William A. Stein *Project Description*

(858) 220-6876 wstein@math.washington.edu http://modular.math.washington.edu

Explicit Approaches to the Birch and Swinnerton-Dyer Conjecture

1 Introduction

My research reflects the rewarding interplay of theory with explicit computation in number theory, as illustrated by 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 goal of this proposal is to carry out a wide range of computational and theoretical investigations on elliptic curves and abelian varieties motivated by the Birch and Swinnerton-Dyer conjecture (BSD conjecture). This will hopefully improve our practical computational capabilities, extend the data that researchers have available for formulating conjectures, and deepen our understanding of theorems about the BSD conjecture.

The PI is one of the more sought after people by the worldwide community of number theorists, for computational confirmation of conjectures, for modular forms algorithms, for data, and for ways of formulating problems so as to make them more accessible to algorithms. The PI has also been successful at involving numerous undergraduate and graduate students at all levels in his research.

1.1 Prior Support

The PI was partly supported by NSF postdoctoral fellowship during 2000–2004 (DMS-0071576) in the amount of $90,000. The PI was also awarded NSF grant DMS-0555776 (and DMS-0400386) from the ANTC program in the amount of $177,917 for the period 2004–2007. The PI's work under DMS-0555776 succeeded at improving the modular forms database and resulted in numerous papers on the arithmetic of elliptic curves, modular forms and abelian varieties [Ste, GJP+05, MST06, SW04, JS05, AS05, ARS06a, ARS06b, Ste04b], one completed book [Ste07] on computing with modular forms, and progress on another book on number theory [Ste05]. It has also led to a new software initiative (see Section 1.4 below). Funds from DMS-0555776 were used to run a successful workshop at UCSD and to purchase a 16-processor compute server with 64GB RAM.

(858) 220-6876 wstein@math.washington.edu http://modular.math.washington.edu

1.2 The BSD Conjecture

The Birch and Swinnerton-Dyer conjecture is a central problems in number theory, and this proposal is based on a group of ideas related to this conjecture.

An *elliptic curve* is a projective genus one curve with a distinguished rational point. Every such curve is the projective closure of a nonsingular affine curve given by $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$. An *abelian variety* is a projective group variety—the one dimensional abelian varieties are exactly the elliptic curves.

Conjecture 1.1 (BSD Conjecture)**.** *Let A be an abelian variety over $\mathbf{Q}$. (The objects and notation in the formula are discussed below.)*

1. *The rank r of $A(\mathbf{Q})$ equals $\operatorname{ord}_{s=1} L(A,s)$.*
2. *We have*
$$\frac{L^{(r)}(A,1)}{r!} = \frac{\#Ш(A)\cdot \Omega_A \cdot \operatorname{Reg}_A}{\#A(\mathbf{Q})_{\mathrm{tor}}\cdot \#A^\vee(\mathbf{Q})_{\mathrm{tor}}} \cdot \prod_{\ell | N} c_\ell.$$

In the conjecture, $L(A,s)$ is the Hasse-Weil L-series of A. 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 $\ell \mid N$, the integer $c_\ell = \#\Phi_{A,\ell}(\mathbf{F}_\ell)$ is the *Tamagawa number* of A at ℓ, where $\Phi_{A,\ell}$ denotes the component group of the Néron model of A at ℓ. The abelian variety 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

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

which is a group that measures the failure of a local-to-global principle. It is implicit in the statement of the conjecture that $Ш(A)$ is finite, though this is only known in some cases. The regulator Reg_A is the absolute value of the discriminant of the Néron-Tate canonical height pairing $A(\mathbf{Q})_{/\mathrm{tor}} \times A(\mathbf{Q})_{/\mathrm{tor}} \to \mathbf{R}$.

If A is an elliptic curve then $\#A(\mathbf{Q})_{\mathrm{tor}}$, $\#A^\vee(\mathbf{Q})_{\mathrm{tor}}$, Ω_A, and c_ℓ are relatively easy to compute; none of the other quantities are known to be computable in general, even when A is an elliptic curve, though many can in practice be computed.

