American Mathematical Society

Centennial Fellowship for 2007-2008

Application Form

Membership and Programs Department
American Mathematical Society
201 Charles Street
Providence, RI 02904-2294

Date: November 28, 2006

Name in Full (First, Middle, Last): William Arthur Stein

Present Address:
University of Washington
Department of Mathematics
Padelford C-138
Seattle, WA 98195-4350

Email Address: wstein@gmail.com

Telephone Number: (858) 220-6876

Fax Number: (206) 543-0397

Present Position: Associate Professor of Mathematics

All Positions and Fellowships since Ph.D.:
(see attached)

I am currently employed full time with a tenured position at the University of Washington, which is a North American institution.

Graduate Education: UC Berkeley, Ph.D., 05/01/1995–05/01/2000

Doctoral Thesis Advisor: Hendrik Lenstra

Title of Thesis: Explicit Approaches to Modular Abelian Varieties

Honors Received: I received the Cal@SiliconValley fellowship and the Vice Chancellor Research Grant when I was a Berkeley graduate student.

Publications: (see attached)

References:
Name and institution: **Barry Mazur, Harvard University**
Name and institution: **Kenneth Ribet, UC Berkeley**
Name and institution: **Karl Rubin, UC Irvine**

Research: (see attached)

Signature of Applicant: ____

Positions Held

- Associate Professor of Mathematics (with tenure), University of Washington, September 2006–present.
- Associate Professor of Mathematics (with tenure), UC San Diego, July 2005–June 2006.
- Benjamin Peirce Assistant Professor of Mathematics, Harvard University, July 2001–May 2005.
- NSF Postdoctoral Research Fellowship under Barry Mazur at Harvard University, August 2000–May 2004.
- Clay Mathematics Institute Liftoff Fellow, Summer 2000.

Publication List

1. *Modular forms, a computational approach*, (284 pages), Graduate Studies in Mathematics (AMS), Volume 79, 2007, with an appendix by Paul Gunnells.

2. *The Manin Constant*, with A. Agashe and K. Ribet (22 pages), 2006, to appear in World Scientific's Coate's Volume.

3. *The Modular Degree, Congruence Primes and Multiplicity One*, with A. Agashe and K. Ribet (16 pages), 2006, submitted.

4. *Computation of p-Adic Heights and Log Convergence*, with B. Mazur and J. Tate (36 pages), 2005, to appear in Documenta Mathematica's Coate's Volume.

5. *Verification of the Birch and Swinnerton-Dyer Conjecture for Specific Elliptic Curves*, with G. Grigorov, A. Jorza, S. Patrikis, and C. Patrascu (26 pages), 2005, submitted.

6. *Visibility of Mordell-Weil Groups* (20 pages), 2005, to appear in Documenta Mathematica.

7. *SAGE: System for Algebra and Geometry Experimentation* with D. Joyner, Communications in Computer Algebra, vol 39, June 2005, pages 61–64.

8. *Modular Parametrizations of Neumann-Setzer Elliptic Curves*, with M. Watkins, in IMRN 2004, no. 27, 1395–1405.

9. *Studying the Birch and Swinnerton-Dyer Conjecture for Modular Abelian Varieties Using* MAGMA (23 pages), to appear in a Springer-Verlag book edited by J. Cannon and W. Bosma.

10. *Conjectures about Discriminants of Hecke Algebras of Prime Level* (16 pages), with F. Calegari, in ANTS VI, Vermont, 2004.

11. *Constructing Elements in Shafarevich-Tate Groups of Modular Motives*, with N. Dummigan and M. Watkins, in "Number theory and algebraic geometry—to Peter Swinnerton-Dyer on his 75th birthday", Ed. M. Reid and A. Skorobogatov, pages 91–118.

12. *Approximation of Infinite Slope Modular Eigenforms By Finite Slope Eigenforms* (13 pages), with R. Coleman, in the Dwork Proceedings.

13. *$J_1(p)$ has connected fibers*, with B. Conrad and B. Edixhoven, Documenta Mathematica, **8** (2003), 331–408.

14. *Shafarevich-Tate Groups of Nonsquare Order*, in Progress in Math., **224** (2004), 277–289, Birkhauser.

15. *Visible Evidence for the Birch and Swinnerton-Dyer Conjecture for Rank* 0 *Modular Abelian Varieties* (30 pages), with A. Agashe, appeared in Mathematics of Computation.

16. *A Database of Elliptic Curves–First Report* (10 pages) with M. Watkins, in ANTS V proceedings, Sydney, Australia, 2002.

17. *Visibility of Shafarevich-Tate Groups of Abelian Varieties*, with A. Agashe, J. Number Theory, **97** (2002), no. 1, 171–185.

18. *Cuspidal Modular Symbols are Transportable*, with H. Verrill, LMS J. Comput. Math., **4** (2001), 170–181.

19. Appendix to Lario and Schoof's *Some computations with Hecke rings and deformation rings*, with A. Agashe, Experiment. Math. **11** (2002), no. 2, 303–311.

20. *There are genus one curves over* $\mathbf{Q}$ *of every odd index*, J. Reine Angew. Math. **547** (2002), 139–147.

21. *Component groups of purely toric quotients of semistable Jacobians*, with B. Conrad, Math. Res. Lett., **8** (2001), no. 5–6, 745–766.

22. *The field generated by the points of small prime order on an elliptic curve*, with L. Merel, Int. Math. Res. Notices, 2001, no. 20, 1075–1082.

23. *An introduction to computing modular forms using modular symbols* (10 pages), to appear in an MSRI proceedings volume.

