Heegner Points and the Arithmetic of Elliptic Curves Over Ring Class Extensions[1]

Robert Bradshaw and William Stein[2a,b]

[a] *Google, Seattle*
[b] *University of Washington*

Abstract

Let E be an elliptic curve over $\mathbb{Q}$ and let K be a quadratic imaginary field that satisfies the Heegner hypothesis. We study the arithmetic of E over ring class extensions of K, with particular focus on the case when E has analytic rank at least 2 over $\mathbb{Q}$. We also point out an issue in the literature regarding generalizing the Gross-Zagier formula, and offer a conjecturally correct formula.

Keywords: elliptic curve, Gross-Zagier formula, Birch and Swinnerton-Dyer conjecture, Shafarevich-Tate groups
2000 MSC: 11G05

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$. By [Wil95, BCDT01], $L(E, s)$ extends to an entire function on $\mathbb{C}$, so $r_{\text{an}}(E/\mathbb{Q}) = \text{ord}_{s=1} L(E, s)$ is defined. Let $r_{\text{alg}}(E/\mathbb{Q}) = \text{rank}(E(\mathbb{Q}))$.

Conjecture 1 (Birch and Swinnerton-Dyer (see [Wil00]))**.** *We have*

$$r_{\text{an}}(E/\mathbb{Q}) = r_{\text{alg}}(E/\mathbb{Q}).$$

Let K be a quadratic imaginary field such that all primes dividing the conductor N of E split in K, and let $u = \#\mathcal{O}_K^\times/2$, which is 1 unless $K = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. For each squarefree product c of primes that are inert

[1] To appear in Journal of Number Theory.
[2] This work was supported by NSF grants DMS-0757627, DMS-0653968 and the Mathematical Sciences Research Institute.

in K, let K_c denote the ring class field of conductor c, which is an abelian extension of K ramified exactly at primes dividing c. Moroever, K_1 is the Hilbert class field of K, and (see [Gro91, §3])

$$\mathrm{Gal}(K_c/K_1) \cong (\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times.$$

Heegner points are certain points in $E(K_c)$ that are constructed using complex multiplication and a fixed choice of modular parametrization $\phi_E : X_0(N) \to E$ of minimal degree. In this paper, we study the subgroup of $E(K_c)$ generated by Galois conjugates of Heegner points, and relate it to $\#Ш(E/K_c)$.

Our motivation for this paper is that the subgroup W of any Mordell-Weil group generated by Heegner points typically fits into an analogue of the BSD conjecture, but with the "difficult" factors such as the Shafarevich-Tate group and Tamagawa numbers removed (see [Ste10b]). Thus according to the BSD formula (see Conjecture 12 below), we expect that the index of W in its saturation (or the closely related index of $E(K) + W$ in $E(K_c)$) in the Mordell-Weil group is related to the order of Ш and Tamagawa numbers. In Theorem 13 below, which is conditional on the BSD formula (see Conjecture 12 below), we compute this index in terms of other invariants of E. Intriguingly, in order for our result to satisfy certain consistency checks, we discover that the previously published explicit generalizations of the Gross-Zagier formula to ring class fields appear to be wrong, e.g., they do not properly take into account either the conductor of the ring class character or the degree of the ring class field.

Our hypothesis that every prime dividing N splits in K implies that there is a factorization of the ideal $N\mathcal{O}_K$ as $\mathcal{N}\bar{\mathcal{N}}$ with $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. Fix an embedding $K \hookrightarrow \mathbb{C}$ and view $\mathcal{O}_K$ as a lattice in $\mathbb{C}$, so $\mathbb{C}/\mathcal{O}_K$ is a CM elliptic curve, and $\mathcal{N}^{-1}/\mathcal{O}_K$ defines a cyclic subgroup of order N. Let $X_0(N)$ be the standard modular curve whose affine points over $\mathbb{C}$ parameterize isomorphism classes of pairs (F, C), where F is an elliptic curve over $\mathbb{C}$ and C is a cyclic subgroup of F of order N. Let x_1 be the point in $X_0(N)(K_1)$ defined by the isomorphism class of $(\mathbb{C}/\mathcal{O}_K, \mathcal{N}^{-1}/\mathcal{O}_K)$. Using the modular parameterization $\phi_E : X_0(N) \to E$, we obtain a point $y_1 = \phi_E(x_1) \in E(K_1)$. Let $y_K = \mathrm{Tr}_{K_1/K}(y_1)$ be the trace of y_1. After fixing our choice of ϕ_E, the point y_K is well defined up to sign, since making a different choice of $\mathcal{N}$ replaces y_K by its image under an Atkin-Lehner involution, as explained in [Wat06, §2] or [Coh07, Thm. 8.7.7], and Atkin-Lehner acts as ± 1 on E.

In addition to their central importance to explicit computation of rational

points on elliptic curves, Heegner points play an essential role in results toward Conjecture 1 (see, e.g., [Gro91]):

Theorem 2 (Gross-Zagier, Kolyvagin, et al.)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with $r_{\mathrm{an}}(E/\mathbb{Q}) \leq 1$. Then $r_{\mathrm{an}}(E/\mathbb{Q}) = r_{\mathrm{alg}}(E/\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ is finite.*

The proof that $Ш(E/\mathbb{Q})$ is finite also yields an explicit computable upper bound on the p-part of $\#Ш(E/\mathbb{Q})$ (see [GJP+09, Thm. 3.4]) at primes p where $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ has sufficiently large image (see [Cha05, GJP+09, Jet08, SW11]). The bound is in terms of $[E(K) : \mathbb{Z}y_K]$, for any choice of K. This bound plays an essential role in verifying the full BSD formula (Conjecture 12) for specific elliptic curves, as in [GJP+09, Mil10, MS10].

If M is any number field, let $\hat{h}_M$ denote the Néron-Tate canonical height on $E(M)$ over M. If S is an extension of M and $P \in E(M)$, then $\hat{h}_S(P) = [S : M] \cdot \hat{h}_M(P)$ (see [Sil92, Prop. VIII.5.4]). Following [GZ86, §I.6 and §V.2], we have

$$\|\omega_E\|^2 = \frac{8\pi^2 \cdot (f, f) \cdot c_E^2}{\deg(\phi_E)}, \tag{1}$$

where ω_E is a minimal differential on E, c_E is the Manin constant, $\deg(\phi_E)$ is the modular degree, f is the newform corresponding to E, and (f, f) is the Petersson inner product of f with itself (see also [GJP+09, §3]).