Conjecture 1.2 (BSD(A,p))**.** *Let A be an abelian variety over $\mathbf{Q}$ of rank r and let p be a prime. Then*

$$\operatorname{ord}_p\left(\frac{L^{(r)}(A,1)}{r!\cdot \operatorname{Reg}_A \cdot \Omega_A}\right) = \operatorname{ord}_p\left(\frac{\#Ш(A)}{\#A(\mathbf{Q})_{\mathrm{tor}}\cdot \#A^\vee(\mathbf{Q})_{\mathrm{tor}}} \cdot \prod_{\ell|N} c_\ell\right).$$

(858) 220-6876 wstein@math.washington.edu http://modular.math.washington.edu

In Conjecture 1.2 the fraction on the left side is not known to be a rational number (except when $r \leq 1$), so its rationality is part of the conjecture.

Tate [Tat66] formulated the BSD conjecture for any abelian variety over a global field K, and proved (generalizing work of Cassels) that if A and B are related by an isogeny, then BSD(A, p) is true if and only if BSD(B, p) is true.

1.3 Modular Abelian Varieties

Modular abelian varieties are a special class of abelian varieties over $\mathbf{Q}$ that have been studied intensively. Computation with modular abelian varieties is attractive because they are easier to describe than arbitrary abelian varieties, have extra hidden structure, and their L-functions are reasonably well understood.

We recall Shimura's construction [Shi73] of modular abelian varieties. 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 $\mathbf{T} \to \mathbf{Z}[a_1, a_2, a_3, \ldots]$ 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 1.3 (Modular abelian variety)**.** An abelian variety over a number field is a *modular abelian varieties* if it is a quotient of $J_1(N)$ for some N.

Algorithms for computing many of the invariants in the BSD conjecture for modular abelian varieties has been a major part of the PI's research program.

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 a modular abelian variety. Also, it is now known (due to very recent work of Khare, Wintenberger, and Dieulefait) that every abelian variety of GL_2-type (see [Rib92]) and odd conductor is a modular abelian variety.

The PI recently completed a book on computing with modular forms [Ste07] that will be published by the AMS. He is working on a graduate textbook with Ken Ribet on modular abelian varieties, and an undergraduate text on number theory, both intended for publication by Springer-Verlag. He led a 2-week high-school student workshop on the Birch and Swinnerton-Dyer conjecture (see [SIM]).

(858) 220-6876 wstein@math.washington.edu http://modular.math.washington.edu

1.4 Software for Algebra and Geometry Experimentation

The PI is the principal author of SAGE—Software for Algebra and Geometry Experimentation (see [SJ05]). Substantial work on SAGE has been done jointly with students (7 undergraduates and 5 graduate students). The goal of SAGE is to create an optimal *open source* software environment for research in algebra, geometry, number theory, and related areas. The PI intends to make all data and algorithms developed as part of the proposed research freely available online and from SAGE.

The PI is the author of the modular forms and modular abelian varieties components of Magma [BCP97]. When possible many of the proposed computations will be independently verified using Magma.

When we describe a result that relies on computation below, there is an implicit assumption that certain software produced correct output. Also, the ranges of computations, e.g., "all curves of conductor up to 1000", are in many cases arbitrary. Our *primary* motivation for doing these computations is to motivate the development of new conjectures and computational and theoretical tools.

2 The BSD Formula: Computing Ш

Much of this research proposal is about computing Ш, which is the most difficult to compute invariant appearing in the BSD conjecture.

2.1 Applying Theorems of Kato and Kolyvagin

The PI, 3 undergraduates and a graduate student proved the following in [GJP+05]:

Theorem 2.1 (Stein et al.)**.** *Suppose that E is a non-CM elliptic curve of rank ≤ 1, conductor ≤ 1000 and that p is a prime. If p is odd, assume further that the mod p representation $\overline{\rho}_{E,p}$ is irreducible and p does not divide any Tamagawa number of E. Then* $\mathrm{BSD}(E,p)$ *is true.*

The proof involves an application of results of Kato and Kolyvagin, new refinements of Kolyvagin's theorem, explicit 2-descent and 3-descent and much explicit calculation. This is a first step toward the following goals:

Goal 2.2. Verify the BSD Conjecture for every elliptic curve over $\mathbf{Q}$ of conductor < 1000, except for the 18 curves of rank 2.

Goal 2.3. For each curve E over $\mathbf{Q}$ of conductor < 1000 and rank 2, prove that $Ш(E)[p] = 0$ for all $p < 1000$.

We hope to make further progress toward Goal 2.3 using p-adic methods (see Section 2.3 below), since unconditional computation of $\mathrm{Sel}^{(p)}(E/\mathbf{Q})$ directly using standard algebraic number theory techniques for $p > 5$ appears to not be practical.