24. *A mod five approach to modularity of icosahedral Galois representations*, with K. Buzzard, Pac. J. Math., **203** (2002), no. 2, 265–282.

25. *Lectures on Serre's conjectures*, with K. A. Ribet, in Arithmetic Algebraic Geometry, IAS/Park City Math. Inst. Series, Vol. 9, 143–232.

26. *Component groups of quotients of* $J_0(N)$, with D. Kohel, Proceedings of the 4th International Symposium (ANTS-IV), 2000, 405–412.

27. *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, with E. V. Flynn, F. Leprévost, E. F. Schaefer, M. Stoll, J. L. Wetherell, Math. of Comp. **70** (2001), no. 236, 1675–1697.

Research Statement

My research reflects the rewarding interplay of theory with explicit computation, as illustrated by Bryan Birch [1]:

> 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.

My main research goal is to carry out a wide range of computational and theoretical investigations into 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.

I am 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. I have also been successful at involving numerous undergraduate and graduate students at all levels in my research, and have started a major project (SAGE) to improve the quality and accessibility of open source mathematics software.

My Ph.D. Research

In my Ph.D. thesis, I investigate the Birch and Swinnerton-Dyer conjecture, which ties together the constellation of invariants attached to an abelian variety. I attempt to verify this conjecture for certain specific modular abelian varieties of dimension greater than one. The key idea is to use Barry Mazur's notion of visibility, coupled with explicit computations, to produce lower bounds on the Shafarevich-Tate group. Nobody has yet proved the full conjecture in these examples; this would require computing explicit upper bounds.

I next describe how to compute in spaces of modular forms of weight at least two. I give an integrated package for computing, in many cases, the following invariants of a modular abelian variety: the modular degree, the rational part of the special value of the L-function, the order of the component group at primes of multiplicative reduction, the period lattice, upper and lower bounds on the torsion subgroup, and the real volume. Taken together, these algorithms are frequently sufficient to compute the odd part of the conjectural order of the Shafarevich-Tate group of an analytic rank 0 optimal quotient of $J_0(N)$, with N square-free, and to give tight bounds in many other cases. I also provide generalizations of some of the above algorithms to higher weight forms with nontrivial character.

My Computational Research

SAGE: Software for Algebra and Geometry Experimentation

I am the director of SAGE—Software for Algebra and Geometry Experimentation [6], a project I started in January 2005. The goal of SAGE is to create quality free open source software for research and teaching in number theory, algebra, geometry, cryptography and numerical computation. SAGE does not reinvent the wheel, but instead builds upon and unifies decades of work on mathematical software. It provides an environment in which to use all of your favorite mathematical software (free or commercial) in a better way. My work so far on SAGE has led to publications and numerous collaborations with undergraduate and graduate students, and there are now over 30 contributors to SAGE. A Centennial Fellowship would increase the amount of energy I could focus on SAGE development and student research projects that involve SAGE.

- SAGE is free open source software for research in **algebra**, **geometry**, **number theory**, **cryptography**, and **numerical computation**.
- SAGE is an **environment for rigorous mathematical computation** built using Python, GAP, Maxima, Singular, PARI, etc., and provides a **unified interface** to Mathematica, Maple, Magma, MATLAB, etc.
- I have organized **several successful SAGE workshops**, and there are many active SAGE developers.
- The primary goal of SAGE is to make **modern research-level algorithms** available in an integrated package with a graphical interface.

The Modular Forms Database

The modular forms database (see [7]) 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 [2] to dimension bigger than one and weight bigger than two. The database is used by many prominent number theorists. I hope to greatly expand the databases with more information about modular forms, elliptic curves, and modular abelian varieties. Support from a Centennial Fellowship would help me to rework and expand the database and make it easier to use.

Theory and Computation

The PI, 3 undergraduates and a graduate student proved the following in [4]:

Theorem 1. *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 the Birch and Swinnerton-Dyer conjecture for E at 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 1. Verify the full Birch and Swinnerton-Dyer Conjecture for every elliptic curve over $\mathbf{Q}$ of conductor < 1000, except for the 18 curves of rank 2.

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

Travel Plans

I would use funds from a Centennial Fellowship to visit Harvard University where I would work mainly with Barry Mazur to **finish a widely accessible book** we are writing on the Riemann Hypothesis, and do work with Mazur on p-adic heights and Heegner points (continuing the work initiated in [5]). Also, one of the main SAGE developers, David Harvey, is a Harvard graduate student so I would work with him on state-of-the-art algorithms for polynomial arithmetic and computation of p-adic heights. I would also visit Ken Ribet in Berkeley in order to **finish a book** on modular forms, Hecke operators, and modular curves that we are writing for the Springer-Verlag GTM series. Our book may be viewed as a sequel to [3] that complements my new AMS book [8]. Finally, I would visit John Cremona to do joint work on computing with modular forms.

References

[1] 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.

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

[3] F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.

[4] G. Grigorov, A. Jorza, S. Patrikis, C. Patrascu, and W. Stein, *Verification of the Birch and Swinnerton-Dyer Conjecture for Specific Elliptic Curves*, To appear in Mathematics of Computation (2005).

[5] B. Mazur, W. Stein, and J. Tate, *Computation of p-adic heights and log convergence*, (2006), To appear in Documenta Mathematica's Coates Volume.

[6] SAGE, *Software for Algebra and Geometry Experimentation,* `http://sage.math.washington.edu/sage`.

[7] W. Stein, *The Modular Forms Database,* `http://modular.math.washington.edu/tables`, (2006).

[8] ———, *Explicitly Computing Modular Forms*, Graduate Studies in Mathematics, vol. 79, American Math. Society, 2007, With an appendix by Paul Gunnells.