalism of Darmon et al. mentioned above (see [DDLR11]), and hopefully (2) by using a new formula of Yuan-Zhang-Zhang [YZZ11] and numerical computation of triple product L-series to compute the height of $P_{E,F}$ without computing $P_{E,F}$. The PI's initial investigations reveal that the conductors of the relevant triple product L-series are enormous, which makes (2) challenging, but not impossible, from a purely computational perspective.

(206) 419-0925 wstein@uw.edu http://wstein.org

3.2 The Triple Product Formula

Let f_1, f_2, f_3 be three newforms of weight 2. Consider the degree 8 triple product L-function $L(s, f_1, f_2, f_3)$ of [GK92], normalized so $1/2$ is the center of the critical strip. Assume $\varepsilon(1/2) = -1$. Let $\Sigma = \{v : \varepsilon_v(1/2) = -1\}$ which includes ∞, and assume $\#\Sigma$ is odd. When $\Sigma = \{\infty\}$ let X be a modular curve $X_0(N)$, with N divisible by the levels of all the f_i. Otherwise, let X be an appropriate Shimura curve associated to the definite quaternion algebra over $\mathbf{Q}$ ramified at $\Sigma - \{\infty\}$.

Now suppose the f_i correspond to optimal elliptic curves E_i. We have a map $X \to E_1 \times E_2 \times E_3$. Suppose moreover that $\varepsilon_p(1/2) = 1$ for all finite p, so that $\Sigma = \{\infty\}$, hence $X = X_0(N)$. Let $\overline{\Delta}_{\mathrm{mod}} \in \mathrm{CH}^2(E_1 \times E_2 \times E_3)_0$ be the cohomologically trivial modified version of the diagonal $\Delta \subset X \times X \times X$.

Theorem 3.2 (Yuan,Zhang,Zhang)**.** *$L'(1/2, f_1, f_2, f_3) = (*) \cdot \langle \overline{\Delta}_{\mathrm{mod}}, \overline{\Delta}_{\mathrm{mod}} \rangle_{\mathrm{BB}}$, where the pairing is the Beilinson-Bloch height pairing, and (*)> 0 is "harmless".*

As part of this project we will, of course, have to nail down (*) explicitly. Now suppose $f_2 = f_3$ and the f_i correspond to elliptic curves. First,

$$L(s, f_1, f_2, f_3) = L(s, f_1) \cdot L(s, f_1, \mathrm{Sym}^2 f_2).$$

Also, let P be the Chow-Heegner point defined above. We have $\langle \overline{\Delta}_{\mathrm{mod}}, \overline{\Delta}_{\mathrm{mod}} \rangle_{\mathrm{BB}} = \langle P, P \rangle_{\mathrm{NT}}$, so $(L(s, f_1) \cdot L(s, f_1, \mathrm{Sym}^2 f_2))'|_{s=\frac{1}{2}} = (*)\langle P, P \rangle_{\mathrm{NT}}$.

Now assume that $\varepsilon(f_1) = -1$. Then

$$L'(1/2, f_1) \cdot L(1/2, f_1, \mathrm{Sym}^2 f_2) = (*) \cdot \langle P, P \rangle_{\mathrm{NT}}. \tag{1}$$

This is analogous to the Gross-Zagier formula, which is

$$L'(1/2, f_1) \cdot L(1/2, f_1, \eta_\chi) = (*) \cdot \langle P_K, P_K \rangle_{\mathrm{NT}}, \tag{2}$$

where η_χ is the theta series corresponding to a quadratic character, and K is the corresponding quadratic field.

3.3 Applications

Extensive numerical data about Chow-Heegner points may provide insight about some questions. When P_K is the Heegner point corresponding to K, the sum $\sum \langle P_K, P_K \rangle q^D$ is a modular form of weight $3/2$. Assume that $E(\mathbf{Q})$ is of rank 1.

Question 3.3 (Asked to the PI by X. Yuan)**.** Is there a parametrization of elliptic curves F so that the points $P = P_{E,F}$ fit into a generating function that is a modular form of some type?

Question 3.4. The gcd of $[E(\mathbf{Q}) : \mathbf{Z}P_K]$ over all K is expected to be $\sqrt{\#Ш(E/\mathbf{Q})} \cdot \prod c_p$. Is there an analogue of this for the indexes $[E(\mathbf{Q}) : \mathbf{Z}P_{E,F}]$? In particular, Gross-Zagier and Kolyvagin's work connect the index $[E(K) : \mathbf{Z}P_K]$ to $\sqrt{\#Ш(E/K)} \cdot \prod c_p$. We speculate that there is a similar relationship between $[E(\mathbf{Q}) : \mathbf{Z}P_{E,F}]$ and the arithmetic of the motive $\mathcal{M}$ attached to $L(s, f_1, \mathrm{Sym}^2 f_2)$. This would address the question of Mazur–Swinnerton-Dyer raised in Example 3.1.

