William A. Stein ***Project Description***

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

The Gross-Zagier Formula and Kolyvagin's Conjecture for Elliptic Curves of Higher Rank

1 Introduction

An *elliptic curve* E is a nonsingular projective genus one curve over $\mathbf{Q}$ with a distinguished rational point. Every such curve is the closure of a curve given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The Hasse-Weil L-series $L(E, s)$ of E is holomorphic on all of $\mathbf{C}$ (see [BCDT01]), so we may define the integer $r_{\mathrm{an}}(E/\mathbf{Q}) = \mathrm{ord}_{s=1} L(E, s)$.

Conjecture 1.1 (Birch, Swinnerton-Dyer)**.**

$$\mathrm{rank}\, E(\mathbf{Q}) = r_{\mathrm{an}}(E/\mathbf{Q}) \tag{1}$$

Conjecture 1.1 is a known when $\mathrm{ord}_{s=1} L(E, s) \leq 1$, due to the combined efforts of [GZ86], [Kol88], the nonvanishing theorem of [Wal85] or [MM91] or [BFH90], and the modularity theorem [Wil95, BCDT01]. There is recent progress [DD09] toward congruence modulo 2 of both sides of (1), which is conditional on finiteness of (a certain part of) the Shafarevich-Tate group of E. In addition, there are p-adic analogs of Conjecture 1.1; see [SW10a] for an overview of the constellation of theorems about these analogs, along with techniques developed by the PI and many others for making them explicit.

The PI intends to investigate Conjecture 1.1 via a research program that involves the interplay of three lines of investigation:

- **Kolyvagin's Conjecture:** Verify the conjecture in specific cases for elliptic curves of rank ≥ 2 by explicitly computing cohomology classes, and prove results about how the cohomology classes are distributed (see Section 2).
- **The Gross-Zagier Formula:** Create new conjectural generalizations of the formula to higher analytic rank, motivated by results and conjectures of Kolyvagin and others (see Section 3).
- **Totally Real Fields:** Compute tables of data, especially about elliptic curves of rank ≥ 2 and bounded conductor over totally real fields, generalize the above two steps to totally real fields (see Section 4), and scrutinize cases in which the parameterizing Shimura curve has small genus.

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

1.1 Intellectual Merit and Broader Impact

Intellectual Merit: The proposed research could shed light on the Birch and Swinnerton-Dyer conjecture for elliptic curves over $\mathbf{Q}$, which is one of the central problems in number theory, e.g., it was chosen by the Clay Mathematics Institute as the Millennium Prize Problem in algebraic number theory [Wil00]. Explicit work in the 1960s and 1970s by Birch, Swinnerton-Dyer, Buhler, Stephens, Atkin, and others provided critical insight on which some of the great triumphs of Gross-Zagier, Kolyvagin, Wiles, and others in the 1980s and 1990s were based. This proposed research may provide tomorrow's researchers with similar clues.

> "The joy of this subject is, of course, that you can *do examples* in it."
>
> – Benedict Gross [Gro01]

Broader Impact: The PI is co-authoring a popular expository book with Barry Mazur on the Riemann Hypothesis, co-authoring an advanced graduate level book with Kenneth Ribet on modular forms and Hecke operators (see Section 5.1), and intends to prepare a new edition of his AMS book on computing with modular forms. He has many tables of data that are freely available online, and whose creation has been supported by NSF FRG grant DMS-0757627, and the proposed research would expand these tables further. He will also continue to organize the development of the NSF-funded open source Sage mathematical software project that he started (see [S$^+$10]). The PI blogs about his research at [Stec]. He also organizes dozens of workshops that involve many graduate students; [Steb] lists over 20 recent Sage-related workshops co-organized by the PI, which involve algebraic topology, combinatorics, special functions, numerical computation, etc., and hence have a potentially broad impact on the mathematics community. The PI is also a co-PI on the new UTMOST NSF grant (DUE-1020378), which seeks to make Sage much more accessible to undergraduate teachers and students.

1.2 Results from Prior NSF Support

The PI was partly supported by an NSF postdoctoral fellowship during 2000–2004 (DMS-0071576) in the amount of $90,000. The PI was also awarded NSF grant DMS-0555776 (and DMS-0400386) from the ANTC program for the period 2004–2007. The PI has received a SCREMS grant that supported purchasing computer hardware, an FRG, and a COMPMATH grant.

The PI was mainly supported by ANTC (DMS-0653968) for the period 2007–2010, and this is the award most closely related to this proposal, so we report in more detail about this award. It resulted in numerous published papers on the arithmetic of elliptic curves, modular forms and abelian varieties, including [JS07, BMSW07, KSW08, JLS07, SP10, Ste10b], and one published undergraduate number theory book [Ste09]. It resulted in the not-yet-published papers [SW10b,

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

Ste10a, SW10a], which are foundational to the current proposal, and the book [Ste07a], which is helpful for graduate students who want to learn about the BSD conjecture. In addition, in joint work with Kamienny and Stoll, the PI determined all possible prime orders of torsion points on elliptic curves over quartic fields, which will appear in a forthcoming paper. This award also supported work on the popular book [MS10] with Mazur.