Remark 3. We assume that $c_E = 1$ in the rest of this paper. As explained in [ARS06] this should be a harmless assumption, and conjecturally holds when working with the optimal elliptic curve isogenous to E.

The following theorem is in [GZ86, §V.2, pg. 311]:

Theorem 4 (Gross-Zagier)**.** *We have*

$$L'(E/K, 1) = \frac{\|\omega_E\|^2}{u^2 \cdot \sqrt{|D_K|}} \cdot \hat{h}_K(y_K).$$

Let E be an elliptic curve over $\mathbb{Q}$ and assume that $r_{\mathrm{an}}(E/K) = 1$. The subgroup of $E(K)$ generated by the Heegner point plays an essential role in the proof of Theorem 2. One uses the nontorsion point $y_K = \mathrm{Tr}_{K_1/K}(y_1)$ to bound the rank of $E(K)$ from below. There are also higher Heegner points $y_c = \phi_E(x_c)$ (see Section 2) that are used to construct elements of various Selmer groups associated to E, which one then uses to bound the rank of $E(K)$ from above.

Assume $L'(E/K,1) \neq 0$. Then, as explained in [Ste10b, §2], the Gross-Zagier formula and the BSD formula for $L'(E/K,1)$ together imply that

$$[E(K) : \mathbb{Z}y_K]^2 = \#Ш(E/K) \cdot \prod c_{v,K},$$

where the $c_{v,K}$ are the Tamagawa numbers of E/K. Note that since each prime divisor $p \mid N$ splits in K, the product of the Tamagawa numbers of E/K is the square of $\prod_{p|N} c_p$, where the c_p are the Tamagawa numbers of $E/\mathbb{Q}$. See the proof of Proposition 14 for related remarks, and [Ste10b, Prop. 2.4] for a discussion of what happens when E has rank ≥ 2.

In Section 2, we recall the definition of Heegner points over ring class fields, set up some notation involving characters and corresponding idempotent projectors, and discuss generalization of the Gross-Zagier formula to higher Heegner points. In Section 3, we introduce the subgroup W of $E(K_c)$ generated by Galois conjugates of Heegner points and describe a theorem of Bertolini-Darmon that allows us to deduce conditions under which $W+E(K)$ has finite index in $E(K_c)$. In Section 4, we use a generalization of the Gross-Zagier formula to derive a formula for $\mathrm{Reg}(W)$, then use the BSD formula to compute the index of $W + E(K)$ in $E(K_c)$. We also compute the index of W in its saturation. Section 5 gives an example that illustrates the results of Section 4. Finally, Section 6 suggests some avenues for future investigation.

2. Higher Heegner Points

Fix a positive squarefree integer c whose prime divisors are inert in K and coprime to N. Let $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ and $\mathcal{N}_c = \mathcal{N} \cap \mathcal{O}_c$. Then the pair $(\mathbb{C}/\mathcal{O}_c, \mathcal{N}_c^{-1}/\mathcal{O}_c)$ defines a CM elliptic curve equipped with a cyclic subgroup of order N, and the isomorphism class of this pair defines a point $x_c \in X_0(N)(K_c)$. We use the modular parameterization ϕ_E to map x_c to a point $y_c = \phi_E(x_c) \in E(K_c)$.

Let $G = \mathrm{Gal}(K_c/K)$ and let

$$h_c = [K_c : K] = \#\,\mathrm{Cl}(\mathcal{O}_c) = \#G$$

be the class number of the order $\mathcal{O}_c$. For any character $\chi : G \to \mathbb{C}^\times$, let e_χ be the idempotent

$$e_\chi = \frac{1}{h_c} \sum_{\sigma \in G} \chi^{-1}(\sigma)\sigma \in \mathbb{C}[G],$$

which projects to the χ-isotypical component of any G-module. Note that if $\sigma \in G$, then $\sigma e_\chi = \chi(\sigma) e_\chi$; also, $1 = \sum_{\chi: G \to \mathbb{C}^\times} e_\chi$.

Following [Gro84, (10.1)], we extend the Néron-Tate height pairing $\langle\ ,\ \rangle_{K_c}$ on $E(K_c)$ defined by h_{K_c} to a Hermitian inner product on the complex vector space $V = E(K_c) \otimes_{\mathbb{Z}} \mathbb{C}$ by letting

$$\langle \alpha P,\, \beta Q \rangle = \alpha \overline{\beta} \langle P,\, Q \rangle_{K_c} \tag{2}$$

and extending linearly. We also view V as a $\mathbb{C}[G]$-module by making $\sigma \in G$ act by $\sigma(P \otimes \alpha) = \sigma(P) \otimes \alpha$. Since E is defined over $\mathbb{Q}$, the height pairing on V is $\mathrm{Gal}(K_c/\mathbb{Q})$-equivariant (see [Sil92, Lem. VIII.5.10]), in the sense that for any $\sigma \in \mathrm{Gal}(K_c/\mathbb{Q})$ and $P, Q \in E(K_c)$, we have $\langle \sigma(P), \sigma(Q) \rangle = \langle P, Q \rangle$.

Lemma 5. *The χ eigenspaces of V are orthogonal with respect to the height pairing.*

Proof. This is standard, but for the convenience of the reader we give a proof. If χ, χ' are two characters of G, then for any $P, Q \in E(K_c)$ and $\sigma \in G$, we have

$$\begin{aligned} \langle e_\chi P,\, e_{\chi'} Q \rangle &= \langle \sigma(e_\chi P),\, \sigma(e_{\chi'} Q) \rangle \\ &= \langle \chi(\sigma) e_\chi P,\, \chi'(\sigma) e_{\chi'} Q \rangle \\ &= \chi(\sigma) \chi'(\sigma)^{-1} \langle e_\chi P,\, e_{\chi'} Q \rangle. \end{aligned}$$

Thus if $\langle e_\chi P,\, e_{\chi'} Q \rangle \neq 0$ for some P, Q, then $\chi(\sigma)\chi'(\sigma)^{-1} = 1$ for all σ, hence $\chi = \chi'$. □

