CSUMS: Undergraduate Computational Research in Arithmetic Geometry

1 Major Highlights

- A group of 6 undergraduate students each year will do research with a computational flavor in number theory and arithmetic geometry. Each project will be directly relevant to research on the Birch and Swinnerton-Dyer conjecture and on modular functions.
- Students will become well versed in how to use computation to do research in mathematics, and these skills will carry over to future graduate or professional work.
- Students will write proposals, give presentations, and speak at national workshops.
- This project will strengthen the University of Washington mathematics department's senior thesis program and course offerings.
- Research projects will involve Sage, which is free open source mathematical software.

2 Introduction

> "The history of mathematics, and of number theory in particular, is studded with examples of general conjectures made after the examination of special cases actually calculated, and the generalization finally proved."
>
> — Oliver Atkin, 1968.

The proposed project is for a group of 6 undergraduate students each year to do research with a strong computational emphasis in number theory and arithmetic geometry, where each project will be relevant to research on the Birch and Swinnerton-Dyer conjecture (BSD conjecture) or modular functions. Participants will become well versed in the practical use of computation in advanced mathematical research, gain knowledge about mathematical software, make long-term connections with a vibrant research and development community, and contribute tools that will be used by expert researchers and students. Number theory is a venerable research area that draws strongly from many areas of mathematics, and the BSD conjecture is one of the deepest problems in number theory, so student research will make connections with a wide range of mathematics. Modular curves, and the functions which uniformize them, have a complexity that belies their classical origins. They are the sine qua non of modern number theory, and the key to such recent advances as Richard Borcherds' Fields Medal work on the Monstrous Moonshine Conjecture. Our program is structured so that students will learn teaching and writing skills, which will prepare them to apply computational mathematics techniques in graduate school and industry.

The PI carried out a project with 6 students on computational verification of the Birch and Swinnerton-Dyer conjecture during Summer 2004 at Harvard University (see **?** and **?**). The co-PI directed the research of 5 students from Columbia University during that same

summer. The current proposal seeks to extend these to a more ambitious project at University of Washington (UW) involving a cohort of 6 students each year for three years, with stronger computational and educational components. The PI's experience collaborating with undergraduates in research projects has convinced him that undergraduates can do work that is esteemed by the mathematical research and education communities.

UW has many active researchers working on number theory, arithmetic geometry, and related areas, including William Stein (PI on this grant), Ralph Greenberg, Neal Koblitz, Trevor Arnold (postdoc on this grant), and Chuck Doran (co-PI on this grant).

2.1 Prior Support and Related Proposals

This is a new project, and as such has received no direct prior support. However, the PI has received substantial support over the last 6 years for a range of joint research projects with undergraduates. The PI received support from the Harvard College Research Program for 8 student research projects. The PI was awarded NSF grant DMS-0555776 (and DMS-0400386) in the amount of $177,917 for the period 2004–2007, and funds from this grant were used to run a workshop at UCSD (Sage Days 1) that had one featured undergraduate speaker (Steven Sivek, MIT) and that several undergraduates participated in (David Roe, MIT; Alex Clemesha, UCSD; and Naqi Jaffery, UCSD). That grant was also used to partially fund Sage Days 2 (October 2006 at UW), in which 6 undergraduates actively partcipated and 1 gave a featured talk. The PI received support for similar workshops in January 2007 at IPAM (UCLA) and from VIGRE/PIMS for Sage Days 4 (June 2007 at UW). He has also received full funding for two upcoming Sage Days workshops on number theory using Sage—one is at the Clay Math Institute in October 2007, and another is at the Heilbronn Institute in Bristol, UK in November 2007. The PI has also received funding from the department VIGRE grant for 6 undergraduate students to work on research during the 2006–2007 academic year.

The PI received NSF grant DMS-0653968 from the ANTC program to support his personal research for 2007–2010 on the Birch and Swinnerton-Dyer conjecture. The PI also received NSF grant DMS-0703583 to support one postdoc for three years, who will work on developing linear algebra algorithms and implementations for Sage; his work will be important for some of the student projects, and he will also serve as a mentor. The PI is also currently applying for an NSF FRG grant jointly with Andrew Booker, Noam Elkies, Brian Conrey, Michael Rubinstein, and Peter Sarnak to provide more postdoctoral and graduate-student oriented supported for a related project that involves invariants of modular forms and L-functions.

The co-PI will submit in November 2007 a proposal to NSF on "Geometry, Periods, and Moduli of Calabi-Yau Manifolds" which includes funding for his research with collaborator Adrian Clingher and graduate students Ursula Whitcher and Jacob Lewis on the differential equations satisfied by modular parametrizations.

The purpose of the present proposal is to complement the above two NSF-funded research projects, and the co-PI's proposed research project, with an extensive undergraduate presence. This will have a significant positive impact on the training of a cohort of undergraduates in the use of serious computational techniques in mathematical research.