2 Kolyvagin's Conjecture

In the early 1990s, Victor Kolyvagin made a conjecture in [Kol91] about nontriviality of a certain collection of Galois cohomology classes that he constructed using Heegner points. This conjecture is remarkable in that it is a conjecture about elliptic curves with $r_{\mathrm{an}}(E/\mathbf{Q}) > 1$, which is the case in which Conjecture 1.1 is still wide open. Section 3.2 below discusses how if Kolyvagin's conjecture is true, then it can be combined with an unproved higher rank analog of the Gross-Zagier formula to obtain Conjecture 1.1 as a consequence.

Assuming his conjecture, Kolyvagin describes the Selmer groups of E in terms of cohomology classes obtained from Heegner points. A more refined result can be proved independently using results of Howard, Mazur, and Rubin [How04, MR04]. This description is critical in motivating the conjectures and ideas of Section 3 about a higher rank generalization of the Gross-Zagier formula.

The PI proposes to verify Kolyvagin's conjecture about nontriviality of his Heegner point Euler system for specific curves of rank 2 and 3, possibly one of rank 4, for some modular abelian varieties of higher rank, and possibly for motives attached to modular forms. The PI also intends to prove results about the density of Kolyvagin's classes, and further extend techniques developed with Jared Weinstein for explicitly computing Kolyvagin's classes system, once nontriviality of one class is known.

> "Heegner points came along, specifically on modular curves. Suddenly, $E(\mathbf{C})$ was a highly structured object, studded all over with points defined over number fields. Instead of searching for structure, one had to analyse a situation with almost too much structure."
>
> – Bryan Birch [Bir01]

2.1 Kolyvagin's Conjecture

In this section, we describe the simplest of Kolyvagin's conjectures from [Kol91]. Let E be an elliptic curve over $\mathbf{Q}$ of conductor N and let K be a quadratic imaginary field of discriminant D_K such that each prime dividing N splits in K.

If you get bogged down reading the rest of this section, skip to Section 2.2. The executive summary is: *there is a natural way to use points on modular curves*

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

to define Galois cohomology classes τ_{m,ℓ^n} in $\mathrm{H}^1(K, E[\ell^n])$, for prime powers ℓ^n, and Kolyvagin conjectures that at least one of these classes is nonzero.

For every positive integer m coprime to ND_K, there is a Heegner point $x_m \in X_0(N)(K_m)$, where K_m is the ring class field associated to m, so K_m is a certain abelian extension of K unramified outside of m. Taking the image of x_m via a fixed choice of modular parameterization $\pi_E : X_0(N) \to E$, we obtain a point $y_m = \pi_E(x_m) \in E(K_m)$.

Suppose ℓ^n is an odd prime power and consider only m that are a squarefree product of primes p that are inert in K and satisfy $\ell^n \mid \gcd(a_p, p+1)$, where $a_p = p + 1 - \#E(\mathbf{F}_p)$. We have $\mathrm{Gal}(K_m/K_1) \cong \prod_{p|m} G_p$, where $G_p = \langle \sigma_p \rangle$ is cyclic of order $p+1$. Let

$$P_m = \mathrm{Tr}_{K_1/K}\left(\prod_{p|m} \sum_{i=1}^{p} i\sigma_p^i(y_m)\right).$$

Kolyvagin observed that

$$[P_m] \in (E(K_m)/\ell^n E(K_m))^{\mathrm{Gal}(K_m/K)}.$$

Let $\delta : E(K_m) \to \mathrm{H}^1(K_m, E[\ell^n])$ be the connecting homomorphism, and assume that $\rho_{E,\ell}$ is surjective. A diagram chase (best explained in [Gro91]) shows that $[P_m]$ defines a cohomology class $\tau_{m,\ell^n} \in \mathrm{H}^1(K, E[\ell^n])$, uniquely determined by the condition $\mathrm{res}_{K_m}(\tau_{m,\ell^n}) = \delta(P_m) \in \mathrm{H}^1(K_m, E[\ell^n])$.

Conjecture 2.1 (Kolyvagin)**.** *There exists a power ℓ^n of ℓ and a squarefree integer m such that $\tau_{m,\ell^n} \neq 0$.*

Conjecture 2.1 is a consequence of the Gross-Zagier formula (Theorem 3.1 below) with $m = 1$ when $r_{\mathrm{an}}(E/K) = 1$, but remains open when $r_{\mathrm{an}}(E/K) > 1$.

Remark 2.2. Apart from the applications of this proposal, the conjecture also provides an alternative approach to proving the main result of [ÇW08] about solvable points on locally trivial genus one curves. In fact, [ÇW08] instead works by claiming that $\tau_{m,\ell^n} \neq 0$ for some m that is *not necessarily squarefree*.

2.2 Explicit Computation of Kolyvagin's Euler System

When $r_{\mathrm{an}}(E/K) > 1$, there is nothing published that verifies Kolyvagin's Conjecture 2.1 in even a single case (for a single prime ℓ, curve E, and field K), though the PI, Jetchev, and Lauter in [JLS07] came *close* in exactly one case (of conductor 389). Nonetheless, new work of the PI, while supported by his previous ANTC grant, has provably verified the conjecture for several dozen cases.