(858) 220-6876 wstein@math.washington.edu http://modular.math.washington.edu

Another approach is to improve on work of Kolyvagin—Theorem 2.1 excludes divisors of Tamagawa numbers because Kolyvagin's theorem is not sufficiently precise at such primes.

Goal 2.4. Refine Kolyvagin's bound when a prime p divides a Tamagawa number.

Dimitar Jetchev (who began working with the PI as an undergraduate) has been working on Goal 2.4 in consultation with the PI. Let E be an elliptic curve over $\mathbf{Q}$, let K be a field that satisfies the *Heegner hypothesis* for E, i.e., such that each prime dividing N splits in K. Assume that E has analytic rank 1 over K, and let $y_K \in E(K)$ be the Heegner point. Suppose $p \geq 5$ and that $\overline{\rho}_{E,p}$ is surjective. Jetchev has made great progress toward the following:

Goal 2.5. If $\mathrm{ord}_p(\prod c_\ell) \geq 1$, where the c_ℓ are the Tamagawa numbers of E, prove that $\mathrm{ord}_p(\#Ш(E/K)) \leq \mathrm{ord}_p([E(K) : \mathbf{Z}y_K]) - 2$.

Kolyvagin gives a formula (see, e.g., [Kol91a, Gro91, McC91]) for $\#Ш(E/K)$ which involves global divisibility of Heegner points and Jetchev links those global divisibility exponents to Tamagawa numbers. Work toward Goal 2.5 uses Poitou-Tate global duality and the Chebotarev density theorem to show that mod p there are no nontrivial Kolyvagin systems; this is equivalent to showing that all Heegner points P_n on E over ring class fields are globally divisible by p.

2.2 Complex Multiplication Curves

A *complex multiplication* (CM) elliptic curve E over a number field is one such that $\mathrm{End}(E_{\mathbf{C}}) \neq \mathbf{Z}$. The PI and Aron Lum proved the following result:

Theorem 2.6 (Stein, Lum)**.** *Suppose E is a CM elliptic curve over $\mathbf{Q}$ with rank at most 1 and conductor at most 5000. Then $\mathrm{BSD}(E, p)$ is true for all primes $p \geq 5$ of good reduction for E.*

This is an application of Rubin [Rub91] for rank 0 curves and Kolyvagin [Kol90, Cor. D] for rank 1 curves. The PI to compute to much higher conductor.

Goal 2.7. Suppose E is a complex multiplication elliptic curve over $\mathbf{Q}$ and that $p \geq 5$ is a prime of bad reduction for E. Find and implement a *practical* algorithm to verify $\mathrm{BSD}(E, p)$, then apply it to all E of conductor up to 5000.

Goal 2.7 is difficult mainly because the mod p representation is not "as surjective as possible", so the methods used for Theorem 2.6 do not apply. One approach to Goal 2.7 is to try do computations using Theorem 2.11 below.

(858) 220-6876 wstein@math.washington.edu http://modular.math.washington.edu

2.3 p-adic Methods

Suppose E is an elliptic curve over a number field K and $p \geq 5$ is a prime (of $\mathcal{O}_K$) of good ordinary reduction for E. In [MST06] the PI, Mazur, and Tate give a new approach to computing p-adic heights

$$h_p : E(K) \to \mathbf{Q}_p$$

that leverages Kedlaya's fast algorithm [Ked01, Ked04] for explicit computation of Monsky-Washnitzer cohomology groups. We made our algorithm explicit only when $K = \mathbf{Q}$ or K is a quadratic imaginary field, though the key ideas for creating a general explicit algorithm are given in [MST06]. The PI, David Harvey, Jen Balakrishnan, and Liang Xiao have implemented and optimized this algorithm over $\mathbf{Q}$ and quadratic imaginary K in both SAGE and Magma (this was a major project at an MSRI graduate student workshop that the PI ran in August 2006).

Goal 2.8. Design and implement a general algorithm for computing p-adic heights (for all primes p) on elliptic curves over arbitrary number fields.

The natural height pairing here is not very well understood; indeed, it still only conjectural that is nondegenerate. It can be verified in particular cases via computation:

Conjecture 2.9 (Schneider)**.** *Suppose E is an elliptic curve over $\mathbf{Q}$ and p is a prime of good ordinary reduction. Then the p-adic cyclotomic height pairing on $E(\mathbf{Q})$ is nondegenerate.*

There are very few general results toward this conjecture (except in the CM case). It can be verified in particular cases:

Goal 2.10. Create a table of p-adic regulators to precision $O(p^5)$ for every elliptic curve of conductor up to 120000 and the first five primes $p \geq 5$ of good ordinary reduction for E.