3 Nature of Student Activities

The Birch and Swinnerton-Dyer conjecture (BSD conjecture) is one of the central problems in number theory. For example, it is one of the seven Clay Math Institute million dollar millenium prize problems **?**. Students will do computational research into the BSD conjecture, and in so doing they will develop substantial skills in mathematical research.

Modular curves form a key entry-point into modern number theory. In addition to their defining property – that of describing moduli of families of elliptic curves with conditions – they are themselves gems of arithmetic geometry. By focusing on the case of modular curves of genus zero, the study of uniformization of these curves by modular functions reduces to working with explicit q-series. This reduction is already sufficient for cutting-edge applications such as Moonshine, and yet is extremely accessible both computationally and mathematically.

In Section 3.1 we describe the BSD conjecture, then in Section 3.2 we detail some aspects of the moonshine modular functions. In Section 3.3 we introduce the mathematical software Sage. Finally, Section 3.4 describes several research projects that the students would attack.

3.1 The Birch and Swinnerton-Dyer Conjecture

Research into the Birch and Swinnerton-Dyer conjecture reflects the rewarding interplay of theory with explicit computation in number theory, as illustrated by Bryan Birch **?**:

> "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."

In this section we describe this famous conjecture.

An *elliptic curve* E is a nonsingular projective cubic curve over the rational numbers that is defined by an equation

$$y^2 + ay + b = x^3 + cx^2 + dx + e,$$

with $a, b, c, d, e \in \mathbf{Q}$. For example, the equation $y^2 + y = x^3 - x$ defines an elliptic curve.

The set $E(\mathbf{Q})$ of rational points on E forms a natural finitely generated abelian group, so

$$E(\mathbf{Q}) \approx \mathbf{Z}^r \oplus T,$$

where $r \geq 0$ is an integer called *the rank of* E and T is a finite abelian group. For example, for $y^2 + y = x^3 - x$, we have $E(\mathbf{Q}) \approx \mathbf{Z}$, with generator the point $(0, 0)$. The sum of two elements $P, Q \in E(\mathbf{Q})$ is obtained by drawing the line through P and Q, finding the third point R of intersection with E, then considering the line L through R and the unique projective point at infinity on E; the other point of intersection of L with E is the sum $P + Q$. For example, on $y^2 + y = x^3 - x$, we have

$$(6, 14) \oplus (2, -3) = \left(\frac{161}{16}, -\frac{2065}{64}\right).$$

Note that the sum is a non-obvious new solution to $y^2 + y = x^3 - x$; amazingly, one can easily generate arbitrarily complicated solution this way.

By counting the number of points on E modulo each prime p, we also obtain a sequence

$$a_p = p + 1 - \#E(\mathbf{F}_p),$$

one for each prime number. For example, for $y^2 + y = x^3 - x$ the numbers a_p with $p < 50$ are

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
a_p	-2	-3	-2	-1	-5	-2	0	0	2	6	-4	-1	-9	2	-9

We put these counts together in a generating function

$$L(E, s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}},$$

called the L-series of E (in fact, one must slightly modify finitely many "bad factors", but this is a technicality that we ignore here). The deep modularity theorem of Wiles et al., which was the key step in Wiles's proof of Fermat's Last Theorem, implies that $L(E, s)$ extends uniquely to a complex analytic function on the whole complex plane. It thus makes sense to consider the behavior of the analytic function $L(E, s)$ in a neighborhood of $s = 1$.

We now introduce *the BSD conjecture*, which is the union of the following two conjectures:

Conjecture 3.1 (Birch and Swinnerton-Dyer)**.** *Let E be an elliptic curve over $\mathbf{Q}$. Then the rank r of $E(\mathbf{Q})$ is equal the order of vanishing $\operatorname{ord}_{s=1} L(E, s)$ of $L(E, s)$ at $s = 1$.*

Conjecture 3.1 exactly as stated is the million dollar Clay Math problem. There is also a more refined conjecture, which involves several quantities that we will *not* define:

Conjecture 3.2 (Birch and Swinnerton-Dyer)**.** *Let E and r be as above. Then*

$$\frac{L^{(r)}(E, 1)}{r!} = \frac{\#Ш(E) \cdot \Omega_E \cdot \operatorname{Reg}_E}{\#E(\mathbf{Q})^2_{\text{tor}}} \cdot \prod_{p|N} c_p.$$

The goal of this proposal is for a group of undergraduates to carry out a wide range of computational and theoretical investigations into elliptic curves motivated by the above conjectures, and produce useful results, conjectures, data, and software.

The PI expects that students in the project will continue to contribute after their first year. Stein is a co-PI on Jim Morrow's summer mathematics REU at UW, and some students from this project will likely participate in the REU. For example, Stein worked with Emily Kirkman and Tom Boothby during the academic year on research, and they both participated in the REU during Summer 2007. The topic of Morrow's REU has traditionally been *Inverse Problems in Electrical Networks*, but the REU has grown to include number theory.

