Heegner Points on Rank Two Elliptic Curves
(**Preliminary Version**)

William Stein*

October 2009

Abstract

Let E be an elliptic curve over $\mathbb{Q}$ of analytic rank 2, and let K be a quadratic imaginary field such that each prime dividing the conductor of E splits in K. We use Heegner points to define $\mathbb{F}_\ell$-rational points $z \in E(\mathbb{F}_\ell) \otimes \mathbb{F}_p$ for certain inert primes ℓ, p of K. We then give the first complete algorithm for computing these points z, and find that they are frequently nonzero, which provides the first ever proof of a deep conjecture of Kolyvagin in these cases. We also observe that if any z is nonzero then $E(\mathbb{Q})$ has algebraic rank at most 2.

1 Introduction

The main motivation for this paper is to give new algorithms for explicit computation with Heegner points on rank 2 elliptic curves. Let E be an elliptic curve over $\mathbb{Q}$ of analytic rank 2, and let K be a quadratic imaginary field such that each prime dividing the conductor of E splits in K. We use Heegner points to define $\mathbb{F}_\ell$-rational points $z \in E(\mathbb{F}_\ell) \otimes \mathbb{F}_p$ for certain inert primes ℓ, p of K. We then give the first complete algorithm for computing these points z when K has class number 1, and find that they are frequently nonzero, which provides the first ever proof of a deep conjecture of Kolyvagin in these cases. We also observe that if any z is nonzero then $E(\mathbb{Q})$ has algebraic rank at most 2.

On [Kol91, pg. 118], Kolyvagin alludes to an algorithm for computing the points he constructs on elliptic curves using Heegner points:

> "in view of (10), we can calculate the coordinates of $\tilde{P}_\lambda \in \tilde{E}(F)$, where F is the residue field of K_c." [notation changed slightly]

Kolyvagin's paper (10) [KL89] doesn't explicitly mention this problem. We take a step in the direction hinted at by Kolyvagin's remark.

In this paper we present a new algorithm—inspired by theoretical work of Cornut, Jetchev, Kane, Mazur, and Vatsal—to for the first time ever provably compute the Heegner points considered by Kolyvagin. 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 class number 1 quadratic imaginary field K. Here's is a conceptual outline of what the algorithm does:

*The work was supported by NSF grants...

1. Take the Heegner point x_c on the modular curve $X_0(N)$ and reduce it modulo an inert prime ℓ to obtain an element of $X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}}$.
2. Compute the "Kolyvagin derivative" on the reduction of x_c to obtain a divisor in $\mathrm{Div}(X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}})$.
3. Use Hecke operators, linear algebra, and Ihara's theorem to compute

$$\mathrm{Div}(X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}}) \otimes (\mathbb{Z}/q\mathbb{Z}) \to E(F_\ell) \otimes (\mathbb{Z}/q\mathbb{Z}),$$

up to a fixed scalar multiple.

Everything above is done *algebraically.* Following [Piz80], we view $\mathrm{Div}(X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}})$ as the set of right ideal classes in an Eichler order of level N in the rational quaternion algebra ramified at ℓ and ∞. We use ternary quadratic forms to find one of the two right ideals I whose left order has an optimal embedding of the order $\mathcal{O}_K$, thus computing the reduction of x_1. Then we use x_1 and a parametrization of the ideals $J \subset I$ with $I/J \cong (\mathbb{Z}/c\mathbb{Z})^2$ to compute the Kolyvagin derivative.

Acknowledgement: The author would like to thank Dimitar Jetchev, Barry Mazur, Karl Rubin, and Jared Weinstein for helpful discussions.

2 Heegner Points

Let E be an elliptic curve over $\mathbb{Q}$ and let

$$L(E,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

be the L-series attached to E.

Conjecture 2.1 (Birch and Swinnerton-Dyer)**.**

$$\mathrm{rank}\, E(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E,s).$$

Conjecture 2.1 is a theorem of Kolyvagin when $\mathrm{ord}_{s=1} L(E,s) \leq 1$, but is completely open when $\mathrm{ord}_{s=1} L(E,s) \geq 2$.