4 Modular Abelian Varieties

Specific Goals:

1. Compute $J_0(N)(\mathbf{Q})_{\mathrm{tor}}$ and $J_1(N)(\mathbf{Q})_{\mathrm{tor}}$ when they are cuspidal, for as many N as we can. Are they always cuspidal?
2. Make a conjecture about the extent to which torsion on modular Jacobians is cuspidal, and investigate generalizing results of [Maz77].
3. Find an algorithm that given a newform $f \in S_2(\Gamma_0(N))$, outputs a complete list of representative abelian varieties in the isogeny class of A_f.
4. Create a table of all $\mathbf{Q}$-simple modular abelian variety factors of $J_0(N)$ over $\mathbf{Q}$ for $N \leq 1{,}000$, and a similar table for $J_1(N)$.
5. Formulate a generalization to higher dimensional abelian varieties of the p-adic analogue of the Birch and Swinnerton-Dyer conjecture.
6. Attempt to extend to $\mathbf{Q}(\sqrt{5})$ the algorithm from [CS01] for computing Tamagawa numbers of purely toric modular abelian varieties.

4.1 Torsion

The PI made the following conjecture in [CES03, Conj. 6.2]:

Conjecture 4.1. *For every prime p, the group $J_1(p)(\mathbf{Q})_{\mathrm{tor}}$ is generated by the differences of cusps on $X_1(p)$ over the cusp ∞ of $X_0(p)$; equivalently, $\#J_1(p)(\mathbf{Q})_{\mathrm{tor}} = \frac{p}{2^{p-3}} \prod_{\varepsilon \neq 1} B_{2,\varepsilon}$, where the product is over even Dirichlet characters of conductor p.*

In [CES03], the PI verified the above conjecture for all primes $p \leq 157$, except for $p \in S = \{29, 97, 101, 109, 113\}$. He did this by using modular symbols to compute the characteristic polynomials of Hecke operators, hence of Frobenius, hence compute $\#J_1(p)(\mathbf{F}_\ell)$ for many ℓ, and deduced a multiple of $\#J_1(p)(\mathbf{Q})_{\mathrm{tor}}$. For any modular Jacobian J, there is the following more refined (and initially much slower) approach to computing a group that contains $J(\mathbf{Q})_{\mathrm{tor}}$. For $\ell \nmid N$, let

$$\eta_\ell = T_\ell - (1 + \langle \ell \rangle \ell) \in \mathrm{End}(J),$$

(206) 419-0925 wstein@uw.edu http://wstein.org

where $\langle \ell \rangle$ is the diamond bracket operator. Using the Eichler-Shimura relation, we see that $J(\mathbf{Q})_{\mathrm{tor}} \subset J[\eta_\ell]$. Let C be the subgroup of $J(\overline{\mathbf{Q}})_{\mathrm{tor}}$ generated by differences of cusps, and I the ideal generated by η_ℓ for all ℓ.

Question 4.2. Is it always the case that $J[I] \subset C$?

The PI has an algorithm to answer Question 4.2 in any particular case. Also, [Ste82] computes the action of $G_{\mathbf{Q}}$ on C, so one can compute $C(\mathbf{Q})$. Thus when $J[I] \subset C$, we have an algorithm to compute $J(\mathbf{Q})_{\mathrm{tor}} = C(\mathbf{Q})$. The PI arrived at this approach in joint work with Loïc Merel in Summer 2010.

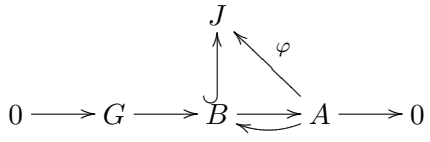
Applications:

- Computing $J_1(29)(\mathbf{Q})_{\mathrm{tor}}$ was needed to efficiently rule out the existence of a 29-torsion point on an elliptic curve over quartic field (see Section 5).
- If we can compute $J(\mathbf{Q})_{\mathrm{tor}}$, then it is straightforward to compute $A_f(\mathbf{Q})_{\mathrm{tor}}$ for each abelian variety $A_f \subset J$ attached to a newform using a straightforward application of the representation in Section 4.2.
- Complete understanding of Question 4.2 in the case of $J_0(p)$ was one of the main contributions of the landmark paper of Mazur [Maz77], and it would be useful to have at least a conjectural sense of how that result extends.
- Determining $J_0(N)(\mathbf{Q})_{\mathrm{tor}}$ for various composite N arises in recent unpublished work of Elkies on computing certain Shimura curves.