3.2 Moonshine modular functions

> "It has been approximately twenty-five years since John McKay remarked that 196 884 = 196 883 + 1. That time has seen the discovery of important structures, the establishment of another deep connection between number theory and algebra, and a reinforcement of a new era of cooperation between pure mathematics and mathematical physics. It is a beautiful and accessible example of how mathematics can be driven by strictly conceptual concerns, and of how the particular and the general can feed off each other. " — Terry Gannon, 2004.

The remark of McKay referred to in the quote **?** is the observation that the left hand side, which is the coefficient of $q = e^{2\pi\imath\tau}$ in the q-series expansion for the elliptic modular function $j(\tau)$ about $\tau = \imath\infty$

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots \ ,$$

is 1 more than the smallest dimension of nontrivial irreducible representations of the monster sporadic simple group. In fact, the coefficient of q^2 in this expansion minus the coefficient of q equals another such dimension, and there are recursions relating the rest of the coefficients to dimensions of the irreducible representations of the monster. Generalizations of this observation, due to Conway and Norton and which apply to normalized q-series for many genus zero modular functions, go under the heading of the Monstrous Moonshine Conjecture **?**.

Calculations by computer have played an important role in the exploration of Moonshine from very early on. This includes computations by Atkin, Fong, and Smith which first established the existence of the moonshine module **?**. On a much more basic level, the accessibility of the basic mathematical ingredients has led to highly successful non-Moonshine computational projects involving undergraduates. In particular, Imin Chen (then a Queens University undergraduate, now on the faculty at Simon Fraser University) and Noriko Yui (Queens University) used computational methods to explore generalizations of the theory of principal moduli for Moonshine modular functions **?**. More recently, Bong Lian (Brandeis University) supervised the Schiff Fellowship research of Joshua Wiczer, resulting in a complete list of uniformizing differential equations for the moonshine modular functions. They have posted their joint paper "Genus Zero Modular Functions" to the arXiv as math.NT/0611291.

For the purposes of our undergraduates working in this area, the primary mathematical objects of study will be the modular functions which arise in the Moonshine conjectures. These generalize the elliptic modular function $j(\tau)$ above. Like $j(\tau)$ they are invariant under certain replacements $\tau \mapsto (a\tau + b)/(c\tau + d)$. For $j(\tau)$, these transformations are those in the elliptic modular group $\mathrm{PSL}(2, \mathbf{Z}) \subset \mathrm{PSL}(2, \mathbf{R})$. The function $j(\tau)$ itself can be thought of as uniformizing the genus zero modular curve with one cusp (at $\imath\infty$) and two elliptic points, one each of order 2 and 3. This is nothing but the j-line, the (coarse) moduli space for elliptic curves over $\mathbf{C}$, realized now as the (genus zero) quotient of the upper half plane by the action of $\mathrm{PSL}(2, \mathbf{R})$. For the more general moonshine modular functions there are analogous subgroups of $\mathrm{PSL}(2, \mathbf{R})$ and corresponding genus zero quotients of the upper half plane by these groups. This raises the question: *How can one describe these generalizations of* $j(\tau)$ *and of* $\mathrm{PSL}(2, \mathbf{Z})$*?*

The most classical approach involves first the subgroup $\Gamma_0(n) \subset \mathrm{PSL}(2,\mathbf{Z})$, consisting of $a, b, c, d \in \mathbf{Z}$ such that c is congruent to 0 modulo n, and then its extension $\Gamma_0(n)^{+n} \subset \mathrm{PSL}(2,\mathbf{R})$ by the Fricke involution $\tau \mapsto -1/(n\tau)$. The quotient of the upper half plane by this first is the modular curve $X_0(n)$. The quotient of the upper half plane by the latter is denoted $X_0(n)^{+n}$, and it has genus zero when $X_0(n)$ does. For certain n, however, $X_0(n)^{+n}$ may have genus zero when $X_0(n)$ does not (e.g., for $n = 11$). The generalization of $j(\tau)$ for $\Gamma_0(n)^{+n}$ is then a parameter on the genus zero curve $X_0(n)^{+n}$, expanded about a cusp (placed at $\imath\infty$).