The PI found a surprising way to use explicit computations with rational quaternion algebras to verify the conjecture algebraically in many specific cases

(see [Ste10a]). The method is inspired by theoretical work of Cornut, Gross, Jetchev, Kane, Mazur, and Vatsal (see [JK09, Cor02, Vat02]). The key idea is to use rational quaternion algebras to explicitly compute the image of Heegner points modulo an auxiliary prime ℓ that is inert in the quadratic imaginary field K.

Let N denote the conductor of E, and let H denote the Hilbert class field of K. Here is an outline of what our algorithm does:

1. Use rational quaternion algebras to explicitly compute the reduction of a choice of Heegner point $x_1 \in X_0(N)(H)$ modulo a choice of prime of H over the inert prime ℓ, thus obtaining a supersingular point $\overline{x}_1 \in X_0(N)(\mathbf{F}_{\ell^2})^{\mathrm{ss}}$.

2. Apply a mod ℓ analog of the "Kolyvagin derivative" to $\overline{x}_1$ to obtain the reduction $\overline{P}_m$ of the Kolyvagin derivative of x_m as an element of $\mathrm{Div}(X_0(N)(\mathbf{F}_{\ell^2})^{\mathrm{ss}})$.

3. Use Hecke equivariance and results of Ihara and Ribet to compute a fixed nonzero scalar multiple of the image of $\overline{P}_m$ under the Hecke module homomorphism $\mathrm{Div}(X_0(N)(\mathbf{F}_{\ell^2})^{\mathrm{ss}}) \otimes (\mathbf{Z}/p\mathbf{Z}) \to E(\mathbf{F}_\ell) \otimes (\mathbf{Z}/p\mathbf{Z})$.

We emphasize that the above steps are all done *algebraically*, without recourse to any numerical approximations. This contrasts with [JLS07], which provided numerical evidence (not proof) for Kolyvagin's conjecture in one case.

To make the above algorithm explicit, we view $\mathrm{Div}(X_0(N)(\mathbf{F}_{\ell^2})^{\mathrm{ss}})$ noncanonically as the set of right ideal classes in an Eichler order of level N in the rational quaternion algebra ramified at ℓ and ∞, which we compute as explained in [Stea]. By computing representation numbers of ternary quadratic forms associated to left orders, we find the right ideals I whose left order admits an optimal embedding of the ring of integers $\mathcal{O}_K$ of K; this allows us to compute the reduction of x_1 modulo a prime over ℓ. Then we use $\overline{x}_1$ and a parametrization of the right ideals $J \subset I$ such that $I/J \cong (\mathbf{Z}/c\mathbf{Z})^2$ to directly compute the reduction of the Kolyvagin derivative of x_m, without computing x_m itself.

There are good reasons to explicitly verify Conjecture 2.1 in specific cases:

1. The conjecture "feels" like the sort of statement that is either always true or never true when $r_{\mathrm{an}}(E/K) > 1$, so knowing that it is true in the first few dozen cases vastly increases our confidence that it is true in general.

2. The development of the algorithm sketched above led to an explicit description of the Kolyvagin "derivative operator" $y_m \mapsto P_m \bmod \ell$ directly in terms of rational quaternion algebras, which may be of independent interest.

3. Computations using this algorithm were an inspiration for and double check on the density results mentioned in Section 2.4 below.

The PI does not believe that the approach of this section has any hope of *directly* leading to a proof of Conjecture 2.1. Even in the simplest case when

$r_{\text{an}}(E/K) = 1$, the only way to prove Conjecture 2.1 is as an application of the Gross-Zagier formula, so even in that case the conjecture seems very deep. Perhaps the right way to prove Conjecture 2.1 is to prove a higher rank analog of the Gross-Zagier formula (see Section 3).

Goal 2.3. Finish writing up the details of how the PI verified Conjecture 2.1 for specific elliptic curves and publish the resulting paper [Ste10a]. This involves writing down precisely how to express the Kolyvagin derivative operator directly in terms of ideals in a rational quaternion algebra, and generalize the exposition and results of [Ste10a] to treat the case of fields K with nontrivial class group.

Goal 2.4. Write a paper explaining the verification of Conjecture 2.1 for $\ell = 3$ for the curve 5077a of rank 3, for $\ell = 7$ and the curve 11197a of rank 3, and for some modular abelian varieties of dimension > 1. Here we must use fields K of class number bigger than 1 in order to make the computation feasible. (The PI and Jennifer Balakrishnan did the 5077a computation.)

Goal 2.5. Verify Conjecture 2.1 for one curve of rank 4, e.g., maybe the one of conductor 234446. This computation will involve massive linear algebra in a space of enormous dimension, along with extensive computations in rational quaternion algebras, which would push the limits of what is computationally possible.

2.3 Motivic Analog of Kolyvagin's Conjecture

We also note that formally our algorithm may be extendable to motives attached to modular forms [Sch90]. The PI found 16 examples of weight 4 and 6 rational newforms f, with $\text{ord}_{s=1} L(f, s) = 2$, and studied their arithmetic in a joint paper [DWS03] with Dummigan and Watkins. Also, Kimberly Hopkins has just written a Ph.D. thesis [Hop10] (under Fernando Rodriguez-Villegas) in which she defines and studies higher weight Heegner points associated to such motives.