For simplicity, we make the running hypothesis for the rest of this paper that E does not have complex multiplication and that

$$\mathrm{ord}_{s=1} L(E,s) = 2,$$

so the above conjecture makes the assertion that $\mathrm{rank}(E(\mathbb{Q})) = 2$. We will relax these hypotheses in a subsequent paper (see Section 3.1).

Elliptic curves over $\mathbb{Q}$ are endowed with extra structure coming from modular curves, which helps in investigating Conjecture 2.1. Fix an odd prime power $q = p^n$ such that

$$\overline{\rho}_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$$

is surjective, and fix a quadratic imaginary field $K = \mathbb{Q}(\sqrt{D})$ of discriminant D such that each prime dividing N splits in K, and such that

$$\mathrm{ord}_{s=1} L(E^D, s) = 1.$$

Let N be the conductor of E and $\pi : X_0(N) \to E$ be the modular parametrization, which exists by [BCDT01].

Let c be any prime number that is inert in K, coprime to ND, and such that

$$q \mid \gcd(a_c,\, c+1).$$

Let K_c be the ring class field of conductor c. This is an abelian extension of the Hilbert class field K_1 of K that is unramified outside c and has Galois group

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

where $\mathcal{O}_K$ is the ring of integer of K. Let $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ be the order in $\mathcal{O}_K$ of conductor c and $\mathcal{N}$ a fixed choice of ideal in $\mathcal{O}_K$ with $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. The Heegner point associated to c is

$$x_c = \left(\mathbb{C}/\mathcal{O}_c,\ \ (\mathcal{N} \cap \mathcal{O}_c)^{-1}/\mathcal{O}_c\right) \in X_0(N)(K_c),$$

which has image

$$y_c = \pi_E(x_c) \in E(K_c).$$

Our motivation is to study $E(\mathbb{Q})$, so it is natural to compute the trace of y_c.

Proposition 2.2. *We have* $\mathrm{Tr}_{K_c/K_1}(y_c) = a_c y_1 \in E(K_1)$.

Proof. This is because if T_c is the cth Hecke operator, then

$$T_c(x_1) = \sum_{\sigma \in \mathrm{Gal}(K_c/K_1)} \sigma(x_c)$$

as divisors on $X_0(N)$. See [JK09] or [[Gross]] or [[Kolyvagin]]. □

The Gross-Zagier theorem implies that the height of $\mathrm{Tr}_{K_1/K}(y_1) \in E(K)$ is a multiple of $L'(E/K,1)$. However, we assumed $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 2$, so $L'(E/K,1) = 0$, hence $\mathrm{Tr}_{K_c/K}(y_c)$ is torsion for all c. Thus the points y_c cannot be used to directly construct nontorsion elements of the Mordell-group $E(\mathbb{Q})$. However, for any inert prime ℓ, we *can* construct elements in $E(\mathbb{F}_\ell) \otimes (\mathbb{Z}/q\mathbb{Z})$ whose properties have profound consequences for the arithmetic of $E(\mathbb{Q})$, as we will soon see.

2.1 Constructing elements of $E(\mathbb{F}_\ell) \otimes (\mathbb{Z}/q\mathbb{Z})$

Let $[y_c]$ denote the equivalence class of y_c in $E(K_c) \otimes (\mathbb{Z}/q\mathbb{Z})$. For any generator $\sigma \in \mathrm{Gal}(K_c/K_1)$, let

$$P = \sum_{i\ \in\ \mathbb{Z}/(c+1)\mathbb{Z}} i\sigma^i([y_c]).$$

Proposition 2.3.

$$P \in (E(K_c) \otimes (\mathbb{Z}/q\mathbb{Z}))^{\mathrm{Gal}(K_c/K_1)}$$

Proof. We have

$$\begin{aligned}\sigma(P) &= \sum_{i\ \in\ \mathbb{Z}/(c+1)\mathbb{Z}} i\sigma(\sigma^i)([y_c]) = \sum_{i\ \in\ \mathbb{Z}/(c+1)\mathbb{Z}} i\sigma^{i+1}([y_c]) \\ &= \sum_{i\ \in\ \mathbb{Z}/(c+1)\mathbb{Z}} (i-1)\sigma^i([y_c]) = P - \mathrm{Tr}_{K_c/K_1}([y_c]) = P,\end{aligned}$$

since $q \mid a_c$ and $\mathrm{Tr}_{K_c/K_1}(y_c) = a_c y_1$ by Proposition 2.2. □