The data from Goal 2.10 will also be of interest in investigations about congruences between algebraic parts of p-adic L-functions.

Theorem 2.11 (Schneider [Sch83] and Perrin-Riou)**.** *Suppose p is an odd prime of good ordinary reduction for E, and let $\mathrm{Reg}_E^{(p)} \in \mathbf{Q}_p$ be the p-adic regulator of E, i.e., the discriminant of the p-adic height pairing on $E(\mathbf{Q})$. If the p-primary part $Ш(E/\mathbf{Q})(p)$ of $Ш(E/\mathbf{Q})$ is finite, then the leading term of the algebraic p-adic L-function of E has the same p-adic valuation as*

$$\frac{\#Ш(E) \cdot \mathrm{Reg}_E^{(p)}}{\#E(\mathbf{Q})_{\mathrm{tor}}^2} \cdot \#E(\mathbf{F}_p)^2 \cdot \prod_{\ell | N} c_\ell.$$

(858) 220-6876 wstein@math.washington.edu http://modular.math.washington.edu

The following is needed in order to apply Theorem 2.11:

Goal 2.12. Create software and better algorithms for computing with p-adic L-functions of elliptic curves and modular abelian varieties.

Much work toward Goal 2.12 in Magma has already been done by the PI, Robert Pollack, and Christian Wuthrich. Substantial work on the main conjecture of Iwasawa theory connects the algebraic and analytic (computable) L-functions.

Remark 2.13. There are other cases where we can apply analogues of Theorem 2.11, e.g., when p is a prime of good supersingular reduction (see [PR03]).

2.4 Constructing Nonzero Elements of Ш(E)

There are 6581 optimal curves in [Cre] of conductor up to 120000 for which p divides the BSD conjectural order of Ш(E) for some $p \geq 3$. Of these, 1387 have conjectural order divisible by a prime $p \geq 5$ and 339 have conjectural order divisible by a prime $p \geq 7$. Of these 1387 curves, the mod p representation is surjective except in 11 cases.

Goal 2.14. For the 1387 curves of conductor up to 120000 for which a prime $p \geq 5$ divides the conjectured $\#$Ш(E), construct an element of order p in Ш(E).

One approach to Goal 2.14 for small p, e.g., $p = 5$, is to construct Ш(E) using visibility, i.e., by finding an elliptic curve F of rank 2 such that $E[p] \cong F[p]$, and using the visibility techniques of [CM00, AS02, AS05].

A second approach, which works in many cases (because the mod p representation is often surjective), is to use results of [Gri05], which gives an explicit criterion in terms of modular symbols to construct nonzero elements of Ш$(E)[p]$. Initial computations of the PI and Grigorov (discussed in [Gri05]) suggest that this approach will succeed in many cases.

A third approach is to use Theorem 2.11 and explicit calculation of p-adic regulators and p-adic L-functions to at least prove that Ш$(E)(p)$ has the conjectured order. This approach doesn't give an explicit construction of Ш$(E)(p)$.

A fourth approach is to explicitly compute Kolyvagin cohomology classes $c_{n,p} \in \mathrm{H}^1(K, E)[p]$ and show that they are in fact elements of Ш$(E)[p]$. Jetchev, Lauter, and the author have done such a computation in a few cases (unpublished).

Recent exciting work of Skinner and Urban also addresses the question of providing very general explicit lower bounds on $\#$Ш(E).

2.5 Tamagawa numbers

The following is a consequence of the BSD conjecture.

(858) 220-6876 wstein@math.washington.edu http://modular.math.washington.edu

Conjecture 2.15. *Suppose E is an elliptic curve and that $p \geq 5$ is odd prime such that $\overline{\rho}_{E,p}$ is irreducible. Then*

$$\mathrm{ord}_p\left(\prod_{\ell|N} c_\ell\right) \leq \mathrm{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right)$$

Let $f = f_E$ be the newform corresponding to E. Under the hypotheses of Conjecture 2.15, [Rib91] implies that there is a newform g of level a proper divisor of the conductor of E whose coefficients (of index coprime to the conductor) are congruent to the coefficients of f. The PI showed in unpublished work how to use this congruence, in some cases, to prove that $L(E,1)/\Omega_E \equiv 0 \pmod{p}$. The PI proposes to write up the details of this argument (jointly with Jetchev), then attempt to refine the argument to yield the congruence of Conjecture 2.15. The PI also hopes to find connections between the components group of E and the $\mathbf{T}$-module (defined using modular symbols) whose order is the p-part of $L(E,1)/\Omega_E$. This approach gives a conceptual explanation of part of the BSD conjecture.