We next explain how the heights $\hat{h}_{K_c}(e_\chi y_c)$ are related to the special values of certain L-functions. Let $f = \sum a_n q^n \in S_2(\Gamma_0(N))$ be the newform corresponding to E, let χ be a character of G, and let $L(f, \chi, s)$ be the Rankin-Selberg L-series $L(f \otimes g_\chi, s)$, as described in [Gro84, §III]. According to [Gro84, Prop. 21.2], the sign in the functional equation for $L(f, \chi, s)$ is -1, so $L(f, \chi, s)$ vanishes to odd order at $s = 1$. In [Zha01a, Thm. 1.2.1], Zhang proves a generalization of the Gross-Zagier formula (Theorem 4 above) that relates the height of $e_\chi y_c$ to $L'(f, \chi, 1)$. Unfortunately, the literature on this formula is inconsistent. For nontrivial χ, [JLS09, §A.2] asserts that Zhang's theorem implies that

$$L'(f, \chi, 1) = \frac{4(f, f)}{u^2 \sqrt{|D_K|}} \cdot \hat{h}_{K_c}(e_\chi y_c). \tag{3}$$

The earlier paper [Hay95, Thm. 2] conjectures that the formula is

$$L'(f,\chi,1) = \frac{8\pi^2(f,f)}{u^2\sqrt{|D_K|}} \cdot \hat{h}_{K_c}(e_\chi y_c). \tag{4}$$

However, somewhat bizarrely, immediately after stating the above, [Hay95] then states that the formula is instead

$$L'(f,\chi,1) = \frac{h_c \cdot 8\pi^2(f,f)}{u^2\sqrt{|D_K|}} \cdot \hat{h}_{K_c}(e_\chi y_c). \tag{5}$$

which is closer to what we expect (see Conjecture 6).

Consistency checks with the BSD formula (see Proposition 14 and the discussion on page 15 right after the proof of Theorem 13) very strongly suggest that Equations (3), (4) and (5) are all incorrect. Zhang remarks at the end of Section 1 of [Zha04], "I would like to thank N. Vatsal and H. Xue for pointing out many inaccuracies in our previous paper [Zha01a]," and in an email to the authors: "You are right that my formula cited in your paper is not accurate. A correct version is in my paper [Zha04]."

Instead, we propose the following closely related formula, which also features the *conductor* of the character $\chi : \mathrm{Gal}(K_c/K) \to \mathbb{C}^\times$, which is the smallest integer divisor $c' \mid c$ such that χ factors through the natural quotient map $\mathrm{Gal}(K_c/K) \to \mathrm{Gal}(K_{c'}/K)$.

Conjecture 6. *If χ is a nontrivial character of G, then*

$$L'(f,\chi,1) = \frac{h_c \cdot 8\pi^2(f,f)}{\mathrm{cond}(\chi) \cdot u^2 \cdot \sqrt{|D_K|}} \cdot \hat{h}_{K_c}(e_\chi y_c).$$

Remark 7. Zhang has explained to us that one can deduce the above conjecture from his [Zha04, Thm 6.1]. Zhang and his students intend to give the details in a future paper, by using the following facts:[3]

1. Zhang's L-series is the full L-series, including Γ-functions, so some factors should be removed.
2. Zhang's D includes both the the conductor of the cyclotomic character, and the discriminant of the imaginary quadratic extension.
3. Zhang's CM point are not averaged.
4. Zhang's height pairings are averaged over the base field F.
5. Zhang does not use the factor of 2 that others use.

[3]This list was removed from the published version of this paper as demanded by the referee.

3. The Heegner Point Subgroup

In this section we state a theorem of Bertolini-Darmon, and use it to understand when $W + E(K)$ generates a finite index subgroup of $E(K_c)$. We also give equivalent conditions under which W and $E(K)$ are orthogonal.

Let E and K be as above. We continue to fix an integer c whose prime divisors are inert in K and coprime to N, and let a_c be the cth Fourier coefficient of the newform attached to the elliptic curve E. Consider the subgroup $W = \mathbb{Z}[G]y_c$ of $E(K_c)$ spanned by the G-conjugates of y_c.

Recall from Section 2 the vector space $V = E(K_c) \otimes_{\mathbb{Z}} \mathbb{C}$, which is a finite-dimensional $\mathbb{C}[G]$-module equipped with a G-invariant bilinear Hermitian height pairing (2). For any character χ of G, let $V^\chi = e_\chi V$ be the subspace of V on which G acts via χ. Because $1 = \sum_\chi e_\chi$, we have

$$V = \bigoplus_{\chi : G \to \mathbb{C}^\times} V^\chi,$$

and Lemma 5 asserts that the V^χ are mutually orthogonal. Let $y_{c,\chi} = e_\chi(y_c) \in V^\chi$.

Theorem 8 (Bertolini-Darmon [BD90])**.** *If $y_{c,\chi} \neq 0$ then $V^\chi = \mathbb{C}y_{c,\chi}$.*

Remark 9. The converse of Theorem 8 is the assertion that if $y_{c,\chi} = 0$ then $V^\chi \neq \mathbb{C}y_{c,\chi} = 0$. As explained in [BD90], this is consistent with a natural refinement of the BSD rank conjecture (Conjecture 1), which asserts that V^χ has odd rank (see also [YZZ10, Conj. 1.4.1]). It is a difficult open problem to come up with any way to construct points in V^χ when $\mathbb{C}y_{c,\chi} = 0$.

Proposition 10. *If for* all *nontrivial characters χ of G we have $L'(f, \chi, 1) \neq 0$, then the index $[E(K_c) : W + E(K)]$ is finite.*

Proof. By tensoring with $\mathbb{C}$, we see that the claim is equivalent to showing that the $\mathbb{C}$ span of $W + E(K)$ is V. Let χ_1 denote the trivial character. Then

$$V = \bigoplus_{\chi : G \to \mathbb{C}^\times} V^\chi = V^{\chi_1} \oplus \bigoplus_{\chi \neq \chi_1} V^\chi.$$

We have $V^{\chi_1} = E(K) \otimes \mathbb{C}$. Theorem 8 and our hypothesis that $L'(f, \chi, 1) \neq 0$ for all nontrivial χ imply that $W \otimes \mathbb{C} = \oplus_{\chi \neq \chi_1} V^\chi$, □

As explained in [Gro84, §6] and [Gro91, Prop. 3.7], we have $\mathrm{Tr}_{K_c/K}(y_c) = a_c y_K$, which motivates the appearance of $a_c y_K$ in the following proposition.