Let

$$P_{c,\sigma} = \mathrm{Tr}_{K_1/K}(P) \in (E(K_c) \otimes (\mathbb{Z}/q\mathbb{Z}))^{\mathrm{Gal}(K_c/K)}.$$

Note that $P_{c,\sigma}$ depends on σ, and replacing σ by a different generator of $\mathrm{Gal}(K_c/K_1)$ changes $P_{c,\sigma}$ by multiplication by an element of $(\mathbb{Z}/q\mathbb{Z})^*$:

$$P_{c,\sigma^j} = \sum_{i\,\in\,\mathbb{Z}/(c+1)\mathbb{Z}} i\sigma^{ji}([y_c]) = \sum_{i\,\in\,\mathbb{Z}/(c+1)\mathbb{Z}} \frac{i}{j}\sigma^i([y_c]) = \frac{1}{j}P_{c,\sigma}.$$

Lemma 2.4. *We have $P_{c,\sigma} \in (E(K_c) \otimes (\mathbb{Z}/q\mathbb{Z}))^{\mathrm{Gal}(K_c/\mathbb{Q})}$.*

Proof. This follows from [Gro91, Prop. 5.3]. The basic idea is that if $\tau \in \mathrm{Gal}(K_c/\mathbb{Q})$ is complex conjugation on K_c, then $\tau\sigma^i\tau = \sigma^{-i}$ for all i, so

$$\begin{aligned}\tau P_{c,\sigma} &= \sum_{i\,\in\,\mathbb{Z}/(c+1)\mathbb{Z}} i\tau\sigma^i([y_c]) = \sum_{i\,\in\,\mathbb{Z}/(c+1)\mathbb{Z}} i\sigma^{-i}\tau([y_c]) \\ &= \sum_{i\,\in\,\mathbb{Z}/(c+1)\mathbb{Z}} (-i)\sigma^i\tau([y_c]) = -\sum_{i\,\in\,\mathbb{Z}/(c+1)\mathbb{Z}} (-i)\sigma^i(\tau([y_c])) = P_{c,\sigma}.\end{aligned}$$

In the last step we use that $\tau(y_c) = -\sigma'(y_c) + (\text{torsion})$ for some σ', and q is coprime to any torsion. The sign is minus because E has analytic rank 2. Also $P_{c,\sigma}$ is $\mathrm{Gal}(K_c/\mathbb{Q})$-equivariant so multiplication by σ' does nothing. ☐

Let $\mathrm{res} : \mathrm{H}^1(\mathbb{Q}, E[q]) \to \mathrm{H}^1(K_c, E[q])$ be the restriction map and δ the connecting homomorphism. We have a commutative diagram:

$$\begin{array}{ccccc} (E(K_c) \otimes (\mathbb{Z}/q\mathbb{Z}))^{\mathrm{Gal}(K_c/\mathbb{Q})} & \xhookrightarrow{\delta} & \mathrm{Sel}^{(q)}(E/K_c)^{\mathrm{Gal}(K_c/\mathbb{Q})} & \longrightarrow & Ш(E/K_c)[q]^{\mathrm{Gal}(K_c/\mathbb{Q})} \\ \uparrow & & \uparrow & & \uparrow \\ E(\mathbb{Q}) \otimes (\mathbb{Z}/q\mathbb{Z}) & \xhookrightarrow{\delta} & \mathrm{Sel}^{(q)}(E/\mathbb{Q}) & \longrightarrow & Ш(E/\mathbb{Q})[q] \end{array}$$

Proposition 2.5. *There is a unique element $\tau_{c,\sigma} \in \mathrm{Sel}^{(q)}(E/\mathbb{Q})$ such that*

$$\mathrm{res}(\tau_{c,\sigma}) = \delta(P_{c,\sigma}) \in \mathrm{H}^1(K_c, E[q]).$$