3 The Rank

Let E be an elliptic curve over $\mathbf{Q}$. If $r_{\mathrm{an}} = \mathrm{ord}_{s=1} L(E,s) \leq 1$, then the rank part of the BSD conjecture is known for E; moreover, in principle, and often in practice (as explained elsewhere in this proposal) one can verify the full BSD conjecture. There isn't a single E with $r_{\mathrm{an}} \geq 2$ for which the PI is aware of even a plausible strategy for proving that $Ш(E)$ is finite, let alone verifying the full BSD conjecture—it is even unknown that $L''(E,1)/(\Omega_E \cdot \mathrm{Reg}_E) \in \mathbf{Q}$ for any E. One can verify in particular cases the rank part of the BSD conjecture if $r_{\mathrm{an}} \leq 3$; the PI is aware of no strategy to verify the rank statement for even a single example when $r_{\mathrm{an}} \geq 4$. Morever, if E has analytic rank 2 or larger, then the PI is aware of no conjectural construction of $E(\mathbf{Q})$ analogous to that of Gross-Zagier in the rank 1 case. Thus new ideas are needed when $r_{\mathrm{an}} \geq 2$, and the PI hopes the computations he proposes might play a role in finding them.

3.1 Kolyvagin's Cohomology Classes

Let E be an elliptic curve over $\mathbf{Q}$ with conductor N, and to simplify the discussion assume that E does not have complex multiplication (there are analogues of everything below even if E has CM). Let K be a quadratic imaginary field that satisfies the Heegner hypothesis for E. Fix a prime p such that $E[p]$ is irreducible (we could also replace p by an integer n and remove the requirement that the representation be irreducible).

Kolyvagin defined (see, e.g., [Gro91]) classes $c_{n,p} \in \mathrm{H}^1(K, E[n])$ for infinitely many squarefree integers n satisfying a Chebotarev condition. Let $d_{n,p}$ be the

(858) 220-6876 wstein@math.washington.edu http://modular.math.washington.edu

image in $\mathrm{H}^1(K,E)[p]$ of $c_{n,p}$. Kolyvagin proved that $\mathrm{res}_v(d_{n,p}) = 0$ for all $v \nmid n$ and computed the order of $\mathrm{res}_\ell(d_{n,p})$ in terms of local properties of the point y_K. He used these classes to prove his celebrated results toward the BSD conjecture.

Dimitar Jetchev, Kristin Lauter and the PI have solved the following problem in a handful of cases, and intend to continue working on refining our methods.

Goal 3.1. Find and implement a practical algorithm to compute the order of $c_{n,p}$ and the order of its image $d_{n,p}$.

For simplicity, assume that $n = \ell$ is a prime. By the modularity theorem there is a surjective homomorphism $\pi : X_0(N) \to E$. The two degeneracy maps $X_0(N\ell) \to X_0(N)$ induce maps δ_1 and δ_ℓ from $J_0(N)$ to $J_0(N\ell)$. We say that $d_{\ell,p}$ is *visible of level* $N\ell$ if $d_{\ell,p}$ maps to 0 under the map on cohomology induced by

$$E \xrightarrow{\pi^*} J_0(N) \xrightarrow{(\delta_1 \pm \delta_\ell)^*} J_0(N\ell)$$

for either choice of sign.

Goal 3.2. Find and implement a practical algorithm to determine whether or not a Kolyvagin class $d_{\ell,p}$ is visible at level $N\ell$.

Goal 3.3. Based on the data obtained from Goal 3.2 formulate a conjecture about visibility of the classes $d_{\ell,p}$.

Suppose E is an elliptic curve over $\mathbf{Q}$ with analytic rank ≥ 2. Fix an odd prime p such that $E[p]$ is irreducible. Then the Kolyvagin classes $d_{n,p}$ are elements of $Ш(E)[p]$ and the classes $c_{n,p}$ lie in $\mathrm{Sel}^{(p)}(E)$.