Proposition 11. *The following are equivalent:*

1. *The two subgroups W and $E(K)$ of $E(K_c)$ are mutually orthogonal.*
2. *The point $a_c y_K$ is torsion.*
3. *$a_c = 0$ or $r_{\mathrm{an}}(E/K) > 1$.*

Proof. To prove that 1 implies 2, suppose that W is orthogonal to $E(K)$. The height pairing on $E(K_c)$ is 0 only on torsion points, so $W \cap E(K)$ is a torsion group. But $a_c y_K = \mathrm{Tr}_{K_c/K}(y_c) \in W \cap E(K)$, so $a_c y_K$ is torsion, as claimed.

To prove that 2 implies 1, assume that $a_c y_K$ is torsion. Choose $P \in E(K)$ and $Q \in W$. For any $\sigma \in G$, we have

$$\mathrm{Tr}_{K_c/K}(\sigma(y_c)) = \sigma(\mathrm{Tr}_{K_c/K}(y_c)) = \sigma(a_c y_K) = a_c y_K \in E(K)_{\mathrm{tor}}. \tag{6}$$

Since Q is a linear combination of $\sigma(y_c)$ for various σ, Equation (6) implies that $\mathrm{Tr}_{K_c/K}(Q)$ is torsion. The height pairing is Galois equivariant, so for all $\sigma \in G$, we have $\langle P, Q\rangle = \langle \sigma P, \sigma Q\rangle = \langle P, \sigma Q\rangle$. Thus

$$\langle P, Q\rangle = \frac{1}{h_c}\sum_{\sigma\in G}\langle P, \sigma Q\rangle = \frac{1}{h_c}\langle P, \mathrm{Tr}_{K_c/K}\, Q\rangle = 0.$$

Finally we observe that 2 and 3 are equivalent. If $a_c = 0$ then $a_c y_K = 0$. If $r_{\mathrm{an}}(E/K) > 1$, then Theorem 4 implies that y_K is torsion. Conversely, suppose $a_c y_K$ is torsion. If $a_c \neq 0$, then y_K is also torsion, so Theorem 4 implies that $r_{\mathrm{an}}(E/K) > 1$. □

4. Regulators and Indexes

In this section we study the index $[E(K_c) : W + E(K)]$, and under certain hypotheses, conjecturally relate it to various arithmetic invariants of E. In particular, we prove Theorem 13, which is a conjectural formula for the index $[E(K_c)_{/\mathrm{tor}} : (E(K) + W)_{/\mathrm{tor}}]$ under any of the equivalent hypotheses of Proposition 11.

If H is any subgroup of a Mordell-Weil group $E(M)$, let $\mathrm{Reg}_M(H)$ be the absolute value of the determinant of the height pairing $\langle\ ,\ \rangle_M$ on a basis of H. We emphasize here that we use the height relative to M and not the absolute height on $E(\overline{\mathbb{Q}})$.

Theorem 13 below is conditional on the BSD formula over number fields.

Conjecture 12 (Birch and Swinnerton-Dyer Formula)**.** *If E is an elliptic curve of rank r over a number field F then*

$$\frac{L^{(r)}(E/F,1)}{r!} = \frac{\Omega_{E/F}\cdot \mathrm{Reg}_F(E(F))\cdot \#Ш(E/F)\cdot \prod_v c_{v,F}}{\sqrt{|D_F|}\cdot \#E(F)_{\mathrm{tor}}^2},$$

where $D_F \in \mathbb{Z}$ is the discriminant of F, and the other quantities are as in [Lan91, III, §5].

If E is defined over $\mathbb{Q}$ and F is totally imaginary, as it is in our application in which $F = K$ or $F = K_c$, we have $\Omega_{E/F} = \|\omega_E\|^{[F:\mathbb{Q}]}$, where $\|\omega_E\|$ is as in Equation (1) (see also [GZ86, §6]).

Much of the rest of this section is devoted to proving the following theorem.

Theorem 13. *Assume Conjectures 6 and 12 for E, that $\mathrm{ord}_{s=1} L(E/K,\chi,s) = 1$ for each nontrivial ring class character χ of conductor dividing c, and that $a_c y_K$ is torsion. Let $r = r_{\mathrm{an}}(E/K) = \mathrm{ord}_{s=1} L(E/K,s)$ and assume that $r = \mathrm{rank}(E(K))$, as predicted by Conjecture 1. Then*

$$[E(K_c)_{/\mathrm{tor}} : (E(K)+W)_{/\mathrm{tor}}]^2 = \frac{\#Ш(E/K_c)}{\#Ш(E/K)}\cdot\frac{\prod_w c_{w,K_c}}{\prod_v c_{v,K}}\cdot\frac{\#E(K)_{\mathrm{tor}}^2}{\#E(K_c)_{\mathrm{tor}}^2}\cdot h_c^{r-1}\cdot u^{2h_c}.$$

Because of the the Cassels-Tate pairing, we expect that $\#Ш(E/K_c)$ and $\#Ш(E/K)$ are both perfect squares (see, e.g., [Ste04, Thm. 1.2]). The following proposition is thus an important consistency check for Theorem 13.

Proposition 14. *Theorem 13 predicts that $\frac{\#Ш(E/K_c)}{\#Ш(E/K)}$ is a perfect square.*

Proof. We check that each factor, except the quotient of Shafarevich-Tate groups appearing in the theorem, is a perfect square, especially the Tamagawa number factors. Each prime of bad reduction for E splits in K, and for the two primes v and v' over a split prime p of $\mathbb{Q}$, we have $c_{v,K} = c_{v',K}$, so

$$\prod_v c_{v,K} = \left(\prod_{p|N} c_{p,\mathbb{Q}}\right)^2.$$

The extension K_c/K is unramified at each prime of bad reduction for E, and the formation of Néron models commutes with unramified base change (see

[BLR90, §1.2, Prop. 2]), so for each prime v of K and each prime w of K_c with $w \mid v$, we have $c_{w,K_c} = c_{v,K}$. Let g_v be the number of primes of K_c over the prime v of K. Then

$$\prod_{w \text{ of } K_c} c_{w,K_c} = \prod_{v \text{ of } K} c_{v,K}^{g_v} = \prod_{p|N} c_{p,\mathbb{Q}}^{2g_v} = \left(\prod_{p|N} c_{p,\mathbb{Q}}^{g_v} \right)^2.$$

Finally, the factor h_c^{r-1} is a perfect square since the sign of the functional equation for $L(E/K, s)$ is odd, so r is odd. □