Proof. By Lemma 2.4, we have $\delta(P_{c,\sigma}) \in \mathrm{H}^1(K_c, E[q])^{\mathrm{Gal}(K_c/\mathbb{Q})}$. As explained in [Gro91, §4], there exists a unique $\tau_{c,\sigma} \in \mathrm{H}^1(\mathbb{Q}, E[q])$ such that $\mathrm{res}(\tau_{c,\sigma}) = \delta(P_{c,\sigma})$. That the image of $\mathrm{res}(\tau_{c,\sigma})$ in $\mathrm{H}^1(\mathbb{Q}, E)[d]$ is locally trivially follows from [Gro91, Prop. 6.2] with $n = c$ and $m = 1$, since $L'(E/K, 1) = 0$. ☐

Lemma 2.6. *The group $E(\mathbb{F}_\ell) \otimes (\mathbb{Z}/q\mathbb{Z})$ is cyclic of order q.*

Proof. See [Ste09, Lem. 5.1]. ☐

For any inert prime $\ell \neq c$, let λ be a prime ideal lying over ℓ in the ring of integers of K_c. Then

$$z_{c,\sigma,\ell} \;=\; P_{c,\sigma} \pmod{\lambda} \in E(\mathbb{F}_\ell) \otimes (\mathbb{Z}/q\mathbb{Z})$$

is well defined by [Ste09, Prop. 5.4].

Theorem 2.7. *Suppose there exists c, ℓ such that $z_{c,\sigma,\ell} \neq 0$. Then*

$$\mathrm{rank}(E(\mathbb{Q})) \leq 2$$

with equality if and only if $\text{Ш}(E/\mathbb{Q})(p)$ is finite. If $\mathrm{rank}(E(\mathbb{Q})) = 2$ and q is prime, then $\text{Ш}(E/\mathbb{Q})[p] = 0$.

Proof. If $z_{c,\sigma,\ell} \neq 0$ then the Kolyvagin cohomology class $\tau_c \in \mathrm{H}^1(K, E[q])$ is nonzero, so Kolyvagin's conjecture A is true. The desired conclusion then follows from [Ste09, Thm 4.2]. □

Suppose q is prime and $\mathrm{rank}(E(\mathbb{Q})) = 2$. If $P_{c,\sigma} \neq 0$, then as remarked above [Ste09, Thm 4.2] implies that $\text{Ш}(E/\mathbb{Q})[p] = 0$. Thus there is a unique element $R_{c,\sigma} \in E(\mathbb{Q}) \otimes (\mathbb{Z}/q\mathbb{Z})$ such that $R_{c,\sigma}$ maps to $P_{c,\sigma}$ under the natural inclusion, and also $\delta(R_{c,\sigma}) = \tau_{c,\sigma}$. Let

$$r_\ell : E(\mathbb{Q}) \otimes (\mathbb{Z}/q\mathbb{Z}) \longrightarrow E(\mathbb{F}_\ell) \otimes (\mathbb{Z}/q\mathbb{Z}). \tag{2.1}$$

be the reduction map modulo ℓ. Then

$$r_\ell(R_{c,\sigma}) = z_{c,\sigma,\ell}.$$

Thus to compute $R_{c,\sigma}$ it suffices to compute z_{c,σ,ℓ_i} for two primes ℓ_1 and ℓ_2 such that $\ker(r_{\ell_1}) \cap \ker(r_{\ell_2}) = 0$.

Conjecture 2.8 (Kolyvagin)**.** *For any prime p as above, there exists a power $q = p^n$ of p and primes c, ℓ such that $z_{c,\sigma,\ell} \neq 0$.*

For each prime number v, let t_v be the Tamagawa number of E at v. Recall that $q = p^n$ is an odd prime power.

Conjecture 2.9. *For every prime ℓ there are infinitely many c with $z_{c,\sigma,\ell} \neq 0$ if and only if*

$$n > \mathrm{ord}_p\left(\sqrt{\#\text{Ш}(E/\mathbb{Q})} \cdot \prod t_v\right).$$

Summary: Though there is as of yet no known satisfactory construction of elements of infinite order in $E(\mathbb{Q})$, we compensate by giving a construction of elements of $E(\mathbb{F}_\ell) \otimes (\mathbb{Z}/q\mathbb{Z})$ for inert primes ℓ. Moreover, if any of these elements is nonzero, then one inequality in the Birch and Swinnerton-Dyer conjecture is true:

$$\mathrm{rank}\, E(\mathbb{Q}) \leq \mathrm{ord}_{s=1} L(E, s) = 2.$$

3 Rational Quaternion Algebras

In this section we explain how to compute $z_{c,\sigma,\ell}$ in some cases. Fix an Eichler order R of level N in the quaternion algebra $B = B_{\ell,\infty}$ ramified at ℓ and infinity. Assume for simplicity that K has class number 1. Then there are exactly two right ideal classes whose left order admits an optimal embedding of $\mathcal{O}_K$. We compute and fix one of these right ideals I using ternary quadratic forms, as explained in [JK09]. The ideal class of I defines the same point on $X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}}$ as the reduction of x_1 modulo ℓ.