The curve $X_0(n)^{+n}$ sits naturally in the surface obtained by taking the product of two copies of the upper half plane and quotienting out by $\mathrm{PSL}(2,\mathbf{R}) \times \mathrm{PSL}(2,\mathbf{R}) \rtimes \mathbf{Z}/2\mathbf{Z}$, where the factors of $\mathrm{PSL}(2,\mathbf{R})$ act separately on the two copies of the upper half plane and the factor of $\mathbf{Z}/2\mathbf{Z}$ exchanges the copies. The curve $X_0(n)^{+n}$ so presented is actually cut out by a *modular equation*, the implicit equation given by an algebraic relation between the functions $j(\tau)$ and $j(n\tau)$. One problem with modular equations is their complexity. Already, for $n = 2$, the modular equation for $X_0(2)^{+2}$ takes the form

$$\begin{aligned} F_2(x,y) &= (x^2 - y)(y^2 - x) - 393768\,(x^2 + y^2) - 42987520\,x\,y \\ &\quad -40491318744\,(x + y) + 12098170833256\ . \end{aligned}$$

By contrast, there are simple *parametrizations* of modular equations, and a simple geometric explanation for many of these. Investigating the properties of such parametrizations using tools from algebra, geometry, and complex analysis, and differential equations will be the focus of the undergraduates working on this project.

3.3 Sage: Open Source Mathematical Software

> "Students at UW did not have any easy way to get started doing mathematics research (no washing petri dishes, etc.). This is something that I have experienced personally and know that many of my math major friends are frustrated about. Sage is opening the door to advanced mathematics research to many students that wouldn't have this chance otherwise." — Yi Qiang, UW undergraduate.

The PI is the main author and director of the Sage **?** open source mathematical software project, which he started in January 2005, which nows has well over 1000 users. Both the Sage development model and the technology itself is distinguished by a strong emphasis on openness, community, cooperation, and collaboration: *Sage is about building the car, not reinventing the wheel*. Sage is over two hundred thousand lines of new code that uses standard open source libraries and programs (such as GAP **?**, Maxima **?**, Singular **?**, PARI **?**, and Python) to create unified and powerful open source mathematical software.

Sage is in some ways similar to the popular commercial systems such as Maple or Mathematica, but is designed to focus much more on cutting edge mathematical research. For example, in addition to traditional symbolic computation like in Maple or Mathematica, one can also define a huge range of mathematical structures such as groups, rings, fields, monoids, modules, vector spaces, elliptic curves, number fields, L-functions, ζ-functions, modular forms, and other more exotic objects in Sage. In this sense, Sage is similar to Magma **?**, which is the most successful commercial system aimed at advanced research in algebra, group theory,

and arithmetic geometry. However, Sage has much more functionality for computing with L-functions of elliptic curves than any other system (including Magma) due to work of the PI, C. Wuthrich, M. Rubinstein, T. Dokchitser, M. Watkins, and others, which makes Sage appropriate for this project.

Some differences between Sage and the commercial systems mentioned above are that Sage is free, the source code to all of Sage is available for anyone to view, and development work on Sage is done in the open by nearly 100 developers.

Undergraduate work on Sage has been a key reason for the rapid growth and fresh ideas in Sage. NSF support is critical to the involvement of undergraduates in Sage development and this project. For example, instead of designing web pages for another department, the mathematics major Tom Boothby has been working for the PI on Sage development and number theory research.

3.4 Specific Projects

This section describes some specific projects that the students would work on during the 3 years that this program would run. Before each year the projects will be re-evaluated by the PI, co-PI, and postdoc in light of previous experiences and student progress.

The projects listed here all involve sophisticated mathematics, but the PI is confident proposing them, because he has worked with over two dozen undergraduates at Harvard, UCSD and UW, and has found repeatedly that given sufficient encouragement, time, support, and a genuine belief in their potential, these students are successful. In fact, many of the projects listed below grew out of undergraduate research that the PI carried out with students during the last 6 years. Also, keep in mind that each student will be involved in this project for a full academic year, so students have more time to master and absorb deep mathematics. Moreover, the PI has written extensively on all the topics discussed below, in connection with courses he has taught, so ample reading materials are available.

3.4.1 Computational Investigation of Conjecture 3.1

Conjecture 3.1 of Section 3.1 has been verified for millions of particular elliptic curves of rank $0, 1$, and 2 by work of Cremona, Watkins, and others **??**, and for many curves of rank 3 using **?**. The paper **?** discusses data about many elliptic curves that (appear to have) rank 4, which we have enumerated. For interesting and deep reasons, Conjecture 3.1 has not been verified for even a single elliptic curve of rank 4, e.g., the curve E given by

$$y^2 + xy = x^3 - x^2 - 79x + 289,$$

of rank 4, with generators $(-9, 19), (-8, 23), (-7, 25), (4, -7)$. It is known that $\mathrm{ord}_{s=1} L(E, s) = 2$ or 4, but there is no known way to decide which. Students will compute $L''(E, 1)$ to several hundred (or even thousand) decimal digits of precision for many specific elliptic curves of rank 4. This—of course—can never prove that $L''(E, 1) = 0$, without further information, but it could disprove it. Either way, this computation will improve algorithmic and practical tools for computing with L-series, e.g., drawing on **?**.

Students will also analyze distributional statistics (related to the Sato-Tate distribution; see **?**) for the integers $a_p = p+1-\#E(\mathbf{F}_p)$ for hundreds of elliptic curves of rank 4 and compare this to statistics for elliptic curves of rank 2. This will extend a project the PI directed last year with Barry Mazur (Harvard) and undergraduates Chris Swierczewski and Bobby Moretti of UW.