4.2 Enumeration

A simple abelian variety A over $\mathbf{Q}$ is *of* GL_2*-type* if $\mathrm{End}(A) \otimes \mathbf{Q}$ is a number field of degree $\dim(A)$. A theorem of Ribet [Rib92] combined with the proof of Serre's conjecture [KW08] implies that every GL_2-type abelian variety over $\mathbf{Q}$ is a quotient of $J_1(N)$ for some N (and conversely). The main goal of this project to generalize some aspects of Cremona's tables of elliptic curves to higher dimension. First we need to find an algorithm for enumerating all simple GL_2-type abelian varieties over $\mathbf{Q}$. The algorithms discussed in this section do not make any use of defining polynomial equations, so they allow us to treat all dimensions uniformly, reducing most questions to problems of linear algebra and module theory.

We represent modular abelian varieties over $\mathbf{Q}$ *explicitly* as follows. For simplicity, assume $J = J_0(N)$ for some N, though everything generalizes. Fix a modular abelian variety A and a finite degree homomorphism $\varphi : A \to J$. Then there is an isogeny from the image $B = \varphi(A) \subset J$ back to A whose kernel we denote by G, so A is isomorphic to B/G and $B \subset J$:



(206) 419-0925 wstein@uw.edu http://wstein.org

It remains to explain how we specify $G \subset B \subset J$.

We specify B as follows. The inclusion $B \hookrightarrow J$ induces an inclusion of rational homology $\mathrm{H}_1(B, \mathbf{Q}) \hookrightarrow \mathrm{H}_1(J, \mathbf{Q})$ and B is determined by the image V of $\mathrm{H}_1(B, \mathbf{Q})$ in the $\mathbf{Q}$-vector space $\mathrm{H}_1(J, \mathbf{Q})$. We explicitly compute a basis for $\mathrm{H}_1(J, \mathbf{Z})$ and $\mathrm{H}_1(J, \mathbf{Q}) = \mathrm{H}_1(J, \mathbf{Z}) \otimes \mathbf{Q}$ using modular symbols [Ste07b], and specify B by giving a basis in reduced echelon form for a subspace $V \subset \mathrm{H}_1(J, \mathbf{Q})$. Not every subspace is valid, but there is an algorithm to determine which are.

We specify G as follows. Suppose V defines $B \subset J$. By the Abel-Jacobi theorem, we have $J(\mathbf{C}) \cong \mathrm{H}_1(J, \mathbf{R})/\mathrm{H}_1(J, \mathbf{Z})$, and letting $\Lambda = \mathrm{H}_1(J, \mathbf{Z}) \cap V$ we have $B(\mathbf{C}) \cong (V \otimes \mathbf{R})/\Lambda$. In particular, $B(\mathbf{C})_{\mathrm{tor}} \cong V/\Lambda$, and we specify $G \subset B(\mathbf{C})_{\mathrm{tor}}$ by giving the lattice L with $\Lambda \subset L \subset V$ such that $L/\Lambda \cong G$.

We represent morphisms in terms of the above data. The PI has found an effective algorithm (unpublished) that, given simple modular abelian varieties A and B, either proves that A and B are not isomorphic, or returns an explicit isomorphism between them. The main idea is to use an explicit isogeny $B \to A$ to embed $\mathrm{Hom}(A, B)$ in a number field, then solve a norm equation.

To enumerate modular abelian varieties of given level, we first enumerate newforms f using modular symbols and linear algebra as in [Ste07b]. To f, we consider $A_f \subset J$, presented as above. Using module theory of the Hecke algebra $\mathbf{T}$, we *hope to devise* an algorithm to write down all candidate isogenies $A_f \to B$. Then we find one representative abelian variety in each isomorphism class, and finally construct the minimal isogeny graph between the representatives. The PI is not sure how to do this, but has some ideas, e.g., using that the Galois representations $\rho^{\mathrm{ss}}_{f,\mathfrak{p}}$ determine the isogenies and are determined by f.

4.3 p-adic BSD

J. Balakrishnan's 2011 MIT Ph.D. thesis contains a generalization to Jacobians of genus 2 modular curves in [FpS$^+$01] of the conjecture for elliptic curves in [MTT86]. Part of that thesis involved computing p-adic L-series of modular abelian varieties, which was joint work with the PI, and another part involved computing p-adic regulators (using Coleman integration), which involved collaboration with Jan Steffen Mueller. The conjecture she gives is still not complete, in that there is a potential sign ambiguity that has not yet been pinned down.