By replacing I by an equivalent ideal, we can arrange so that $I \otimes (\mathbb{Z}/c\mathbb{Z}) = R \otimes (\mathbb{Z}/c\mathbb{Z})$, and can then *pick* a local splitting, so

$$I \otimes (\mathbb{Z}/c\mathbb{Z}) = R \otimes (\mathbb{Z}/c\mathbb{Z}) \cong M_2(\mathbb{Z}/c\mathbb{Z}).$$

Suppose the equivalence class of $\alpha \in \mathcal{O}_K$ is a generator of $(\mathcal{O}_K/c\mathcal{O}_K)^*/(\mathbb{Z}/c\mathbb{Z})^*$. Using the embedding of $\mathcal{O}_K$ into the left order of I from above, we may view α as an element of B. Let $\overline{\alpha} \in M_2(\mathbb{Z}/c\mathbb{Z})$ be its image via the above splitting. For each $i = 0, \ldots, c$, let $\overline{J}_i$ be the set of elements of $M_2(\mathbb{Z}/c\mathbb{Z})$ whose left kernel contains $(1,0)\overline{\alpha}^i$. Let J_i be the inverse image in I of $\overline{J}_i$ under the map $I \to M_2(\mathbb{Z}/c\mathbb{Z})$, and note that J_i is a right R-ideal such that $I/J_i \cong (\mathbb{Z}/c\mathbb{Z})^2$.

Theorem 3.1. *Let $\sigma \in \mathrm{Gal}(K_c/K_1)$ correspond to α via class field theory. Then the divisor*

$$\sum_{i=0}^{c} i[J_i] \in \mathrm{Div}(X_0(N)^{\mathrm{ss}}_{\mathbb{F}_{\ell^2}})$$

maps to $z_{c,\ell,\sigma}$ under $\mathrm{Div}(X_0(N)^{\mathrm{ss}}_{\mathbb{F}_{\ell^2}}) \to E(\mathbb{F}_\ell) \otimes (\mathbb{Z}/q\mathbb{Z})$.

Proof. □

Remark 3.2. If T_c is the cth Hecke operator then

$$T_c([I]) = \sum_{i=0}^{c} [J_i].$$

Proposition 3.3. *If q does not divide the modular degree of E, then the map*

$$\mathrm{Div}(X_0(N)^{\mathrm{ss}}_{\mathbb{F}_{\ell^2}}) \to E(\mathbb{F}_\ell) \otimes (\mathbb{Z}/q\mathbb{Z})$$

is surjective.

Proof. Let $\mathfrak{m}$ be the maximal ideal of the Hecke algebra $\mathbb{T}$ generated by the prime q and by $T_n - a_n(E)$ for all n. The map

$$X = \mathrm{Div}(X_0(N)^{\mathrm{ss}}_{\mathbb{F}_{\ell^2}}) \to E(\mathbb{F}_\ell) \otimes (\mathbb{Z}/q\mathbb{Z})$$

factors through

$$X \longrightarrow X \otimes (\mathbb{T}/\mathfrak{m}).$$

Since the modular degree is coprime to q the composition of the maps

$$E(\mathbb{F}_{\ell^2}) \to J_0(N)(\mathbb{F}_{\ell^2}) \to E(\mathbb{F}_{\ell^2}) \otimes (\mathbb{Z}/q\mathbb{Z})$$

is surjective.