3.4.2 Computational Investigation of Conjecture 3.2

Conjecture 3.2 of Section 3.1 has been nearly verified for all but 18 of the 2463 (optimal) elliptic curves in Cremona's landmark book **?**, due to work of the PI, C. Wuthrich (see **?**), and many students. Students will finish this verification (except for the 18 rank 2 curves); this is still a nontrivial task since the remaining curves are perhaps the most difficult and may require interesting theoretical advances. They will next ensure that it is possible for other researchers to automatically replicate the verification in a reasonable amount of time, which will improve ad hoc algorithms and implementations, and speeding up and documenting code. Also, the verification in some cases relies on computing ranks of 3-Selmer groups, an algorithm that is only implemented in Magma (which is closed source). This 3-descent algorithm will have to be studied and implemented in Sage from scratch, which will likely result in improvements to the existing algorithm, and provide an important tool.

Another project is to verify as much as possible about Conjecture 3.2 for Cremona's much larger online dataset of curves. This will be a new calculation that will provide ample opportunities for collaboration and result in a motivating paper about what current theory and computation do not allow us to deduce in a reasonable amount of time about BSD.

Conjecture 3.2 has never been completely verified for even a single elliptic curve of rank ≥ 2. For example, consider the curve E defined by the equation $y^2 + y = x^3 + x^2 - 2x$. This curve has rank 2, with group generators $(-1, 1), (0, 0)$. The quantity $Ш(E)$ in Conjecture 3.2 is an abelian group, which is not known to be finite for the curve E, though Conjecture 3.2 predicts that $\#Ш(E) = 1$. Students will attempt to prove using p-adic and other methods that $Ш(E)[p] = 0$ for all primes $p < 10^4$, and carry out similar calculations for several hundred other rank 2 elliptic curves. Such verification is reasonably straitforward for most—but not all—primes, by explicit computation of p-adic L-series and Iwasawa theory, as explained in **?**. For some primes, i.e., those where $a_p = 0$, the computation is more involved. A major part of this project will be to search for algorithms to make this verification much faster, and to try to find a way to verify triviality for infinitely many primes at once.

3.4.3 Computational Investigation of p-adic Analogues of Conjecture 3.1

In **?** Mazur, Tate and Teitelbaum constructed p-adic analogues of Conjectures 3.1 and 3.2 of Section 3.1 for almost all primes p. For several hundred thousand elliptic curves and primes p, students will compute the p-adic analogues of the quantities in Conjecture 3.2 to high precision. In many cases this will be enough to mostly verify the conjecture (see **?**). This will involve developing algorithms for computing these objects to high precision.

Students would also implement Rob Pollack and Glenn Steven's algorithm for computing p-adic L-series to high precision. This algorithm has so far only been partly implemented in

an ad hoc way, and never been generally available or easy to use.

Students would use the result of the work above to create tables of p-adic L-series and related p-adic invariants of elliptic curves, and based on these they would formulate conjectures.

Ralph Greenberg, a professor at UW, is one of the world's leading experts in this area, and would be a valuable resource to this project.

3.4.4 Computing Heegner Points

Perhaps the fundamental question behind the Birch and Swinnerton-Dyer conjecture is the following: *Given an elliptic curve E how can we systematically construct the points on E?*

As mentioned above, the elliptic curve E defined by $y^2 + y = x^3 - x$ has rank 1 with group generated by $(0, 0)$. There is an explicit analytic construction of the point $(0, 0)$, which goes under the moniker of *Heegner points*, that involves quadratic forms and a map from the complex upper half plane to the group of complex solution to the elliptic curve equation. Amazingly, for any elliptic curve of rank 1 there is such a construction, and it is perhaps the most potent tool for work on the Birch and Swinnerton-Dyer conjecture. To date, nothing similar is known *or even conjectured* for curves of rank 2 or larger.

There is no general purpose software for computing Heegner points for the purposes of theoretical research. Magma computes Heegner points internally for certain calculations, and there are packages for PARI that can do some Heegner point calculations. Students will create an optimized general purpose package for computing Heegner points, which will be specifically designed for investigating theoretical questions about them (and their corresponding *Euler systems*), e.g., the questions raised in Kolyvagin's tantilizing paper **?**. The algorithms will also draw on recent work of Watkins, Delaunay, and Jetchev-Lauter-Stein **?**.

Once this package is in place, students will investigate the Kolyvagin subgroup of $E(\mathbf{Q})$ that is defined at the end of **?** for *any elliptic curve*, even those of rank ≥ 2. They will attempt to compute something about this group in concrete examples, and possible work to gather data that might lead to a completely new conjectural analogue of the Gross-Zagier theorem **?**.