Conjecture 3.4 (Kolyvagin)**.** *Let E and p be as above. Then $\mathrm{Sel}^{(p)}(E)$ is generated by the classes $c_{n,p}$.*

The PI intends to develop a theory for computing with the subgroup of $\mathrm{Sel}^{(p)}(E)$ generated by a given finite collection of classes $c_{n,p}$. Kolyvagin hints at doing this in [Kol91b, Pg. 120].

For example, let E be the rank 2 elliptic curve $y^2 + y = x^3 + x^2 - 2x$ of conductor 389. The PI, Jetchev, and Lauter computed the class $c_{5,3}$ and showed that it defines a nonzero element of $\mathrm{Sel}^{(3)}(E)$—this computation did not require computing $E(\mathbf{Q})$. This computation thus gives an explicit construction using Heegner points of the image in $\mathrm{Sel}^{(3)}(E)$ of a nonzero element of the rank 2 Mordell-Weil group $E(\mathbf{Q})$. Making this computation practical has already involved interesting techniques (e.g., using p-adic methods to verify global non-divisibility of Heegner points). Moreover, we are computationally verifying Kolyvagin's conjecture, which has interesting consequences (unpublished work of Cornut, Nekovar).

(858) 220-6876 wstein@math.washington.edu http://modular.math.washington.edu

3.2 Mazur and Rubin's Shadow Lines

When E is an elliptic curve over $\mathbf{Q}$ of rank 2 there is a construction of Mazur and Rubin, using p-adic heights, that attaches to appropriate quadratic imaginary fields K a certain line in the p-adic completion of the Mordell-Weil group; these are sometimes referred to as "shadow lines". Conjecturally, for every quadratic imaginary field K such that the Mordell-Weil group of the twist of E by the quadratic character of K has rank one (and such that the discriminant of K is prime to the conductor of E) we have such a "shadow line". On the one hand the shadow line is the image of universal norms in the p-adic completion $E(\mathbf{Q}) \otimes \mathbf{Z}_p$ of the Mordell-Weil group of the elliptic curve over layers of the p-adic anticyclotomic tower attached to K, and on the other hand the shadow line is the null space of the p-adic anti-cyclotomic height pairing.

Goal 3.5. Gather extensive numerical data about Mazur-Rubin shadow lines. In particular, are they uniformly distributed as we vary K?

The PI has done computations in this direction using slow methods (see [MR04]). More recently, he and Liang Xiao have been applying the methods of Section 2.3.

4 Databases

The modular forms database (see [Ste04a]) is a freely-available collection of data about objects attached to modular forms. It is analogous to Neil Sloane's tables of integer sequences, and generalizes John Cremona's tables of elliptic curves [Cre] to dimension bigger than one and weight bigger than two. The database is used by many prominent number theorists. The PI proposes to greatly expand the databases with more information about modular forms, elliptic curves, and modular abelian varieties. In each enumeration problem below, we intend to store the result of the computation in two forms:

1. A plain text file that can be easily parsed, similar to [Cre].
2. SAGE provides robust support for saving nearly arbitrary individual objects. Since SAGE is free and every version of SAGE is archived in multiple locations, this data will not be lost because of changes to SAGE.

4.1 Elliptic Curves

The elliptic curve over $\mathbf{Q}$ with rank 4 and smallest known conductor is the curve $y^2 + xy = x^3 - x^2 - 79x + 289$, with conductor $234446 = 2 \cdot 117223$. Nobody knows if there is a curve with smaller conductor and rank 4, though the PI showed that any such curve has composite conductor by finding all curves of prime conductor up to 234446 (see [JBS03]).

(858) 220-6876 wstein@math.washington.edu http://modular.math.washington.edu

Goal 4.1. Enumerate every elliptic curve up to isogeny of conductor up to 234446.

Cremona [Cre] has spent years methodically enumerating all curves of conductor up to 130000 and computing the invariants in the BSD conjecture (except #Ш). The PI believes an independent computation whose goal is just to find all curves would be extremely valuable, as the following illustrates:

> Bad news: Bill Allombert found an elliptic curve not in my database, conductor 97200 (it was $[0,0,0,0,15]$!!!!) and I just found that there are 40 conductors in the range 90k–100k where there are curves in Stein-Watkins and not in Cremona. Misery!
>
> – email to me from John Cremona, 2006-09-07

The Stein-Watkins table [SW02, BMSW06] mentioned above is a massive table by the PI and Mark Watkins of over 100 million elliptic curves, which was made by systematically enumerating Weierstrass equations. Though it does not contain every curve of a given conductor, a substantial fraction are there.