Lemma 15. *With hypotheses as in Theorem 13, $L(E/K_c, s)$ vanishes to order exactly $r + h_c - 1$ and*

$$\frac{L^{(r+h_c-1)}(E/K_c, 1)}{(r + h_c - 1)!} = \frac{L^{(r)}(E/K, 1)}{r!} \cdot \prod_{\chi \neq \chi_1} L'(E/K, \chi, 1). \tag{7}$$

Proof. The L-function of E over K_c factors as

$$L(E/K_c, s) = \prod_{\chi} L(f, \chi, s) = L(E/K, s) \cdot \prod_{\chi \neq \chi_1} L(f, \chi, s),$$

where the first product is over characters $\chi : G \to \mathbb{C}^\times$, and χ_1 is the trivial character. This implies the order of vanishing statement. The leading coefficient of the product of power series is the product of the leading coefficients of those series, which gives the formula for the leading coefficient. □

In using Conjecture 12 to deduce Theorem 13, we will make use of an explicit formula for the discriminant D_{K_c}.

Lemma 16. *We have*

$$D_{K_c} = D_K^{h_c} \cdot \prod_{p|c} p^{\frac{2 \cdot p \cdot h_c}{p+1}}.$$

Proof. Consider a prime divisor $p \mid c$, and write $c = pc'$. The prime $p\mathcal{O}_K$ above p splits completely in $K_{c'}/K$ (as explained in [Ste10b, Lem. 5.3]). Going from $K_{c'}$ to K_c, the primes above $p\mathcal{O}_K$ are totally ramified, with ramification index $[K_c : K_{c'}] = [K_p : K_1] = p+1$. Combining this information for all $p \mid c$ and applying [FT93, Thm. 26, Ch. III], implies that the different

$\delta_{K_c/K}$ is $\prod_{p|c}\prod_{\mathfrak{p}|p}\mathfrak{p}^p$. Let $\mathfrak{p}$ be any prime of K_c over p. As explained above, since p is inert in $K/\mathbb{Q}$, the prime $p\mathcal{O}_K$ splits completely in $K_{c'}/K$, then totally and tamely ramifies in K_c/K_c', so $\mathrm{norm}_{K_c/\mathbb{Q}}(\mathfrak{p}) = p^2$, and the number of primes $\mathfrak{p}$ over a given p is $h_c/(p+1)$. The different ideal is multiplicative in towers, and the discriminant is the norm of the different, so

$$\begin{aligned} D_{K_c} &= \mathrm{norm}_{K_c/\mathbb{Q}}(\delta_{K_c/\mathbb{Q}}) \\ &= \mathrm{norm}_{K_c/\mathbb{Q}}(\delta_{K/\mathbb{Q}} \cdot \delta_{K_c/K}) \\ &= \mathrm{norm}_{K_c/\mathbb{Q}}(\delta_{K/\mathbb{Q}}) \cdot \prod_{p|c}\prod_{\mathfrak{p}|p} \mathrm{norm}_{K_c/\mathbb{Q}}(\mathfrak{p})^p \\ &= D_K^{h_c} \cdot \prod_{p|c} p^{\frac{2h_c p}{p+1}}. \end{aligned}$$

□

The product of prime divisors of c in Lemma 16 can be expressed in terms of conductors as follows:

Lemma 17. *We have*

$$D_{K_c} = D_K^{h_c} \cdot \prod_{\chi \neq \chi_1} \mathrm{cond}(\chi)^2. \tag{8}$$

Proof. Consider the set of characters $\chi : G \to \mathbb{C}^\times$. A character χ has conductor not divisible by p precisely if it factors through $\mathrm{Gal}(K_{c'}/K)$, so the number of characters χ with conductor not divisible by p is the number of characters of $\mathrm{Gal}(K_{c'}/K)$, which is $\#\,\mathrm{Gal}(K_{c'}/K) = h_c/(p+1)$. Thus the number of characters with conductor divisible by p is $h_c - h_c/(p+1)$. As $\mathrm{cond}(\chi) \mid c$ we have

$$\prod_{\chi \neq \chi_1} \mathrm{cond}(\chi) = \prod_{p|c} p^{h_c - h_c/(p+1)} = \prod_{p|c} p^{h_c p/(p+1)},$$

which, combined with Lemma 16, implies the claimed formula. □

We will use the following lemma in computing a certain regulator in the proof of Proposition 19 below.

Lemma 18. *Let $M_m(a,b)$ be the $m \times m$ matrix with $a+b$ along the diagonal and all other entries equal to b. Then* $\det M_m(a,b) = (a+mb)a^{m-1}$.

Proof. The case for $m = 1, 2$ is clear. For $m > 2$, first consider the determinant of the matrix $M'_m(a, b)$ of size $m \times m$ whose entries are all b except for the first upper off diagonal whose entries are all $a + b$ (see Equation (9) below). We claim that $\det M'_m(a, b) = (-a)^{m-1}b$. For $m = 1, 2$ this is clear. For larger m we perform a row operation (subtract row 2 from row 1) and expand by minors, as follows:

$$\det M'_m(a,b) = \begin{vmatrix} b & a+b & \cdots & b \\ b & b & \ddots & \vdots \\ \vdots & & \ddots & a+b \\ b & \cdots & b & b \end{vmatrix} = \begin{vmatrix} 0 & a & \cdots & 0 \\ b & b & \ddots & \vdots \\ \vdots & & \ddots & a+b \\ b & \cdots & b & b \end{vmatrix} \tag{9}$$

$$= -a \cdot \det M'_{m-1}(a,b) = -a(-a)^{m-2}b = (-a)^{m-1} \cdot b. \tag{10}$$

Using this formula for $\det M'_m(a, b)$ allows us to compute $\det M_m(a, b)$ as follows, where in the first step we subtract the last row from the first row:

$$\det M_m(a,b) = \begin{vmatrix} a+b & b & \cdots & b \\ b & a+b & & \vdots \\ \vdots & & \ddots & b \\ b & \cdots & b & a+b \end{vmatrix} = \begin{vmatrix} a & 0 & \cdots & -a \\ b & a+b & & \vdots \\ \vdots & & \ddots & b \\ b & \cdots & b & a+b \end{vmatrix}$$

$$= a \cdot \det M_{m-1}(a,b) \; + \; (-1)^m(-a) \det M'_{m-1}(a,b)$$

$$= (a + mb) \cdot a^{m-1}.$$

□

Proposition 19. *With hypotheses as in Theorem 13 (but without assuming any conjectures!), we have*

$$\mathrm{Reg}_{K_c}(W) = h_c^{h_c-2} \cdot \prod_{\chi \neq \chi_1} \hat{h}_{K_c}(y_{c,\chi}).$$

Proof. In this proof we will work everywhere with the images of points in $V = E(K_c) \otimes \mathbb{C}$, which should not cause confusion.