Goal 2.6. Extend Conjecture 2.1 to motives attached to modular forms.

Goal 2.7. Find, implement, and run an algorithm to verify the conjecture in some case for the motives attached to some of the 16 rational newforms f with $\text{ord}_{s=1} L(f, s) = 2$ of weight 4 and 6 in Table 1 of [DWS03]. This will start with the description of higher weight modular forms in terms of rational quaternion algebras, and proceed formally.

2.4 Density of Kolyvagin Classes

As an application of the PI's implementation of the algorithm of Section 2.2, the PI explicitly computed—up to a nonzero scalar—the cohomology classes $\tau_{m,\ell} \in \text{Sel}^{(\ell)}(E/K)$ for hundreds of pairs m, ℓ and many different rank 2 elliptic curves E and fields K, where in all cases we considered, $\text{Sel}^{(\ell)}(E/K) \cong (\mathbf{Z}/\ell\mathbf{Z})^2$. (The

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

smallest known conductor of a rank 2 curve over $\mathbf{Q}$ with $\mathrm{rank}(\mathrm{Sel}^{(\ell)}(E/K)) > 2$ for some odd prime ℓ is the daunting $N = 53295337$ for the curve $y^2 + xy = x^3 - x^2 + 94x + 9$ and $\ell = 3$.)

The resulting tables suggested (incorrect!) conjectures about how these classes are distributed as elements of $(\mathbf{Z}/\ell\mathbf{Z})^2$. At the Sage Days 17 workshop ([sd109]), which the PI co-organized, Jared Weinstein and the PI followed up on a remark of Rubin and used the Chebotarev density theorem along with [How04, MR04] to deduce a surprising theoretical density result for the distribution of these classes.

In further joint work with Weinstein, the PI intends to finish writing up the density result mentioned above. He also would like to generalize and understand it better in the case of elliptic curves with nontrivial Shafarevich-Tate group, Tamagawa numbers, higher rank, etc., and generalize it to (some) curves over totally real fields (see Section 4). Some work in this direction was done by Weinstein and many of the students at a 2-week Graduate Student Workshop that the PI organized at MSRI in Summer 2010 (see [sd210]).

3 The Gross-Zagier Formula

Let E be an elliptic curve over $\mathbf{Q}$ of conductor N and let K be a quadratic imaginary field of discriminant $D_K \leq -5$ such that each prime dividing N splits in K. *We assume for simplicity of notation in the rest of this proposal that the Manin constant $c = 1$ for E, which is a reasonable assumption (see [ARS06]).*

Let $y_K = \mathrm{Tr}_{K_1/K}(y_1) \in E(K)$ be the Heegner point, where y_1 is as in Section 2.1. Let

$$\Omega_{E/K} = \frac{\Omega_{E/\mathbf{Q}} \cdot \Omega_{E^D/\mathbf{Q}}}{\#(E(\mathbf{R})/E(\mathbf{R})^0)}.$$

In the 1980s, Gross and Zagier computed the height of y_K:

Theorem 3.1 (Gross-Zagier, Zhang)**.**

$$L'(E/K, 1) = \Omega_{E/K} \cdot h(y_K). \tag{2}$$

(In fact, Gross and Zagier proved the above formula in [GZ86] under the hypothesis that D is odd; for the general assertion see [Zha04, Thm. 6.1].)

About the proof, Gross says (see [Gro01]):

> "This conjecture of Birch seemed like a much more *provable statement* than his conjectures with Swinnerton-Dyer because at least everything in the conjecture was *defined*. ... it didn't involve the Tate-Shafarevich group which at the time we didn't know (in some cases) was finite."

Here, the conjecture with Swinnerton-Dyer that Gross refers to is:

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

Conjecture 3.2 (BSD Formula)**.** *Let E be an elliptic curve over a number field F and let $r = \mathrm{rank}(E(F))$. Then*

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\#Ш(E) \cdot \Omega_E \cdot \mathrm{Reg}_E \cdot \prod_p c_p}{\#E(F)^2_{\mathrm{tor}} \cdot \sqrt{|D_F|}},$$

where $Ш(E)$ is the Shafarevich-Tate group, Ω_E is the product of archimedean periods, Reg_E is the regulator, and c_p are the Tamagawa numbers.

3.1 Generalizations of Gross-Zagier to Higher Rank

In the paper [Ste10b], the PI gives one possible *conjectural* generalization of Theorem 3.1 to curves E with $r_{\mathrm{an}}(E/K) > 1$. This generalization is implied by "standard conjectures" and is motivated by the *structure theorem* of Kolyvagin that expresses Selmer groups in terms of the Euler system of Heegner points (see Section 2). In [Ste10b], the PI defines a *Gross-Zagier* subgroup of $E(K)$ to be any $W \subset E(K)$ such that[1]

$$[E(K)_{/\mathrm{tor}} : W_{/\mathrm{tor}}] = \prod c_p \cdot \sqrt{Ш(E/K)_{\mathrm{an}}}, \tag{3}$$

where $Ш(E/K)_{\mathrm{an}}$ is the order of the Shafarevich-Tate group predicted by the BSD formula. Easy algebra (see [Ste10b, Prop. 2.4]) shows that the BSD formula implies that for such W,

$$\frac{L^{(r)}(E/K,1)}{r!} = \Omega_{E/K} \cdot \mathrm{Reg}(W), \tag{4}$$

where $\mathrm{Reg}(W)$ is the absolute value of the determinant of the height pairing matrix on any basis for W.