Cremona enumerates elliptic curves by computing the matrix of the Hecke operator T_2 on the space of weight 2 modular symbols for $\Gamma_0(N)$, then finding the kernels of $T_2 - 2$, $T_2 - 1$, T_2, $T_2 + 1$, $T_2 + 2$. Next, he computes the Hecke operator T_3 restricted to each of the kernels, and decomposes those kernels under T_3, and likewise for T_5, etc. The crucial point is that for the purposes of finding elliptic curves it is not necessary to compute the minimal polynomial of T_2, which is extremely difficult when N is large, e.g., if $N = 200003$ then this dimension is 16667. Another key fact is that Cremona computes Hecke operators using modular symbols, which yield dense matrices, so the linear algebra is difficult.

Goal 4.2. Use the Mestre method of graphs [Mes86] to find all elliptic curves of conductor $N \leq 234446$, for all integers N that are either prime or of the form pM with p prime and $M \leq 10$ or $M = 12, 13, 16, 18$.

The method of graphs, when applicable, very quickly produces *extremely sparse matrices* of the Hecke operators T_p on $S_2(\Gamma_0(N))_{p-\text{new}}$ for small p (e.g., $p = 2, 3, 5, 7, 11$, say). Sparse linear algebra then yields an upper bound on the number of isogeny classes of elliptic curves of conductor N. Consulting the tables of Stein-Watkins and Cremona yields a lower bound. If these disagree, it is likely that we have found a new curve; we then prove this by sparse linear algebra computations over $\mathbf{Q}$, which we do via a multimodular algorithm (see [Ste07, Ch. 7]). Ifti Burhanuddin did partial work toward Goal 4.2 at the MSRI summer graduate student workshop that the PI organized.

David Kohel, Lassina Dembele, and the PI have been working on a strategy to carry out the following computation:

Goal 4.3. Use quaternion algebra arithmetic over $\mathbf{Q}$ (much as in [Dem05]) to compute sparse matrices for several Hecke operators, then proceed as above to find all curves of conductor ≤ 234446 for which some prime exactly divides N.

Computing the quaternion algebra presentation and the Hecke operators in the first place can be time consuming—however, for large levels linear algebra with matrices of Hecke operators dominates the runtime, so obtaining sparse matrices using quaternion algebras or the method of graphs is extremely helpful.

There are only 960 integers up to 234446 that do not satisfy the conditions of Goal 4.3 (which is about 0.4%). For these remaining conductors we might use modular symbols to compute all rational eigenforms:

Goal 4.4. Compute using modular symbols all elliptic curves of the 960 conductors up to 234446 not covered by Goal 4.3.

These calculations are easy to parallelize, and the linear algebra involved in some cases requires a huge amount of memory (which is one reason the PI is requesting a memory upgrade to 128GB for his main server).

4.2 Modular Abelian Varieties

In each case the elliptic curves enumeration in Goals 4.2–4.4 starts by computing matrices of Hecke operators. The PI will store these matrices and also use them to enumerate modular abelian varieties (and, equivalently, newforms in $S_2(\Gamma_0(N))$).

The linear algebra involved in searching for higher-degree factors is much more prohibitive than in searching for elliptic curves.

Goal 4.5. Compute every quotient A_f of $J_0(N)$ for all $N \leq 10000$.

Note, for example, that $\dim S_2(\Gamma_0(10000)) = 1411$, so computing and factoring the relevant minimal polynomials should be possible.

Goal 4.6. Compute every quotient A_f of $J_1(N)$ for all $N \leq 1000$.

For Goal 4.6, we directly compute the spaces $S_2(\Gamma_1(N), \varepsilon)$ for each Dirichlet character ε of modulus N. The main difficulty is linear algebra over large cyclotomic fields. Recent work in progress of the PI on algorithms for multimodular linear algebra over cyclotomic fields will be very helpful (see [Ste07, Ch. 7]).

(858) 220-6876 wstein@math.washington.edu http://modular.math.washington.edu

References

[ARS06a] A. Agashe, K. A. Ribet, and W. A. Stein, *The Manin Constant*, JPAM Coates Volume (2006), `http://modular.math.washington.edu/papers/ars-manin/`.