Now use Ihara's theorem... [[more details needed]]. □

We implemented in Sage[1] algorithms based on the above results, and used them to compute $z_{c,\sigma,\ell}$ for 10 different rank 2 curves, and various primes ℓ, primes $q = 3, 5, 7$, discriminants D of class number 1, and primes c, as in Table 3.1. Let r_ℓ be the reduction map from Equation (2.1). We chose the pairs (E, ℓ) so that r_ℓ is surjective and if ℓ_1 and ℓ_2 are the first two primes for a given elliptic curve E, then $\ker(r_{\ell_1}) \cap \ker(r_{\ell_2}) = 0$. For each pair (E, ℓ) in the table, we considered all fundamental discriminants $D \leq -5$ such that $K = \mathbb{Q}(\sqrt{D})$ has class number 1, satisfies the Heegner hypothesis for E, and for which ℓ is inert.

[1] All computations in this section can be done in Version 4.1.1 + patches from trac 6616 of the free and open source software Sage `http://sagemath.org`. The code we used to do the computations along with the output files is at `http://wstein.org/home/wstein/db/kolyconj/`. All computations were done under Linux (Ubuntu and Redhat) on several Sun Fire X4450 servers with 24 2.6Ghz cores and 128GB RAM each, at University of Washington and Univervisty of Georgia [[ack. NSF and Sun]].

Table 3.1: Rank 2 elliptic curves for which we computed $z_{c,\sigma,\ell}$.

E	D	q	ℓ	E	D	q	ℓ	E	D	q	ℓ
389a1	-7	3	5	**563a1**	-8	3	23	**643a1**	-8	3	29
389a1	-7	3	17	**563a1**	-163	3	17	**643a1**	-11	3	29
389a1	-7	3	41	**563a1**	-163	3	23	**643a1**	-19	3	29
389a1	-7	5	19	**571b1**	-7	3	47	**643a1**	-43	3	29
389a1	-11	3	17	**571b1**	-7	7	97	**643a1**	-67	3	11
389a1	-11	3	41	**571b1**	-7	7	167	**655a1**	-19	3	29
389a1	-11	5	19	**571b1**	-8	3	47	**681c1**	-8	3	23
389a1	-19	3	41	**571b1**	-8	5	29	**709a1**	-7	3	5
389a1	-67	3	5	**571b1**	-8	5	149	**709a1**	-7	3	47
389a1	-67	3	41	**571b1**	-8	7	167	**709a1**	-43	3	5
433a1	-8	5	79	**571b1**	-19	5	29	**709a1**	-67	3	5
433a1	-8	5	199	**571b1**	-19	7	97	**709a1**	-163	3	5
433a1	-11	3	17	**571b1**	-19	7	167	**718b1**	-7	3	5
433a1	-11	3	41	**571b1**	-67	3	11	**997c1**	-19	3	41
433a1	-11	5	79	**571b1**	-67	7	97	**997c1**	-67	3	41

Table 3.1 has columns E, D, q, ℓ. Each row has the property that E has rank 2, ℓ is inert in the field $K = \mathbb{Q}(\sqrt{D})$, and K satisfies the Heegner hypothesis for E. Also, we have $q \mid \gcd(\ell + 1, a_\ell(E))$. We chose these for because the rank of $\mathrm{Div}(X_0(N)^{\mathrm{ss}}_{\mathbb{F}_{\ell^2}})$ is relatively small.

Warning: In about 25% of the cases, q divides the modular degree of E, so Proposition 3.3 does not apply. In these cases the computation of $z_{c,\sigma,\ell}$ that we give in Tables 3.2–3.4 is not rigorous. The problematic cases are the following pairs (E, q):

$$(\mathbf{389a1}, 5), (\mathbf{571b1}, 3), (\mathbf{655a1}, 3), (\mathbf{681c1}, 3), (\mathbf{997c1}, 3).$$

We proceed as if this warning does not apply in the following discussion.

The Tamagawa numbers of all of our curves are 1 or 2, and in all cases $\overline{\rho}_{E,q}$ is surjective.