Let ℓ be any good prime that is inert in K. Using Heegner points, the PI defines in [Ste10b] a finite index subgroup $W_\ell \subset E(K)$. The basic idea is to take the Kolyvagin derivative points P_m of Section 2.1 above, reduce them modulo certain primes, obtain subgroups of quotients of $E(K)$, then take the inverse image of these subgroups and obtain a group W_ℓ. If a natural refinement of Kolyvagin's conjectures are true and the BSD formula holds, then a somewhat complicated argument using the Chebotarev density theorem shows that the groups W_ℓ with $[E(K) : W_\ell]$ maximal are Gross-Zagier subgroups (up to a factor of 2 and primes where $\rho_{E,p}$ is not surjective), so we expect them to satisfy Equation (4) above. It is striking that subgroups obtained via a construction involving Heegner points conjecturally satisfies a higher rank analog of Gross-Zagier.

Goal 3.3. Investigate the case when $\ell = 2$ or $\overline{\rho}_{E,\ell}$ is reducible.

[1] In [Ste10b] there are other constraints on W that are not needed for the exposition here.

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

Like Theorem 3.1, Equation (4) is a formula directly involving E. Another goal is to state a formula more in the spirit of what Gross-Zagier really proved, i.e., something involving $J_0(N)$ and the Hilbert class field H of K. Let $\sigma \in \mathrm{Gal}(H/K)$, with corresponding ideal class $\mathcal{A}$, and let $\langle\ ,\ \rangle$ denote the height pairing on $J_0(N)(H) \otimes \mathbf{C}$ and $(\ ,\ )$ the Petersson inner product. Let

$$g_{\mathcal{A}} = \sum_{n \geq 1} \langle x_1, T_n(x_1^{\sigma}) \rangle q^n \in S_2(\Gamma_0(N)).$$

Theorem 3.4 (Gross-Zagier)**.** *We have* $(f, g_{\mathcal{A}}) = \frac{\sqrt{|D|}}{8\pi^2} L'_{\mathcal{A}}(f, 1)$ *for all* f *in the space of newforms in* $S_2(\Gamma_0(N))$.

Goal 3.5. Find a reformulation of Equation (4) directly in $J_0(N)$ over H. See the next section for a more canonical approach to this problem.

3.2 A Canonical Higher Rank Generalization of Gross-Zagier

Let E be an optimal elliptic curve over $\mathbf{Q}$ of analytic rank $r_{\mathrm{an}}(E/\mathbf{Q}) \geq 1$, let $K = \mathbf{Q}(\sqrt{D})$ be a quadratic imaginary field with discriminant $D \leq -5$ that satisfies the Heegner hypothesis for E, and assume that $r_{\mathrm{an}}(E^D) \leq 1$. This section describes a more canonical approach to generalizing Gross-Zagier to higher rank, which the PI intends to vigorously pursue. Unlike the previous section, there are unresolved, but likely surmountable, theoretical difficulties with proving that our conjecture below follows from standard conjectures. However, the connection between this conjecture and the BSD Conjecture 1.1 is clear, as we will see.

For each prime number ℓ that is inert in K, we define a finite index subgroup $U_\ell \subset E(K)$ as follows. Let $A = \gcd(a_\ell, \ell + 1)$, and let m be a squarefree product of either $r_{\mathrm{an}}(E/\mathbf{Q}) - 1$ or $r_{\mathrm{an}}(E/\mathbf{Q})$ inert primes p_i such that $A \mid \gcd(a_{p_i}, p_i + 1)$ for each i. Then reducing the Kolyvagin point $P_m \in E(K_m)$ modulo any choice of prime of K_m over ℓ yields a well-defined (independent of choice) element $\overline{P}_m \in E(\mathbf{F}_{\ell^2}) \otimes (\mathbf{Z}/A\mathbf{Z})$. This is because altering the choice of prime is the same as applying an automorphism in $G = \mathrm{Gal}(K_m/K)$, and our hypothesis on m implies that $[P_m] \in (E(K_m) \otimes (\mathbf{Z}/A\mathbf{Z}))^G$. Finally, there is a natural reduction map $E(K) \to E(\mathbf{F}_{\ell^2}) \otimes (\mathbf{Z}/A\mathbf{Z})$, and we let U_ℓ be the inverse image in $E(K)$ of the subgroup of $E(\mathbf{F}_{\ell^2}) \otimes (\mathbf{Z}/A\mathbf{Z})$ generated by all $\overline{P}_m$.

The definition of U_ℓ of course depends on our choice of prime ℓ. The subgroup

$$U = \bigcap_{\text{inert } \ell} U_\ell \subset E(K)$$

is canonical, but standard conjectures imply that U is not in general a Gross-Zagier subgroup, i.e., it *does not* satisfy Equation (4).