The PI intends to continue collaborating with Balakrishnan on this project. In addition to generally assisting with enumerating data about modular abelian varieties that will be useful in formulating a general p-adic BSD conjecture (with evidence to back it up!), he intends to carry out the following specific projects:

1. *Riemann Sums:* Create an optimized implementation of the Riemann sums algorithm for computing p-adic L-functions associated to arbitrary newforms. The PI has substantial recent experience with this in the case of elliptic curves as a result of the large tables he created for [SW11].

2. *Overconvergent Modular Symbols:* Create an optimized implementation of the Pollack-Stevens-Greenberg approach to computing high precision p-adic L-functions using overconvergent modular symbols. The PI has done preliminary work on planning such an implementation while attending the lectures by Pollack-Stevens on this algorithm at the 2011 Arizona Winter School. Ben Lundell, who is a new postdoc at Univ. of Washington, was in the Pollack-Stevens project group at AWS, and intends to collaborate with the PI on this implementation.

4.4 Tamagawa Numbers of Abelian Varieties over $\mathbf{Q}(\sqrt{5})$

The algorithm of [CS01] makes it possible to compute the odd part of the Tamagawa number of any optimal simple modular $A = A_f$ over $\mathbf{Q}$ at a prime p of purely toric reduction. Some reasons Tamagawa numbers are of interest include their appearance in the Birch and Swinnerton-Dyer formula, and their relation to congruences between modular forms. The main inputs to the algorithm in [CS01] are computation of the modular degree of A, and computation of a certain local-at-p analogue of the modular degree of A using rational quaternion algebras.

Now suppose instead that A is a purely toric modular abelian variety over $\mathbf{Q}(\sqrt{5})$ associated to a Hilbert modular newform f, and that some prime $\mathfrak{p}$ exactly divides the level. The algorithm (of [Dem04]), which uses quaterion algebras to compute f, may yield an analogue of the local-at-$\mathfrak{p}$ modular degree mentioned above. The PI is optimistic that there is an analogue of [Wat02], which might lead to an algorithm to compute the global modular degree of A as a quotient of the Jacobian of the relevant Shimura curve. Combining all this may yield an algorithm to compute the odd part of the Tamagawa number of A at $\mathfrak{p}$.

5 Torsion on Elliptic Curves over Number Fields

Specific Goals:

1. Write up and publish a theorem that classifies the possible primes p that divide $\#E(K)_{\mathrm{tor}}$ for some elliptic curve E over a quartic field K. (Joint with Sheldon Kamienny, Michael Stoll and Maarten Derickx.)
2. Generalize these methods to classify what we can about the primes that divide $\#E(K)_{\mathrm{tor}}$ for E an elliptic curve over number fields of degrees 5,6,7.

The PI, Maarten Derickx (a graduate student of Bas Edixhoven in Leiden, Holland), Sheldon Kamienny, and Michael Stoll have been collaborating on a project to explicitly determine possible torsion points on elliptic curves over number fields. In particular, we have devised, implemented, and run code to verify the following:

(206) 419-0925 wstein@uw.edu http://wstein.org

Theorem 5.1. *Suppose E is an elliptic curve over a number field K of degree 4, and $p \mid \#E(K)_{\mathrm{tor}}$. Then $p \in \{2,3,5,7,11,13,17\}$, and every such p occurs.*

The PI intends to write this result up for publication, including incorporating new work of Maarten Derickx that makes the modular symbols part of the computation very efficient (with these improvements, the computation takes only minutes!): this is an application of [Par00] that rules out primes with $29 < p \leq 97$.

Dealing with $19 < p \leq 29$ involves application of results of [CES03] and computation with models for modular curves using Riemann-Roch spaces (see [Hes02]).

Maarten Derickx has coded an unpublished refinement of the above strategy, which yields results for degrees up to 7, and specific computational challenges, as summarized below. Let $S(d)$ be the set of primes that divide the order of a torsion point on an elliptic curve over a number field of degree $\leq d$, and let $P(N)$ be the set of primes $\leq N$. Our current knowledge of $S(d)$ is:

$S(d) \subset P((3^{d/2}+1)^2)$	Merel-Oesterlé
$S(1) = P(7)$	Mazur
$S(2) = P(13)$	Kamienny-Mazur
$S(3) = P(13)$	Parent
$S(4) = P(17)$	Kamienny-Stein-Stoll
$S(5) \supseteq P(19)$	Derickx
$S(5) \subseteq P(19) \cup \{29,31,41\}$	Derickx
$S(6) \subseteq P(41) \cup \{73\}$	Derickx
$S(7) \subseteq P(151)$	Derickx

6 Congruences, Visibility, and Heegner Points

This project involves proving new results and develop computational techniques related to congruences, visibility, and Heegner points.