The hypotheses imply that for each nontrivial character χ, the point $y_{c,\chi}$ has infinite order. Lemma 5 asserts that the $y_{c,\chi}$ are mutually orthogonal, so there is a lattice Λ in $W \otimes \mathbb{C}$ with basis the $y_{c,\chi}$, which has rank $h_c - 1$ (the number of nontrivial characters χ). Because the $y_{c,\chi}$ are all nonzero and orthogonal, we have

$$\mathrm{Reg}_{K_c}(\Lambda) = \prod_{\chi \neq \chi_1} \hat{h}_{K_c}(y_{c,\chi}).$$

By Proposition 10, the elements $(y_c^\sigma)_{1\neq\sigma\in G}$ are independent and nonzero, so they form a basis for their $\mathbb{Z}$-span $W_{/\mathrm{tor}}$ in V. Let M be the $(h_c-1)\times(h_c-1)$ change of basis matrix with respect to these two bases. More precisely, if for any fixed basis of V, we let B_Λ be the matrix with rows our chosen basis for Λ and B_W the matrix with rows our basis for W, then $B_\Lambda = M \cdot B_W$. We have $\mathrm{Reg}_{K_c}(\Lambda) = \det(M)^2 \cdot \mathrm{Reg}_{K_c}(W)$, so to compute $\mathrm{Reg}_{K_c}(W)$, it suffices to compute $\det(M)^2$. By definition of e_χ and using that $\mathrm{Tr}_{K_c/K}(y_c) = 0$ (in V) we have

$$y_{c,\chi} = \frac{1}{h_c}\sum_{\sigma\in G}\chi^{-1}(\sigma)y_c^\sigma = \frac{1}{h_c}\sum_{1\neq\sigma\in G}(\chi^{-1}(\sigma)-1)y_c^\sigma,$$

from which we read off the rows of the matrix M. For any two rows M_{χ_i}, M_{χ_j} of M,

$$\begin{aligned} M_{\chi_i}\cdot M_{\chi_j} &= \frac{1}{h_c^2}\sum_{1\neq\sigma\in G}(\chi_i^{-1}(\sigma)-1)(\chi_j^{-1}(\sigma)-1) \\ &= \frac{1}{h_c^2}\sum_{\sigma\in G}(\chi_i^{-1}(\sigma)-1)(\chi_j^{-1}(\sigma)-1) \\ &= \frac{1}{h_c^2}\sum_{\sigma\in G}(\chi_i\chi_j)^{-1}(\sigma)-\chi_i^{-1}(\sigma)-\chi_j^{-1}(\sigma)+1 = \begin{cases} \frac{2}{h_c} & \text{if } \chi_i=\chi_j^{-1}, \\ \frac{1}{h_c} & \text{otherwise.}\end{cases} \end{aligned}$$

Thus

$$(\det M)^2 = \det MM^T = \det(M_{\chi_i}\cdot M_{\chi_j})_{i,j} = \pm\begin{vmatrix} \frac{2}{h_c} & \frac{1}{h_c} & \cdots & \frac{1}{h_c} \\ \frac{1}{h_c} & \frac{2}{h_c} & & \vdots \\ \vdots & & \ddots & \frac{1}{h_c} \\ \frac{1}{h_c} & \cdots & \frac{1}{h_c} & \frac{2}{h_c}\end{vmatrix},$$

where the columns in the final matrix have been permuted so we have $2/h_c$ down the diagonal and $1/h_c$ everywhere else, which only affects the determinant up to sign. To evaluate this determinant we use Lemma 18 with $a = b = 1/h_c$ and $m = h_c - 1$ and obtain

$$\det(M)^2 = \left(\frac{1}{h_c}+(h_c-1)\cdot\frac{1}{h_c}\right)\cdot\left(\frac{1}{h_c}\right)^{h_c-2} = 1/h_c^{h_c-2}.$$

Thus

$$\mathrm{Reg}_{K_c}(W) = (\det M)^{-2} \cdot \mathrm{Reg}_{K_c}(\Lambda) = h_c^{h_c-2} \cdot \prod_{\chi \neq \chi_1} \hat{h}_{K_c}(y_{c,\chi}).$$

□

Proof of Theorem 13. Apply Conjecture 12 to the left-hand side of Equation (7), and to the first factor on the right-hand side, and Conjecture 6 to the remaining factors on the right hand side, to get

$$\begin{aligned}
&\frac{\|\omega_f\|^{2h_c} \cdot \mathrm{Reg}_{K_c}(E(K_c)) \cdot \#Ш(E/K_c) \cdot \prod c_{w,K_c}}{\sqrt{|D_{K_c}|} \cdot \#E(K_c)_{\mathrm{tor}}^2} \\
&\quad = \frac{\|\omega_f\|^2 \cdot \mathrm{Reg}_K(E(K)) \cdot \#Ш(E/K) \cdot \prod c_{v,K}}{\sqrt{|D_K|} \cdot \#E(K)_{\mathrm{tor}}^2} \cdot \prod_{\chi \neq \chi_1} \frac{h_c \cdot \|\omega_f\|^2}{\mathrm{cond}(\chi) \cdot u^2 \cdot \sqrt{|D_K|}} \cdot \hat{h}_{K_c}(y_{c,\chi}).
\end{aligned}$$

Cancelling $\|\omega_f\|^{2h_c}$ from both sides, and rearranging factors gives

$$\begin{aligned}
u^{2h_c} \cdot \frac{\sqrt{|D_K|^{h_c}} \cdot \prod_{\chi \neq \chi_1} \mathrm{cond}(\chi)}{\sqrt{|D_{K_c}|}} \cdot \frac{\prod c_{w,K_c}}{\prod c_{v,K}} \cdot \frac{\#Ш(E/K_c)}{\#Ш(E/K)} \\
= \frac{\mathrm{Reg}_K(E(K)) \cdot h_c^{h_c-1} \cdot \prod_{\chi \neq \chi_1} \hat{h}_{K_c}(y_{c,\chi})}{\mathrm{Reg}_{K_c}(E(K_c))} \cdot \frac{\#E(K_c)_{\mathrm{tor}}^2}{\#E(K)_{\mathrm{tor}}^2}.
\end{aligned} \tag{11}$$