Table 3.2 contains data about the points $z_{c,\sigma,\ell}$. The columns labeled E, D, q, and ℓ correspond exactly to the entries in Table 3.2. The column labeled dim gives the dimension of $\mathrm{Div}(X_0(N)^{\mathrm{ss}}_{\mathbb{F}_{\ell^2}})$, which greatly impacts the complexity of our algorithm. The column labeled $\max c$ contains the largest c such that we managed to compute $z_{c,\sigma,\ell}$. The columns $= 0$ and $\neq 0$ are a count of how many $z_{c,\sigma,\ell}$ are 0 and not 0 among those we computed; note that for each c, ℓ we compute $z_{c,\sigma,\ell}$ for only one choice of σ, since other choices of σ would yield a nonzero scalar multiple, hence we often just write $z_{c,\ell}$. The columns labeled $z_{c,\ell} = 0$ and $z_{c,\ell} \neq 0$ give the first few c such that $z_{c,\ell}$ is zero or nonzero, respectively.

One consistency check on Table 3.2 comes from the rows labeled $(\mathbf{389a1}, -7, 3, 17)$ and $(\mathbf{389a1}, -7, 3, 41)$, since the reduction maps

$$E(\mathbb{Q}) \to E(\mathbb{F}_\ell) \otimes (\mathbb{Z}/3\mathbb{Z})$$

have the same kernel for $\ell = 17$ and 41. Hence the $z_{c,17} \neq$ if and only if $z_{c,41} \neq 0$, which was indeed the case in the range of our computations.

In every single case in Table 3.2 we find at least one c such that $z_{c,\ell} \neq 0$, as predicted by Conjecture 2.9. This gives strong computational evidence for Kolyvagin's conjecture for $q = 3, 5, 7$. Note, however, that the distribution between 0 and nonzero is often far from uniform.

Tables 3.3–3.4 provide further details about the distribution of elements of

$$\mathrm{Sel}^{(q)}(E/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^2$$

coming from this construction. The first 5 columns labeled E, D, q, ℓ_1 and ℓ_2 specify an elliptic curve, fundamental discriminant, prime q and two primes ℓ_1 and ℓ_2, chosen from the data summarized in Table 3.2. The primes ℓ_1 and ℓ_2 are chosen so that the intersection of the two reduction maps to $E(\mathbb{F}_{\ell_i}) \otimes (\mathbb{Z}/q\mathbb{Z})$ is 0. Since the Selmer group has dimension 2 and in our implementation we chose the generator $\sigma \in \mathrm{Gal}(K_c/K_1)$ in a consistent manner, this allows us to deduce the subspace spanned by $\tau_{c,\sigma}$ in $\mathrm{Sel}^{(q)}(E/\mathbb{Q})$ with respect to some unknown basis for $\mathrm{Sel}^{(q)}(E/\mathbb{Q})$. The column labeled $\tau_{c,\sigma}$ gives the normalized generator for this subspace. The next column, labeled # gives the number of c such that $\tau_{c,\sigma}$ spans the given subspace, and the last column gives the first few such primes c.

One surprising observation about Tables 3.3–3.4 is that the classes $\tau_{c,\sigma}$ appear to *not* be equidistributed in the most naive possible sense. For $q = 3$, in every single example we consider, the 0 subspace occurs about twice as much as any other subspace.

3.1 Future Projects

There are several future projects that naturally arise from the algorithm of this paper:

1. Compute the exact element $\tau_{c,\sigma}$ in the Selmer group instead of just computing it up to a fixed choice of automorphism. This could be done by normalizing the reduction maps by numerically computing $\tau_{c,\sigma}$ for one small c.

2. Do the same computations as we do here, but for abelian varieties A_f attached to newforms with $\mathrm{ord}_{s=1} L(f, s) = 2$. There is a table of such abelian varieties in [AS05]. For example, we did this for the abelian variety 1061b of dimension 2 and indeed verified the higher dimensional analogue of Kolyvagin's conjecture for this abelian variety.

3. Generalize to K with class number > 1.

4. Generalize to $q = p^n$ with $n > 1$.

5. Generalize to $q = p^n$ with $\overline{\rho}_{E,p}$ reducible and/or $p = 2$.

6. Do some computations on a curve E with a Tamagawa number divisible by q.

7. Verify Conjecture 2.8 for the rank 3 elliptic curve of conductor 5077.

8. Verify Conjecture 2.8 for the rank 4 elliptic curve of conductor 234446 given by the equation $y^2 + xy = x^3 - x^2 - 79x + 289$. The group $\mathrm{Div}(X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}})$ would then have dimension around 300000, so this computation is perhaps just possible.

Table 3.2: Data about $z_{c,\sigma,\ell}$.