Specific Goals:

1. Study visibility of elements of order 7 and 11 of $Ш(E/\mathbf{Q})$, jointly with Tom Fisher. Exhibit examples of visible of elements of order 7, and prove that there is some $c \in Ш(E/\mathbf{Q})[7]$ that is not visible in any abelian surface, showing that the visibility dimension is sometimes larger than 2.
2. Construct cohomology classes on rank 2 curves using Heegner points. In particular, for every (optimal) elliptic curve E over $\mathbf{Q}$ of conductor up to 1000 and every prime $p = 3, 5, 7$, use congruences to construct a nonzero cohomology class in $\mathrm{Sel}^{(p)}(E/\mathbf{Q})$ attached to a Heegner point.

(206) 419-0925 wstein@uw.edu http://wstein.org

6.1 Visibility of Shafarevich-Tate Groups in Abelian Surfaces

Let E be an elliptic curve over $\mathbf{Q}$. Mazur proved in [Maz99] that each $c \in Ш(E)[3]$ is visible in an abelian surface, which means that associated to c there is an abelian surface A and an inclusion $\iota : E \hookrightarrow A$ such that $c \mapsto 0$ under the induced map $Ш(E) \to Ш(A)$. Klenke [Kle01] proved the same result for elements of order 2 in $\mathrm{H}^1(\mathbf{Q}, E)$. Note that $F = A/\iota(E)$ is an elliptic curve, and $A \cong (E \times F)/\Phi$, for some subgroup Φ of A, so we can view A as built from E and F by gluing along a finite subgroup. For $p = 7$, there are *finitely many* elliptic curves F with $E[7] = F[7]$ and recent work of Fisher ([Fis11]) provides powerful techniques for finding many of these curves. He has considered hundreds of examples from [Cre] of E with $7 \mid \#Ш(E/\mathbf{Q})$, and in many cases finds another curve F which explains an element of order 7 in Ш. In some of the explicit remaining cases, we expect that there is some $c \in Ш(E/\mathbf{Q})[7]$ that is *not* visible in any abelian surface.

Challenge 6.1. In collaboration with Fisher and M. Stoll, prove (assuming GRH) in at least one case that $c \in Ш(E/\mathbf{Q})[7]$ is not visible in any abelian surface. This may involve rational point computations on twists of the Klein quartic $X(7)$.

Moreover, in cases when c is not visible in an abelian surface, the next step is searching for a 2-dimensional modular abelian variety A_f such that $E[7] \hookrightarrow A_f[7]$, and then establishing that c is visible in an abelian 3-fold that is isogenous to $E \times A_f$. Here, we may assume the BSD conjecture, since computing algebraic ranks of higher analytic rank abelian varieties without explicit equations is often not feasible. This will shed light on the following conjecture and question:

Conjecture 6.2 (-)**.** *Every element of* $Ш(E/\mathbf{Q})$ *is modular, i.e., visible in some modular Jacobian* $J_0(N)$*.*

In [AS02, §2], the PI introduced a notion of *visibility dimension* of $c \in Ш(E/\mathbf{Q})$, which is the smallest dimension of an abelian variety A such that $E \hookrightarrow A$ and $c \mapsto 0 \in Ш(A/\mathbf{Q})$. For example, if c has order 2 or 3, then the results above show that visibility dimension of c is 2; in general, a restriction of scalars construction of the PI (see [AS02, §1.3]) shows that it is at most the order of c.

Question 6.3. If $c \in Ш(E/\mathbf{Q})$ has order 7, is the visibility dimension at most 3?

This project would improve tables and software for computing with modular forms. We will have to search for many degree 2 newforms of relatively high level, and compute their L-series and some arithmetic invariants.