We have $r = \mathrm{rank}(E(K))$, because we are assuming Conjecture 1 for E/K, and Proposition 11 implies that W and $E(K)$ are orthogonal, so

$$\mathrm{Reg}_{K_c}(E(K)+W) = \mathrm{Reg}_{K_c}(E(K)) \cdot \mathrm{Reg}_{K_c}(W) = h_c^r \cdot \mathrm{Reg}_K(E(K)) \cdot \mathrm{Reg}_{K_c}(W). \tag{12}$$

Combining Equation (12) with Proposition 19 yields

$$\begin{aligned}
\mathrm{Reg}_K(E(K)) \cdot h_c^{h_c-1} \cdot \prod_{\chi \neq \chi_1} \hat{h}_{K_c}(y_{c,\chi}) &= \mathrm{Reg}_K(E(K)) \cdot h_c \cdot \mathrm{Reg}_{K_c}(W) \\
&= h_c^{1-r} \cdot \mathrm{Reg}_{K_c}(E(K)+W).
\end{aligned}$$

Taking square roots of the absolute value of both sides of the formula in Lemma 17 and simplify Equation (11) using the above, we obtain

$$\begin{aligned}
u^{2h_c} \cdot \frac{\prod c_{w,K_c}}{\prod c_{v,K}} \cdot \frac{\#Ш(E/K_c)}{\#Ш(E/K)} &= h_c^{1-r} \cdot \frac{\mathrm{Reg}_{K_c}(E(K)+W)}{\mathrm{Reg}_{K_c}(E(K_c))} \cdot \frac{\#E(K_c)_{\mathrm{tor}}^2}{\#E(K)_{\mathrm{tor}}^2} \\
&= h_c^{1-r} \cdot [E(K_c)_{/\mathrm{tor}} : (E(K)+W)_{/\mathrm{tor}}]^2 \cdot \frac{\#E(K_c)_{\mathrm{tor}}^2}{\#E(K)_{\mathrm{tor}}^2}.
\end{aligned}$$

Solving for $[E(K_c)_{/\mathrm{tor}} : (E(K) + W)_{/\mathrm{tor}}]^2$ then yields the claimed formula in Theorem 13. $\square$

If we remove the $\mathrm{cond}(\chi)$ factor from Conjecture 6, then rederive Theorem 13 as in the proof above, the one change is that in Equation (11), instead of having

$$\frac{\sqrt{|D_K|^{h_c}} \cdot \prod_{\chi \neq \chi_1} \mathrm{cond}(\chi)}{\sqrt{|D_{K_c}|}} = 1$$

we get an extra factor of

$$\frac{\sqrt{|D_K|^{h_c}}}{\sqrt{|D_{K_c}|}}$$

next to u^{2h_c}. According to Lemma 16, we have

$$\frac{\sqrt{|D_{K_c}|}}{\sqrt{|D_K|^{h_c}}} = \prod_{p|c} p^{\frac{ph_c}{p+1}}.$$

In the special case when $c = p$ is an odd prime and K has class number 1, this simplifies to

$$\frac{\sqrt{|D_{K_c}|}}{\sqrt{|D_K|^{h_c}}} = p^{\frac{p(p+1)}{p+1}} = p^p,$$

which is never a perfect square, which leads to a contradiction (see Proposition 14).

5. An Example

Suppose E is the elliptic curve 389a given by $y^2 + y = x^3 + x^2 - 2x$, which has rank 2 and conductor 389. The field $K = \mathbb{Q}(\sqrt{-7})$ satisfies the Heegner hypothesis, $c = 5$ is inert in K, and $u = 1$. Since K has class number 1, we have $h_c = c + 1 = 6$. According to [JLS09], the field K_c is obtained by adjoining a root of

$$z^6 + 1750z^5 - 26551875z^4 - 570237500z^3 + 202540106562500z^2$$
$$- 292113275671875000z + 134537112978310546875$$

to K, and we find by computer calculation (or Lemma 16) that

$$D_{K_c} = 5^{10} \cdot 7^6 = (-7)^6 5^{(2 \cdot 5 \cdot 6)/(5+1)}.$$

All of the p-adic Galois representations associated to E are surjective, so $E(K_c)_{\mathrm{tor}} = 0$. The BSD conjecture and a computation using [S$^+$11] implies that $Ш(E/K) = 1$, and we find by computation that $r = r_{\mathrm{an}}(E/K) = 3$. The Tamagawa numbers of E at 389 is 1. Assuming the hypotheses of Theorem 13 are satisfied, we have

$$[E(K_5) : E(K) + W]^2 = \#Ш(E/K_5) \cdot 6^2. \tag{13}$$

Let σ be a choice of generator for $G = \mathrm{Gal}(K_5/K)$. As explained in [JLS09, Ste10a], the Kolyvagin class $\tau \in \mathrm{H}^1(K, E[3])$ associated to y_5 is nonzero and $Ш(E/K)[3] = 0$, so there is some nonzero $P \in E(K)/3E(K)$ such that $[P] \mapsto [P_5] \in E(K_5)/3E(K_5)$, where $P_5 = \sum i\sigma^i(y_5) \in W$. Thus $P - P_5 = 3Q \in 3E(K_5)$, where $Q \in E(K_5)$ but $Q \notin E(K) + W$. Hence $3 \mid [E(K_5) : E(K) + W]$, as predicted by Equation (13).

6. Ideas for Future Work

It would be of interest to compute the relevant L-functions in this paper for several specific examples, using the methods of Dokchitser [Dok04] or Rubinstein. In addition, one could explicitly compute the Mordell-Weil group $E(K_c)$ in some examples. It would also be of interest to find explicit examples that illustrate the situation discussed in Remark 9, in which $\mathrm{ord}_{s=1} L(E, \chi, s) \geq 3$, since we are currently not aware of any such examples.