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

Let $t = r_{\mathrm{an}}(E/K)$, and consider the following canonical subgroup of the t-th exterior power of the Mordell-Weil group:

$$V = \bigcap_{\text{inert } \ell} \left(\bigwedge^t U_\ell \right) \subset \bigwedge^t E(K).$$

The following proposition is an application of Kolyvagin's structure theorem and Chebotarev density:

Theorem 3.6. *If V has positive rank, then the abelian group $\bigwedge^t E(K)$ has rank 1 and Kolyvagin's Conjecture 2.1 is true.*

Define a height function on $\bigwedge^t E(K)$ as follows. If V has rank 0, we define the height function to be 0. If V has positive rank, the height of $x = x_1 \wedge \cdots \wedge x_t \in E(K)$ is the regulator of the subgroup of $E(K)$ generated by $x_1, \ldots, x_t$. Let v_K be one of the (at most) two choices of generators for the group $V_{/\mathrm{tor}}$. Then $h(v_K) = n^2 \operatorname{Reg}(E(K))$, where

$$n = \left[\left(\bigwedge^t E(K) \right)_{/\mathrm{tor}} : V_{/\mathrm{tor}} \right].$$

Conjecture 3.7 (Stein)**.** $\dfrac{L^{(t)}(E/K, 1)}{t!} = \Omega_{E/K} \cdot h(v_K)$

The above conjecture when $t = 1$ follows from the Gross-Zagier theorem. Moreover, in light of Proposition 3.6, we have

Theorem 3.8. *Conjecture 3.7 $\Longrightarrow$ Conjecture 1.1.*

Goal 3.9. The PI hopes to prove the following statement (at least in some cases) using the refined structural results that go into his work with Weinstein on computing the density of Kolyvagin classes (see Section 2.4): *Conjecture 3.7 follows from the Manin constant conjecture, the BSD conjecture, and a refinement of Kolyvagin's conjecture, at least up to 2 and primes ℓ where the ℓ-adic representation attached to E is not surjective.*

Part of the subtlety in Goal 3.9 is that unlike in Kolyvagin's work, in the definition of V we consider subgroups U_ℓ that are defined using m where the condition on each prime divisor of m is divisibility by the integer A. In the PI's previous conjecture and in Kolyvagin's work, A is replaced by a fixed prime power divisor of A, which makes the condition on m vastly less restrictive.

It will also be interesting to see if Conjecture 3.7 is true at 2 or primes p where the mod p representation is reducible.

The PI also intends to compare the above conjecture with Rubin's [Rub96], which also involves wedge powers. Indeed, Rubin suggested to the PI to consider this idea in the first place, and Rubin has sketched out a general plan to the PI to attack the conjecture.

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

Goal 3.10. Assuming a favorable outcome to Goal 3.9, find a more general formulation similar to Theorem 3.4. This will be much more technically interesting, because the wedge product will be over the Hecke algebra instead of $\mathbf{Z}$.

3.3 Gross-Zagier and Kolyvagin over Ring Class Fields

The Gross-Zagier formula of Equation (2) above is only a formula for the height of y_K, hence it neglects the other Heegner points $y_m \in E(K_m)$ defined over ring class fields. Zhang [Zha01a] generalized the Gross-Zagier formula, and it is claimed in [JLS07] that Zhang's formula specializes to give

$$L'(f,\chi,1) = \frac{4}{\sqrt{|D_K|}}(f,f)h(e_\chi y_m)$$

for any nontrivial character $\chi : \mathrm{Gal}(K_m/K) \to \mathbf{C}^*$, where e_χ is the corresponding idempotent. The earlier paper [Hay95] conjectures that the formula should be

$$L'(f,\chi,1) = \frac{[K_m:K]}{\sqrt{|D_K|}}\|\omega_f\|^2 h(e_\chi y_m).$$

The PI's 2010 Ph.D. student Robert Bradshaw computed numerically in several cases, and found that neither of the above are correct! Instead, he conjectures the following based on numerical data and consistency checks with the BSD formula:

Conjecture 3.11 (Bradshaw)**.** $L'(f,\chi,1) = \dfrac{[K_m:K]}{\mathrm{cond}(\chi)\sqrt{|D_K|}}\|\omega_f\|^2 h(e_\chi y_m)$.

Goal 3.12. Prove this conjecture. This *should* follow formally from the results of Zhang, suitably understood.

Bradshaw then goes on to formally deduce (via a rather involved computation) the following formula, valid *only for curves with* $r_{\mathrm{an}}(E/\mathbf{Q}) \geq 2$:

Conjecture 3.13 (Bradshaw)**.** *Let $E/\mathbf{Q}$ be an elliptic curve with rank $r = r_{\mathrm{an}}(E/\mathbf{Q}) \geq 2$, let K be a quadratic imaginary field so that all primes dividing the conductor of N split in K, and let m be a squarefree integer divisible only by primes that are inert in K. Let $W = \mathbf{Z}[\mathrm{Gal}(K_m/K)]y_m$ be the group generated by the Galois conjugates of y_m. Then*

$$[K_m:K]^{r-1} \cdot \frac{\prod c_{v,K_m}}{\prod c_{v,K}} \cdot \frac{\#Ш(E/K_m)}{\#Ш(E/K)} = [E(K_m) : E(K) + W],$$

where $c_{v,F}$ denotes the Tamagawa number of E at v over the field F.