3.4.5 Fricke's Groups and Computation of Normal Forms for Families of Elliptic Curves and K3 Surfaces

Parametrizations of the genus zero curves $X_0(n)^{+n}$ by functions quadratically related to rational functions were obtained by Cohn, who adapted the computational methods of Fricke. Still better parametrizations can be derived from the functional invariants of n-isogenous families of elliptic curves, though there are few cases where such families are explicitly known.

First, starting from the parametrizations of Fricke-Cohn, the students will derive explicit equations for n-isogenous families of elliptic curves whose functional invariants parametrize the modular curves $X_0(n)$. This step is necessarily restricted to the values of $n \geq 2$ for which $X_0(n)$ has genus zero, i.e., n equal to 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, and 25. In these cases, there is an alternative construction of the parametrizations using Gauss hypergeometric functions due to Maier (math.NT/0611041: "On Rationally Parametrized Modular Equations"), which they can use for comparison. This step requires that they develop both an understanding of

elliptic curves over $\mathbf{C}$ in various normal forms (e.g., Weierstrass cubics, Legendre hyperelliptic presentation, Hasse normal form) and also skill with techniques for optimization.

Next, the students will extend their constructions to those coming from parametrizations of $X_0(n)^{+n}$, still of genus zero for n equal to 11, 14, 15, 17, 19, 20 , 21, 23, 24, 26, 27, 29, 31, 32, 35, 36, 39, 41, 47, 49, 50, 59, and 71. What is more natural to consider here, rather than families of pairs of elliptic curves, is families of K3 surfaces of a very special type (so-called M_n-polarized K3 surfaces). The explicit correspondence between these two classes of geometric objects was established by Clingher-Doran in **?** using a normal form as singular quartic hypersurfaces which applies equally well for any n. The students will explore alternative normal forms for K3 surfaces, themselves each presented as families of elliptic curves over a rational base.

3.4.6 Computation of Modular Parametrizations for Moonshine Modular Equations

The modular equations for the elliptic modular function $j(\tau)$ correspond to the curves $X_0(n)^{+n}$; these are genus zero for the values of n listed in §3.4.5. Analogously, there are generalized modular equations due to Cummins and Gannon **?** for the moonshine modular functions; for each moonshine modular function some of these are still genus zero.

The final project is for the students to adapt to the setting of general moonshine modular functions the methods used by Fricke and Cohn **?** to obtain parametrizations of the curves $X_0(n)^{+n}$. This computation involves using known expressions for the monstrous modular functions in terms of modular forms, special theta functions, and cruder approximation methods with power series. We restrict our attention to the cases where the generalized modular equation for the moonshine modular function is itself of genus zero. It is known that the moonshine modular functions can be characterized as q-series by the property that they satisfy certain infinite families of generalized modular equations. Computational evidence **?** suggests in fact that they can be characterized as satisfying modular equations just for n equal 2 and 3. The students will investigate alternative means of characterizing the moonshine modular functions through properties of the parametrizations of their generalized modular equations.

4 Overview

4.1 Target Student Participants

The student participants in this project will be majors in the mathematical sciences with an interest in research and in using computation to improve mathematics research and education.

Since many of the problems are at the forefront of research, students will become involved with advanced mathematics. For example, after Tom Boothby (undergraduate, UW) began working on Sage, he carried out a project to enumerate and draw all possible isogeny diagrams of elliptic curves, in collaboration with the world leader in elliptic curve enumeration (John Cremona). Another student, Jennifer Balakrishnan (Harvard) implemented much of a program for computing p-adic heights on elliptic curves, and gave three talks on the underlying theory and implementation; this work eventually led to a published paper written by David Harvey (grad student, Harvard).

The PI intends that students involved with this project will become *future leaders in tranforming how computational methods are used in mathematical research.*

4.2 Organizational Structure and Timetable

The students will be paid by the hour for up to 15 hours of work per week. Of this time, 4 hours each week will be spent in a structured "working sprint", which will take place in the Sage lab each Thursday 2pm–6pm, and will involve the PI, all the students participating in the project, and interested graduate students. The sprint will start with 15–30 minutes spent organizing the project groups, followed by 3 hours of intense research and computer work. The last 30 minutes will be a wrapup session in which the students describe their progress during the sprint.

Graduate students will be encouraged to play an informal mentoring roll and to be involved in the working sprints and talks. There are currently numerous graduate students involved in Sage work at UW, including the following three: Robert Bradshaw, Josh Kantor, and Robert Miller. Each of these three have mentored several undergraduate projects. The co-PI is Ph.D. advisor of four UW graduate students. Of these, Ursula Whitcher and Jacob Lewis are particularly well-suited to help mentor undergraduate projects involving modular functions.

In addition to the sprint mentioned above, students will also be expected to attend a 1-hour meeting each Tuesday. The 1-hour meeting will be a lecture by the PI or student about each of the student projects (giving relevant background), or about how to use relevant software.