[ARS06b] ———, *The Modular Degree, Congruence Primes and Multiplicity One*, IMRN Coates Volume (2006), `http://modular.math.washington.edu/papers/ars-congruence/`.

[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. MR 2085902

[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.

[BMSW06] B. Bektemirov, B. Mazur, W. Stein, and M. Watkins, *Average Ranks of Elliptic Curves: Tension Between Data and Conjecture*, Bulletins of the AMS (2006), to appear.

[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

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

[Dem05] Lassina Dembélé, *Explicit computations of Hilbert modular forms on* $\mathbb{Q}(\sqrt{5})$, Experiment. Math. **14** (2005), no. 4, 457–466. MR MR2193808

[GJP+05] G. Grigorov, A. Jorza, S. Patrikis, C. Patrascu, and W. Stein, *Verification of the Birch and Swinnerton-Dyer Conjecture for Specific Elliptic Curves*, (Submitted) `http://modular.math.washington.edu/papers/bsdalg/` (2005).

[Gri05] G. Grigorov, *Kato's Euler System and the Main Conjecture*, Harvard Ph.D. Thesis (2005).

[Gro91] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.

[JBS03] A. Jorza, J. Balakrishna, and W. Stein, *The Smallest Conductor for an Elliptic Curve of Rank Four is Composite*, `http://modular.math.washington.edu/rank4/` (2003).

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

[Ked01] Kiran S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), no. 4, 323–338. MR MR1877805 (2002m:14019)

[Ked04] K. Kedlaya, *Computing zeta functions via p-adic cohomology*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 1–17.

[Kol90] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483. MR 92g:11109

[Kol91a] ———, *On the structure of Selmer groups*, Math. Ann. **291** (1991), no. 2, 253–259. MR 93e:11073

[Kol91b] ———, *On the structure of Shafarevich-Tate groups*, Algebraic geometry (Chicago, IL, 1989), Springer, Berlin, 1991, pp. 94–121.

[McC91] W. G. McCallum, *Kolyvagin's work on Shafarevich-Tate groups*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 295–316. MR 92m:11062

[Mes86] J.-F. Mestre, *La méthode des graphes. Exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata) (1986), 217–242.

[MR04] B. Mazur and K. Rubin, *Pairings in the arithmetic of elliptic curves*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 151–163. MR MR2058649 (2005g:11095)

[MST06] B. Mazur, W. Stein, and J. Tate, *Computation of p-adic heights and log convergence*, To appear in Documenta Mathematica's Coates Volume.

[PR03] Bernadette Perrin-Riou, *Arithmétique des courbes elliptiques à réduction supersingulière en p*, Experiment. Math. **12** (2003), no. 2, 155–186. MR MR2016704

[Rib91] K. A. Ribet, *Lowering the levels of modular representations without*

multiplicity one, International Mathematics Research Notices (1991), 15–19.

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

[Rub91] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68. MR 92f:11151

[Sch83] P. Schneider, *Iwasawa L-functions of varieties over algebraic number fields. A first approach*, Invent. Math. **71** (1983), no. 2, 251–293. MR 85d:11063

[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.

[SIM] SIMUW, *Summer Institute of Mathematics at University of Washington*, `http://modular.math.washington.edu/simuw/`.

[SJ05] W. Stein and D. Joyner, *Sage: System for algebra and geometry experimentation*, Communications in Computer Algebra (SIGSAM Bulletin) **39** (June 2005), no. 2, `http://sage.sourceforge.net/`.

[Ste] W. Stein, *Visibility of mordell-weil groups*, 20, to appear in Documenta Mathematica.

[Ste04a] ———, *The Modular Forms Database* `http://modular.math.washington.edu/tables`.

[Ste04b] ———, *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).

[Ste05] ———, *Elementary Number Theory,* `http://modular.math.washington.edu/ent/`, 2005.

[Ste07] ———, *Explicitly Computing Modular Forms*, Graduate Studies in Mathematics, American Math. Society, 2007, With an appendix by Paul Gunnells.

[SW02] W. Stein and M. Watkins, *A database of elliptic curves—first report*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 267–275. MR MR2041090 (2005h:11113)

[SW04] ———, *Modular parametrizations of Neumann-Setzer elliptic curves*, Int. Math. Res. Not. (2004), no. 27, 1395–1405. MR MR2052021 (2005c:11070)

[Tat66] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geo-*

metric analog, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1965/66, pp. Exp. No. 306, 415–440.