Goal 3.14. Prove that Kolyvagin's conjecture implies that in the formula in Conjecture 3.13, the left-hand side divides the right-hand side. This would build on Bertolini-Darmon [BD90, BD98] and Howard-Mazur-Rubin [How04, MR04].

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

4 Totally Real Fields

This third part of the proposal is about generalizing ideas from Sections 2 and 3 to elliptic curves over totally real fields that are parametrized by Shimura curves. Much work by Zhang, Darmon, Fujiwara, Shimura, Deligne, Drinfeld, Carayol, and many others has gone into generalizing to totally real fields the theorems and constructions that play an important role in the work of Gross-Zagier and Kolyvagin, so fortunately a substantial amount of important foundational work is already done in this context.

One motivation for generalizing our results to totally real fields is that the first (when ordered by conductor) elliptic curve over $\mathbf{Q}$ of rank ≥ 2 is the curve of conductor 389. This curve is furnished with a modular parametrization by the modular curve $X_0(389)$, which has genus 32. Unfortunately, from the point of view of some explicit computations, 32 is huge, and this derails some investigations into ideas related to generalizing Theorem 3.1 to higher rank. This has not stopped people from trying: in [Del02], Delaunay explicitly numerically computes the fibers in $X_0(389)$ over some rational points in $E(\mathbf{Q})$, but this appears to have led nowhere.

Thus the PI's naive hope is that there are several elliptic curves of rank ≥ 2 over totally real fields parameterized by Shimura curves of genus much smaller than 32. The goal of this part of the proposal is to find some of them by any method, and generalize whatever we can from Sections 2 and 3 to them. The PI would then attempt to make the constructions even more explicit in these small cases, perhaps motivated by Mazur's focus on $X_0(11)$ in his 1979 paper [Maz79], which treated an early variant of the Gross-Zagier formula in the case of a curve of conductor 11. To quote Gross (see [Gro01]): "I was introduced to Birch's work through a paper of Barry Mazur in 1979 in Inventiones on Heegner points, [...] and Mazur had a decisive influence on all of us at the time." On the other hand, Mark Watkins points out (personal communication) that [Mes86] studies how small the conductor can be given the rank in general, and the results suggests perhaps one cannot "beat the system."

A secondary motivation for this generalization is that many elliptic curves over $\mathbf{Q}$ are parameterized by Shimura curves, and there may be some unknown advantage in trying to generalize the Gross-Zagier formula to higher rank using such parameterizations instead of using the classical modular curves.

Let E be an elliptic curve over a totally real field F, and let $\mathcal{N}$ be the conductor of E, which is an ideal in the ring $\mathcal{O}_F$ of integers of F. Assume that either $[F : \mathbf{Q}]$ is odd or $\mathrm{ord}_{\mathfrak{p}}(\mathcal{N})$ is odd for at least one prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$. In [Zha01b], Zhang explains how to generalize the "Gross-Zagier–Kolyvagin machine" to this context. Assume, in addition, that E is attached to a (Hilbert) modular form of parallel weight 2 (for technical reasons, Zhang also assumes that $\mathrm{ord}_{\mathfrak{p}}(\mathcal{N}) = 1$ for some $\mathfrak{p}$ when $[F : \mathbf{Q}]$ is even).

Theorem 4.1 (Zhang)**.** *Let E be a modular elliptic curve over a totally real field F, as above. If $r_{\mathrm{an}}(E/F) \leq 1$, then $r_{\mathrm{an}}(E/F) = \mathrm{rank}(E(F))$.*

In order to prove Theorem 4.1, Zhang explicitly describes certain integral models of Shimura curves, defines CM and Heegner points on them (building on work of Shimura [Shi67] and others), proves an analog of the Gross-Zagier formula for them, and constructs over F an analog of Kolyvagin's Euler system of Heegner points.

Goal 4.2. Extend Kolyvagin's structure theorem for Selmer groups to (some) elliptic curves over totally real fields, by generalizing the work of [How04, MR04].

Goal 4.3. State a generalization to totally real fields of Kolyvagin's conjecture about nontriviality of the Euler system of Heegner points. Also, formulate analogs of Kolyvagin's other more precise conjectures from [Kol91], inspired by the results of Goal 4.2. It might also be straightforward to generalize the density results mentioned in Section 2.4.

Goal 4.4. *Computation:* Find all examples of elliptic curves E/F parametrized by Shimura curves of genus ≤ 2 for which $r_{\mathrm{an}}(E/F) \geq 2$. The PI recently asked several experts (Elkies, Dembélé, Voight) if they knew of *any* such examples, and it seems nobody does. However, Voight classified all Shimura curves of genus ≤ 2 in [Voi09], which is an important first step. If necessary, we will relax the condition that the genus be ≤ 2 and that the enumeration be exhaustive. The PI might also be happy with an Atkin-Lehner quotient of a Shimura curve mapping to an elliptic curve of rank 2, which would massively expand the list of possibilities.