The PI will also spend at least 4 additional hours in the Sage lab each week to direct student projects. This will allow him to meet with each student individually every week.

The timetable for the year will be as follows. This is based mainly on the PI's extensive experience mentoring 8 senior undergraduate theses at Harvard University (during 2003–2005), and working with 6 undergraduates on research for a year at UW.

1. **A crash course in computation:** The first 5 weeks will be a general crash course in the practical use of computation as an aid to mathematical research. Topics will include programing in Python with Sage, creating and querying object-oriented and relational databases, setting up and running distributed computations, and writing optimized compiled code. We will also discuss the meaning of "proof" in computational mathematics and standards of ethics and verifiability in the context of computer-assisted mathematical research. Students will gain a general understanding of some of the capabilities of most major mathematical software and libraries. This course will involve lectures, exercises, and group and individual student projects. The PI will be teaching a course in Spring 2008 at UW that expands upon the above topics, and which will provide course materials for the crash course for the first cohort of undergraduates.
2. **A crash course in number theory:** The second 5 weeks will be a crash course in number theory. Topics will include prime numbers, integer factorization, the Euclidean algorithm, continued fractions, and sums of squares. Students will read selected parts of the PI's book *Elementary Number Theory*, which culminates with a discussion of the BSD conjecture. Students will then read materials based on a book the PI is co-authoring with Barry Mazur about the Riemann Hypothesis that is aimed at the undergraduate level,

which the PI used for a 2-week summer workshop for high school students (SIMUW 2007), and Mazur has used for numerous large expository talks. Students will also learn about number fields, Galois groups, class groups and unit groups of number fields. Students will read the PI's book on algebraic number theory, which he wrote based on two *undergraduate* courses he taught at Harvard in 2004 and 2005 on this topic, and other books. Finally, students will learn about *elliptic curves*, including normal forms, the group law, L-function, the BSD conjecture, basics of Galois cohomology, elliptic surfaces. Students will read survey articles, books (Silverman-Tate), and parts of the PI's preliminary book on the BSD conjecture, which grew out of an introductory graduate course that he taught at UW in 2007.

3. **Choose a project:** During the final week before the Winter holiday break, students will choose a research project. They will then be given reading materials.
4. **Intense research:** Right after returning from the Winter holiday, and for the next 8 weeks, students will begin serious work on their research projects. This will include reading theoretical background material and giving talks about what they learn, doing small and large-scale computations using software, creating tables. Students will also learn, improving, and implement new and existing algorithms, and make conjectures based on data. The students will spend about 15 hours a week working on this research. Of that, 6 of those hours will be spent in the collaborative Sage lab working sprints.
5. **A rough draft:** After 8 weeks of open-ended research, students will spend 2 weeks writing up a rough summary of what they have discovered, accomplished, and learned, before Spring break. This will include expositions of theoretical background material and notes from talks, a report describe all data they gathered, a description of any algorithms they implemented, and what improvements or modifications they made to existing algorithms that are in the literature, conjectures, and a sketches of any results they may have proved.

Since all students will be working on projects related to the BSD conjecture, the student work will be tightly related. The rough drafts will be distributed to all the other students (and to the PI, co-PI, postdoc, and graduate student mentors) for feedback.

Write it up: After returning from Spring break, students will critically revisit their rough drafts. They will then spend the following seven weeks writing up their theoretical and computational results, and documenting any code they implemented.

Students will finish their projects 2 weeks before finals, and the program will officially end 2 weeks before finals, which will give students time to focus on studying for exams.

5 Connection to Regular Academic Studies

5.1 Local Impact

UW has a senior thesis program, and students who are seniors will be encouraged to submit their project as a senior thesis. At UW, the senior thesis in mathematics is currently not so popular. After researching this problem, the PI suspects that this lack of popularity may be partly the result of insufficient structure in the mathematics department for the senior thesis;

also, many honors students at UW are dual majors and consequently they end up doing a senior thesis in their other major. Funding this proposal would likely directly address this.

Undergraduate participants in the project will be encouraged to give talks in the UW undergraduate mathematics seminar, the UW number theory seminar, and the UW computational number theory and cryptography seminar. In fact, in 2007 the UW undergraduate Chris Swierczewski did research with the PI and Barry Mazur on refinements to the Sato-Tate distribution and his talk in the number theory seminar on the topic was the most well attended talk of the year. There is also an undergraduate research project day at UW in April, in which students would participate. Also, UW has been successful in the international applied math modeling contest, and students in this CSUMS project would be encouraged to interact with students preparing for the applied math modeling contest.

5.2 National Impact

The Birch and Swinnerton-Dyer conjecture is a problem of extreme interest to most number theorists, so any successful work on it will have a national impact. Moreover, any free software that students produce is likely to be useful to many other mathematicians and students. For example, much work related to the BSD conjecture requires improving algorithms for computing modular forms, which in turn requires improving methods and creating better tools for exact linear algebra and polynomial arithmetic. Thus work the students do is likely to have a positive effect nationally in a range of areas.