6.2 Kolyvagin Classes and Visibility

The PI has written three papers about Heegner points on elliptic curves of rank ≥ 2, and Kolyvagin's construction of cohomology classes. Without going into

(206) 419-0925 wstein@uw.edu http://wstein.org

technical details, for any elliptic curve E over $\mathbf{Q}$, quadratic imaginary field K satisfying certain hypotheses, and certain squarefree integers λ and prime powers ℓ^n, there is a cohomology class $\tau_{E,\lambda,\ell^n} \in \mathrm{H}^1(K, E[\ell^n])$, which is constructed in a natural way from the Heegner point $y_\lambda \in E(K[\lambda])$, where $K([\lambda])$ is a ring class field. *Kolyvagin's conjecture* is that for every ℓ there is some n and λ such that $\tau_{E,\lambda,\ell^n} \neq 0$. This implies a structure theorem for the Selmer group (see [Kol91a]).

The PI's first paper, [JLS09] uses numerical techniques to directly compute a Heegner point over an extension of the field $K = \mathbf{Q}(\sqrt{-7})$ on the rank 2 elliptic curve $E =$**389a** over $\mathbf{Q}$, and verifies that this point gives rise (via [Kol91a]) to a nonzero class in $\mathrm{Sel}^{(3)}(E/\mathbf{Q})$. This was the first example that showed that Kolyvagin's construction gives rise to a nonzero class. The second paper, [Ste10] used the construction to define subgroups of $E(K)$ that conjecturally satisfies a higher rank analogue of the Gross-Zagier formula. The third paper [Ste11] mimics and refines the argument of [Cor02] and uses rational quaternion algebras to verify algebraically that many specific Kolyvagin classes are nonzero.

The proposed project (Goal 2 on page 13 above) involves a fourth strategy for investigating Kolyvagin classes, which is illustrated by the following (unpublished) theorem, whose proof is a relatively easy exercise in Galois cohomology.

Theorem 6.4 (–)**.** *Suppose E and F are optimal elliptic curves of the same conductor N, and that $E[\ell]$ is irreducible. If $E[\ell] = F[\ell]$ as subsets of $J_0(N)$, then $\tau_{E,\lambda,\ell} \in \mathrm{H}^1(K, E[\ell])$ and $\tau_{F,\lambda,\ell} \in \mathrm{H}^1(K, F[\ell])$ are identified by the canonical isomorphism induced by the equality $E[\ell] = F[\ell]$ in $J_0(N)$.*

For example, take for E the curve **681c** of rank 2, for F the curve **681b** of rank 0, take $\ell = 3$, and $K = \mathbf{Q}(\sqrt{-8})$. We have [CM00, AS05] that $E[3] = F[3] \subset J_0(681)$. Thus Kolyvagin's conjecture would follow if we knew that some $\tau_{F,\lambda,3} \neq 0$. A computation shows that $\mathrm{ord}_3([F(K)/_{\mathrm{tor}} : \mathbf{Z}y_{F,K}]) = 1$, and visibility (as in [CM00]) shows that $9 \mid \#Ш(F/K)[3]$. Kolyvagin's structure theorem [Kol91b] applied to F then implies that some $\tau_{F,\lambda,3} \neq 0$. Usually, verifying the hypothesis of Theorem 6.4 amounts to showing that $\mathrm{ord}_\ell([F(K) : \mathbf{Z}y_{F,K}]) = 1$ and using visibility to show that $Ш(F/K)[\ell]$ is nontrivial ([GJP+09, §3.5] is helpful).

1. Verify the hypothesis of Theorem 6.4 in as many cases as possible given the speed of the algorithms mentions above.
2. Generalize Theorem 6.4 to cover the case of congruent elliptic curves of different conductor. In general, this is significantly complicated by the existence of several degeneracy maps between the modular curves of each level.
3. Generalize Theorem 6.4 to replace F by an abelian variety A_f attached to a newform of any level. The main difficulty in applying this result would be that the PI does not know of any way to verify the analogue of the hypothesis that $\mathrm{ord}_\ell([F(K) : \mathbf{Z}y_{F,K}]) = 1$. The PI hopes to find a way in particular cases or prove a general congruence theorem that, under suitable hypotheses, ensures the existence of such an A_f.

(206) 419-0925 wstein@uw.edu http://wstein.org

References

[AS02] A. Agashe and W. Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185.

[AS05] ———, *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, http://wstein.org/papers/shacomp/. MR 2085902

[Bil11] Nicolas Billerey, *Criteres d'irreductibilite pour les representations des courbes elliptiques*, International Journal of Number Theory **7** (2011), 1001–1032.

[BK75] B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable. IV*, Springer-Verlag, Berlin, 1975, Lecture Notes in Mathematics, Vol. 476.