Goal 4.5. Generalize the main result of the PI's paper [Ste10a] to find an explicit expression for reduction of Heegner points on Shimura curves modulo certain primes, make this algorithmic and computable, and implement the resulting algorithm. Use this algorithm to determine whether or not the conjecture from Goal 4.3 holds in some cases (especially those of Goal 4.4) in which $r_{\mathrm{an}}(E/F) \geq 2$.

To complete the above goals, it might not be *necessary* to explicitly compute Heegner points themselves as explicit points on elliptic curves over totally real fields. Instead, we only compute their homomorphic image in some finite group, and deduce information from that. Nonetheless, there is work on explicit computation of Heegner points themselves (see [Voi06]), which may prove useful.

4.1 Tables of Elliptic Curves over Totally Real Fields

To help with Goal 4.4, it would likely be helpful to have a huge table of data about elliptic curves of bounded conductor and discriminant over various totally real fields, similar to the massive table of elliptic curves over $\mathbf{Q}$ that the PI created in collaboration with Mark Watkins (see [SW02] and [BMSW07]). Donnelly and

Voight are also currently computing huge tables of Hilbert modular forms, and it would be of great interest to match up these forms with the above curves.

Voight reports (personal communication) that in his naive approaches to enumerating curves, the sizes of fundamental units makes the creation of useful tables difficult (see, e.g., [GV10, pg. 17]). On the other hand Elkies (also personal communication) has sketched out to the PI a plan for making tables that gets around by clever applications of lattice reduction.

The paper [GV10] outlines approaches to finding explicit equations for elliptic curves attached to Hilbert modular forms, but challenges have been encountered by Dembélé, Donnelly, Greenberg, Voight, and others when putting these strategies into play.

5 Other Projects

In this section we describe a few other projects that the PI is involved with that have little to do with the main theme of this proposal.

5.1 Books

The PI has published an undergraduate text on number theory [Ste09] with Springer-Verlag and a graduate book on computing with modular forms [Ste07b] that was published by the AMS. He is currently working on an advanced graduate-level textbook with Kenneth Ribet on modular forms, Hecke operators, Galois representations, and modular abelian varieties that will be published with Springer-Verlag. He is also writing an expository book coauthored with Barry Mazur on the Riemann Hypothesis (draft at [MS10]), which presents a novel approach to understanding the statement of RH using Fourier transform.

Jointly with Paul Gunnells, the PI also intends to create a new edition of his AMS book [Ste07b]. In addition to the improvements Paul Gunnells would make to the appendix on higher degree groups, the PI would update the book to include a new chapter on how to use rational quaternion algebras to efficiently compute certain spaces of modular forms. He would also update the linear algebra chapter to reflect recent progress in fast linear algebra over cyclotomic fields, which is relevant to many modular forms algorithms.

5.2 Sage: open source mathematical software

The PI is the author of the modular forms and modular abelian varieties components of Magma [BCP97]. He is the principal author of Sage (see [S$^+$10]). The PI has also started a project "Purple Sage" (PSAGE): `http://purple.sagemath.org`, which is a spinoff from Sage. The Sage project has become large and relatively stable, and PSAGE provides a much *less* stable environment in which to

distribute cutting edge research-level number theory code, whose interface may not yet be stable. The PI hopes to include all code coming out of the research described in this proposal in PSAGE, along with new code from Skorrupa, Ryan, and others for computing with Siegel modular forms, code from Fredrik Strömberg for computing with Maass forms, code from Chris Hall and Sal Baig for computing with elliptic curves over function fields, and much other code. Some of the code in PSAGE that is sufficiently stable will eventually be included in Sage.

5.3 Torsion Points on Elliptic Curves over Number Fields

The PI, Sheldon Kamienny, and Michael Stoll have been collaborating on a project to explicitly determine possible torsion points on elliptic curves over number fields. In particular, we have devised, implemented, and run code to verify the following:

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

The PI intends to write this up for publication, and also make several parts of the computation more efficient. In particular, the application of [Par00] to ruling out primes with $31 < p \leq 97$ can probably be substantially sped up (it now takes about a day). Also, the application of results of [CES03] and explicit computation with models for modular curves using Riemann-Roch spaces (see [Hes02]) would be dramatically sped up by proving that $J_1(29)(\mathbf{Q})$ is cuspidal, as was conjectured in [CES03]. The PI intends to carry out this latter computation using a strategy suggested to him by Loïc Merel, which involves explicitly computing the kernel of an Eisenstein ideal on $J_1(29)$, then computing the actual of Galois on that kernel using [Ste82]. This strategy is in fact very general, and itself could lead to important new conjectures and results about modular curves, and perhaps an eventual proof of some of the conjectures left open in [CES03]. The PI also intends to finish creating a free open source implementation of computation of Riemann-Roch spaces (for Sage) of the closed implementation of Hess (see [Hes02]), since this is essential in order that Theorem 5.1 not fundamentally rely on closed source software (every other part of the computation was done in Sage).

The PI intends to attempt a similar computation, but for number fields of degree 5. The results of [Par00] also apply in this case, so this is primarily a matter of "making things much faster", which may require new algebraic or combinatorial insight into the results of [Par00].