Regarding generalizations, it would be natural to fully treat the case when $r = 1$, so that W has finite index in $E(K_c)$. It would also be good to extend the results of this paper to modular abelian varieties A_f attached to newforms in $S_2(\Gamma_0(N))$. Another possible generalization would be to quadratic imaginary fields that do not satisfy the Heegner hypothesis, so the modular curve $X_0(N)$ is replaced by a Shimura curve (see, e.g., the extensive work of Bertolini and Darmon). In another direction, one could likely generalize our results to elliptic curves (or abelian varieties) over totally real fields, following the program initiated by Zhang in [Zha01b].

Assume that for all nontrivial χ we have $\mathrm{ord}_{s=1} L(E, \chi, s) = 1$. Under this hypothesis, it would be of great interest to prove the divisibility

$$\frac{\#Ш(E/K_c)}{\#Ш(E/K)} \;\Big|\; [E(K_c) : E(K) + W]^2,$$

at least away from an explicit finite list of primes. This might make it possible to compute $Ш(E/K_c)/Ш(E/K)$ for a specific elliptic curve. This would be

a generalization of the explicit upper bounds on $\#Ш(E/K)$ from [GJP+09, Thm. 3.4]. The cryptic [Ber10, Remark 5.23(1)] is relevant, because it claims one can prove at least finiteness of $Ш(E/K_c)(\chi)$, in the Shimura curve case, though warns "The original methods of Kolyvagin, based on the Gross-Zagier formula, allow to prove a similar statement only when χ is quadratic." This should be contrasted with [YZZ10, §1.6, Thm. C], where it is claimed that under our hypothesis Tian-Zhang have in fact proved that $Ш(E/K_c)(\chi)$ is finite, using the original method of Kolyvagin based on their generalization of the Gross-Zagier formula.

References

[ARS06] Amod Agashe, Kenneth Ribet, and William A. Stein, *The Manin constant*, Pure Appl. Math. Q. **2** (2006), no. 2, part 2, 617–636, `http://wstein.org/papers/ars-manin/`. MR 2251484 (2007c:11076)

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic), `http://math.stanford.edu/~conrad/papers/tswfinal.pdf`. MR 2002d:11058

[BD90] Massimo Bertolini and Henri Darmon, *Kolyvagin's descent and Mordell-Weil groups over ring class fields*, J. Reine Angew. Math. **412** (1990), 63–74, `http://www.math.mcgill.ca/darmon/pub/Articles/Research/04.Kolyvagin-descent/paper.pdf`. MR 1079001 (91j:11048)

[Ber10] Massimo Bertolini, *Report on the Birch and Swinnerton-Dyer conjecture*, Milan J. Math. **78** (2010), 153–178, `http://newrobin.mat.unimi.it/users/mbertoli/report.bsd.pdf`. MR 2684777

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990. MR 91i:14034

[Cha05] Byungchul Cha, *Vanishing of some cohomology groups and bounds for the Shafarevich-Tate groups of elliptic curves*, J. Number Theory. **111** (2005), 154–

178, http://wstein.org/papers/bib/cha-vanishing_of_some_cohomology_groups_and_bounds_for_the_Shafarevich-Tate_groups_of_elliptic_curves.pdf.

[Coh07] Henri Cohen, *Number theory. Vol. I. Tools and Diophantine equations*, Graduate Texts in Mathematics, vol. 239, Springer, New York, 2007. MR 2312337 (2008e:11001)

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

[FT93] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993. MR 1215934 (94d:11078)

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

[Gro84] Benedict H. Gross, *Heegner points on $X_0(N)$*, Modular forms (Durham, 1983), Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester, 1984, http://wstein.org/papers/bib/gross-heegner_points_on_X0N.pdf, pp. 87–105. MR 803364 (87f:11036b)

[Gro91] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, http://wstein.org/papers/bib/gross-kolyvagins_work_on_modular_elliptic_curves.pdf, pp. 235–256.

[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320, http://wstein.org/papers/bib/Gross-Zagier_Heegner_points_and_derivatives_of_Lseries.pdf. MR 87j:11057

[Hay95] Yoshiki Hayashi, *The Rankins L-function and Heegner points for general discriminants.*, Proc. Japan Acad.

Ser. A Math. Sci. (1995), no. 71(2), 30–32, http://projecteuclid.org/DPubS/Repository/1.0/Disseminate?view=body&id=pdf_1&handle=euclid.pja/1195510808.

[Jet08] Dimitar Jetchev, *Global divisibility of Heegner points and Tamagawa numbers*, Compos. Math. **144** (2008), no. 4, 811–826, http://arxiv.org/abs/math/0703431. MR 2441246 (2010b:11072)

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

[Lan91] S. Lang, *Number theory. III*, Springer-Verlag, Berlin, 1991, Diophantine geometry. MR 93a:11048

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

[MS10] Robert L. Miller and Michael Stoll, *Explicit isogeny descent on elliptic curves*, http://arxiv.org/abs/1010.3334, 2010.

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

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Ste04] W. A. Stein, *Shafarevich-Tate Groups of Nonsquare Order*, Modular Curves and Abelian Varieties, Progress of Mathematics (2004), 277–289, http://wstein.org/papers/nonsquaresha/.

[Ste10a] William Stein, *Heegner points on rank two elliptic curves*, http://wstein.org/papers/kolyconj2/.

[Ste10b] ———, *Toward a Generalization of the Gross-Zagier Conjecture*, Internat. Math. Res. Notices (2010), http://wstein.org/papers/stein-ggz/.

[SW11] William Stein and Christian Wuthrich, *Computations About Tate-Shafarevich Groups Using Iwasawa Theory*, in preparation (2011), http://wstein.org/papers/shark/.

[Wat06] Mark Watkins, *Some remarks on Heegner point computations*, Preprint (2006), http://arxiv.org/abs/math/0506325.

[Wil95] A. J. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551, http://users.tpg.com.au/nanahcub/flt.pdf.

[Wil00] ———, *The Birch and Swinnerton-Dyer Conjecture*, http://www.claymath.org/prize_problems/birchsd.htm.

[YZZ10] X. Yuan, S. Zhang, and W. Zhang, *Gross-Zagier formula*, http://www.math.columbia.edu/~yxy/preprints/GZ.pdf.

[Zha01a] Shou-Wu Zhang, *Gross-Zagier formula for* GL_2, Asian J. Math. **5** (2001), no. 2, 183–290, http://intlpress.com/AJM/p/2001/5_2/AJM-5-2-183-290.pdf. MR 1868935 (2003k:11101)

[Zha01b] ———, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), no. 1, 27–147. MR 1826411 (2002g:11081)

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