[BMSW07] Baur Bektemirov, Barry Mazur, William Stein, and Mark Watkins, *Average ranks of elliptic curves: tension between data and conjecture*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), no. 2, 233–254 (electronic). MR 2291676

[BS02] K. Buzzard and W. A. Stein, *A mod five approach to modularity of icosahedral Galois representations*, Pacific J. Math. **203** (2002), no. 2, 265–282. MR 2003c:11052

[BS11] R. Bradshaw and W. A. Stein, *Heegner Points and the Arithmetic of Elliptic Curves over Ring Class Extensions*, Submitted (2011), http://wstein.org/papers/bs-heegner/.

[CDT99] B. Conrad, F. Diamond, and R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), no. 2, 521–567.

[CES03] B. Conrad, S. Edixhoven, and W. A. Stein, $J_1(p)$ *Has Connected Fibers*, Documenta Mathematica **8** (2003), 331–408, http://www.wstein.org/papers/j1p/.

[CL07] J. E. Cremona and M. P. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experiment. Math. **16** (2007), no. 3, 303–312. MR 2367320 (2008k:11057)

[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

[Cor02] Christophe Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), no. 3, 495–523, http://www.math.jussieu.fr/~cornut/papers/mcinv_published.pdf.

[Cre] J. E. Cremona, *Elliptic Curves Data*, http://www.warwick.ac.uk/~masgaj/ftp/data/.

[Cre97] ———, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997, http://www.warwick.ac.uk/~masgaj/book/fulltext/.

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

[DDLR11] Henri Darmon, Michael Daub, Sam Lichtenstein, and Victor Rotger, *The Effective Computation of Iterated Integrals and Chow-Heegner Points on Triple Products*, In Preparation (2011).

[Del02] Christophe Delaunay, *Formes modulaires et invariants de courbes elliptiques définies sur* $\mathbf{Q}$, Thèse de Doctorat, Université Bordeaux I, available at http://math.univ-lyon1.fr/~delaunay/.

[Dem04] Lassina Dembélé, *Quaternionic Modular Symbols and omputing Hilbert modular forms,* http://wstein.org/mcs/archive/spring2004/dembele.html.

[Dem05] ———, *Explicit computations of Hilbert modular forms on* $\mathbb{Q}(\sqrt{5})$, Experiment. Math. **14** (2005), no. 4, 457–466. MR 2193808

[Dok04] Tim Dokchitser, *Computing special values of motivic L-functions*, Experiment. Math. **13** (2004), no. 2, 137–149, http://arxiv.org/abs/math/0207280. MR 2068888 (2005f:11128)

[Fis11] Tom Fisher, *On Families of n-congruent Elliptic Curves*, Preprint (2011).

[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

[Gee06] Toby Gee, *A modularity lifting theorem for weight two Hilbert modular forms*, Math. Res. Lett. **13** (2006), no. 5-6, 805–811. MR 2280776 (2007m:11065)

[GJP+09] G. Grigorov, A. Jorza, S. Patrikis, C. Tarnita, and W. Stein, *Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves*, Math. Comp. **78** (2009), 2397–2425, http://wstein.org/papers/bsdalg/.

[GK92] B. H. Gross and S. S. Kudla, *Heights and the central critical values of triple product L-functions*, Compositio Math. **81** (1992), no. 2, 143–209. MR 93g:11047

[GSL11] GSL, *GNU Scientific Library*, http://www.gnu.org/s/gsl/.

[GV10] Matthew Greenberg and John Voight, *Computing systems of hecke eigenvalues associated to hilbert modular forms*, Math. Comp. (2010), http://www.cems.uvm.edu/~voight/articles/heckefun-021910.pdf.

[Hes02] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445. MR 1890579 (2003j:14032)

[JLS09] Dimitar Jetchev, Kristin Lauter, and William Stein, *Explicit Heegner points: Kolyvagin's conjecture and non-trivial elements in the Shafarevich-Tate group*, J. Number Theory **129** (2009), no. 2, 284–302, http://wstein.org/papers/kolyconj/. MR 2473878 (2009m:11080)

[JS07] Dimitar P. Jetchev and William Stein, *Visibility of the Shafarevich-Tate group at higher level*, Doc. Math. **12** (2007), 673–696, http://wstein.org/papers/vishigher/. MR 2377239 (2009c:11081)

[Kis09] Mark Kisin, *Moduli of finite flat group schemes, and modularity*, Ann. of Math. (2) **170** (2009), no. 3, 1085–1180. MR 2600871 (2011g:11107)

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

[Kol91a] V. A. Kolyvagin, *On the structure of Selmer groups*, Math. Ann. **291** (1991), no. 2, 253–259, http://wstein.org/papers/stein-ggz/references/kolyvagin-structure_of_selmer_groups/. MR 93e:11073

[Kol91b] ———, *On the structure of Shafarevich-Tate groups*, Algebraic geometry (Chicago, IL, 1989), Springer, Berlin, 1991, http://wstein.org/papers/bib/kolyvagin-structure_of_sha.pdf, pp. 94–121.