6 Research Environment and Mentoring Activities

The PI is experienced at organizing student seminars and presentations; he ran a Sage seminar at UW in 2006 with numerous undergraduate talks, he ran an MSRI graduate student summer school **?**, and led two freshman seminars at Harvard (one on elliptic curves and one on Fermat's Last Theorem) which consisted of 3 hours of student presentations per week.

Having a common space for the students to come together and work is vital to encouraging collaboration. Fortunately, the Computer Science department at University of Washington has donated a Sage lab to the project, which provides ample space for up to 6 students to work at once. Each student will be given a key to the lab. There will also be a *weekly Sage seminar* attended by the PI's, other interested faculty and students.

The PI has a strong **track record of mentoring undergraduates** in theoretical and computational research. During the last five years he has directed over 24 projects with a nontrivial research component at Harvard, UCSD, and UW, many of which are available at **?**. For example, he directed the Harvard senior theses of Jayce Getz, John Gregg, Dimitar Jetchev, Andre Jorza, Seth Kleinerman, Daniellie Li, Chris Mihelich and David Speyer, and he ran summer research programs on the Birch and Swinnerton-Dyer conjecture at Harvard during 2003 and 2004 with five students (Jennifer Balakrishnan, Andrei Jorza, Stefan Patrikas, Jennifer Sinnott, Tseno Tselkov). When Baur Bektemirov was a freshman at Harvard, he did a year-long project with the PI in which he computed surprising statistics about elliptic curves that led to a joint paper in the Bulletins of the AMS (**?**). The PI also worked for a year with Kevin Grosvenor, another Harvard freshman, on drawing pictures of L-functions. At UCSD

the PI worked on Sage development with Naqi Jaffery and Alex Clemesha, and since April 2006 at UW he has worked with UW undergraduates Tom Boothby, Emily Kirkman, Bobby Moretti, and Yi Qiang and MIT undergraduates Steven Sivek and David Roe on research related to Sage.

The PI has been at UW since 2006, and has been pleased with the undergraduate students he has worked with. The mathematics undergraduate program at UW attracts some of the best UW students: the department at UW has had five Goldwater Scholars in the past three years, three of the past four College of Arts and Sciences Deans Medalists in Science, seven teams of Outstanding Winners in the CO-MAP Mathematical Contest in Modeling during the past six years, and most recently a Rhodes Scholar, an Astronaut Foundation Scholar, and a Davidson Fellow. Also, the Seattle area has substantial programming talent due to the proximity of Microsoft and Digipen.

7 Student Recruitment and Selection

The PI finds and builds professional relationships with students by a combination of methods. He gives talks and gets involved with student activities at UW, e.g., in 2006 and 2007 he led a 2-week SIMUW high school workshop on computational aspects of the Birch and Swinnerton-Dyer conjecture and the Riemann Hypothesis. For this specific program the PI would find 6 students by talking with students he already knows well from courses and prior research experience, putting posters around the university, and ask for recommendations from students he knows and other faculty for students who would be interested in this project.

8 Project Management

The PI is a tenured associate professor at the host institution. He directs the Sage project and organized 14 workshops and conferences during 2006–2007, so the PI has a demonstrated management record. He will be responsible for fulfilling the technical requirements of the project, including submission of annual reports. The PI will also organize the seminar and give weekly talks. He will choose students in consultation with the co-PI and postdoc.

9 Project Evaluation and Reporting

9.1 Documentation and Dissemination

Slides from talks, student proposals, and research papers the students write, will be made available online (with student permission). Quality computer code that becomes part of Sage will be distributed online in the way that Sage is currently distributed (from `http://sagemath.org`).

9.2 Evaluation

The quarterly evaluation will involve forms filled out by the student participants. These will be both the standard university course evaluation forms, and custom forms designed by the PI, in consultation with the advisory board, which specifically address the project.

The annual evaluation will summarize the quarterly evaluations. Near the end of the academic year all students involved in the project will give final presentations on their work. Each student will give a 1-hour presentation about their work that includes a general overview of the project and survey of relevant mathematics, and research results, including conjectures, theorems, hard-to-compute data, and algorithms. The PI will then synthesize feedback on the student projects. The measure of success for a student project will be the extent to which the project produces well-documented useful high-quality maintainable research, data, and code.

The final evaluation will summarize the previous annual evaluations. It will also assess the long-term impact of this project on education and research: research papers resulting from student work, impact of software, and placement of students in jobs and graduate schools.

9.3 Tracking Beyond Project

Alumni will be asked, when possible, to speak to the current group of students, and be encouraged to participate in certain workshops that the PI is involved with. These activities provide many opportunities for feedback about how involvement with this project has affected student career paths. The PI will also contact all students who were involved in the program once per year for an update on what they are currently doing, and will record the results.