[KSW08] Koopa Tak-Lun Koo, William Stein, and Gabor Wiese, *On the generation of the coefficient field of a newform by a single Hecke eigenvalue*, J. Théor. Nombres Bordeaux **20** (2008), no. 2, 373–384. MR 2477510 (2010d:11047)

[KW08] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (i)*, Preprint (2008).

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978), http://archive.numdam.org/article/PMIHES_1977__47__33_0.pdf.

[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

[Mil10] Robert L. Miller, *Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one*, http://arxiv.org/abs/1010.2431, 2010.

[MS11] Robert L. Miller and Michael Stoll, *Explicit isogeny descent on elliptic curves*, To appear in Math. Comp. (2011), http://arxiv.org/abs/1010.3334.

[MSD74] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48. MR MR830037 (87e:11076)

[Par00] Pierre Parent, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier (Grenoble) **50** (2000), no. 3, 723–749. MR 1779891 (2001i:11067)

[Rib92] K. A. Ribet, *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

[S$^+$11] W. A. Stein et al., *Sage Mathematics Software (Version 4.6.2)*, The Sage Development Team, 2011, http://www.sagemath.org.

[SP10] William Stein and Clement Pernet, *Fast computation of hermite normal forms of random integer matrices*, J. Number Theory **130** (2010), no. 7, 1675–1683, http://wstein.org/papers/hnf/.

[Ste82] G. Stevens, *Arithmetic on modular curves*, Birkhäuser Boston Inc., Boston, Mass., 1982. MR 87b:11050

[Ste07a] William Stein, *The Birch and Swinnerton-Dyer Conjecture, a Computational Approach*, 2007, http://wstein.org/edu/2007/spring/bsd/.

[Ste07b] ———, *Modular Forms, A Computational Approach*, Graduate Studies in Mathematics, vol. 79, American Mathematical Society, Providence, RI, 2007, With an appendix by Paul E. Gunnells, http://wstein.org/books/modform/. MR 2289048

[Ste09] ———, *Elementary number theory: primes, congruences, and secrets*, Undergraduate Texts in Mathematics, Springer, New York, 2009, A computational approach. MR 2464052 (2009i:11002)

[Ste10] ———, *Toward a Generalization of the Gross-Zagier Conjecture*, Internat. Math. Res. Notices (2010), http://wstein.org/papers/stein-ggz/.

[Ste11] ———, *Verification of kolyvagin's conjecture for specific elliptic curves*, Submitted (2011), http://wstein.org/papers/kolyconj2/.

[SW02] William Stein and Mark Watkins, *A database of elliptic curves—first report*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, http://wstein.org/ecdb, pp. 267–275. MR 2041090 (2005h:11113)

[SW10] William Stein and Jared Weinstein, *Kolyvagin classes on elliptic curves: structure, distribution, and algorithms*, In preparation (2010).

[SW11] William Stein and Christian Wuthrich, *Algorithms for the Arithmetic of Elliptic Curves using Iwasawa Theory*, Submitted (2011), http://wstein.org/papers/shark/.

[Tao] Terry Tao, *Distinguished Lecture Series III: Shou-wu Zhang, "Triple L-series and effective Mordell conjecture"*, http://terrytao.wordpress.com/2007/05/04/distinguished-lecture-series-iii-shou-wu-zhang-%E2%80%9Ctriple-l-series-and-effective-mordell-conjecture%E2%80%9D/.

[Wat02] M. Watkins, *Computing the modular degree of an elliptic curve*, Experiment. Math. **11** (2002), no. 4, 487–502 (2003). MR 1 969 641

[YZZ11] X. Yuan, S. Zhang, and W. Zhang, *Triple product L-series and Gross-Schoen cycles I: split case*, Preprint (2011), http://www.math.columbia.edu/~yxy/preprints/triple.pdf.

[Zha01] Shou-Wu Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), no. 1, 27–147. MR 1826411 (2002g:11081)

[Zha04] ———, *Gross-Zagier formula for* GL(2). *II*, Heegner points and Rankin L-series, Math. Sci. Res. Inst. Publ., vol. 49, Cambridge Univ. Press, Cambridge, 2004, http://www.math.columbia.edu/~szhang/papers/gzes.pdf, pp. 191–214. MR 2083213