E	D	q	ℓ	dim	$\max c$	$=0$	$\neq 0$	$z_{c,\ell}=0$	$z_{c,\ell}\neq 0$
389a1	-7	3	5	130	19031	152	121	17, 173, 227, 269	41, 59, 83, 587
389a1	-7	3	17	520	14657	122	92	41, 83, 173, 227	5, 59, 503, 587
389a1	-7	3	41	1300	11681	102	74	17, 83, 173, 227	5, 59, 503, 587
389a1	-7	5	19	586	28229	32	67	349, 509, 769, 2539	419, 929, 1049, 1399
389a1	-11	3	17	520	14717	116	101	29, 41, 83, 107	233, 263, 347, 479
389a1	-11	3	41	1300	14879	117	104	17, 29, 83, 107	233, 263, 347, 479
389a1	-11	5	19	586	22189	24	60	239, 569, 1759, 1999	149, 349, 359, 769
389a1	-19	3	41	1300	14699	132	98	29, 53, 107, 227	59, 113, 173, 449
389a1	-67	3	5	130	23663	170	147	41, 113, 281, 347	53, 233, 599, 653
389a1	-67	3	41	1300	15473	129	82	53, 113, 281, 587	5, 233, 347, 503
433a1	-8	5	79	2822	15199	19	30	1319, 2269, 2549, 3079	199, 389, 1039, 1669
433a1	-8	5	199	7162	11149	14	26	1319, 1879, 2269, 2549	79, 389, 1039, 1669
433a1	-11	3	17	580	12473	91	88	131, 239, 293, 359	41, 83, 107, 197
433a1	-11	3	41	1448	11579	82	84	239, 281, 293, 359	17, 83, 107, 131
433a1	-11	5	79	2822	15329	12	37	1889, 2309, 3079, 4759	409, 1289, 1319, 1669
563a1	-8	3	23	1034	14813	113	109	197, 263, 311, 383	47, 173, 191, 269
563a1	-163	3	17	752	15887	123	93	137, 293, 311, 887	23, 59, 191, 269
563a1	-163	3	23	1034	15149	114	92	137, 311, 521, 569	17, 59, 191, 269
571b1	-7	7	97	4576	12011	15	32	167, 503, 937, 1511	349, 839, 881, 1063
571b1	-7	7	167	7914	9547	16	16	97, 503, 937, 1063	349, 839, 881, 1483
571b1	-8	5	149	7056	11159	5	43	29, 1319, 2239, 7639	79, 229, 349, 359
571b1	-8	7	167	7914	12109	8	13	1063, 1861, 2141, 2309	349, 503, 839, 1511
571b1	-19	5	29	1336	15259	16	33	79, 1709, 2179, 2339	439, 829, 1229, 1319
571b1	-19	7	97	4576	13789	9	23	2309, 2953, 4157, 7349	167, 839, 1063, 1511
571b1	-19	7	167	7914	10639	9	13	97, 1063, 1861, 2141	839, 1511, 1931, 3989
571b1	-67	3	11	478	16889	129	108	239, 281, 353, 521	191, 233, 251, 311
571b1	-67	7	97	4576	12641	9	14	503, 2239, 4157, 4507	937, 1063, 1861, 2309
643a1	-8	3	29	1504	12527	104	82	47, 71, 149, 173	167, 263, 359, 431
643a1	-11	3	29	1504	12953	91	93	83, 131, 149, 197	167, 173, 263, 359
643a1	-19	3	29	1504	12143	107	86	89, 293, 509, 641	71, 113, 167, 173
643a1	-43	3	29	1504	12647	102	83	89, 131, 137, 149	71, 113, 503, 521
643a1	-67	3	11	538	14753	115	104	113, 137, 191, 251	197, 311, 353, 443
655a1	-19	3	29	1848	12149	96	77	59, 89, 113, 167	53, 179, 227, 257
681c1	-8	3	23	1672	11909	101	81	29, 47, 167, 263	191, 317, 479, 557
709a1	-7	3	5	238	16061	131	107	47, 257, 269, 419	59, 83, 227, 353
709a1	-7	3	47	2724	9833	92	56	257, 269, 419, 503	5, 59, 83, 227
709a1	-43	3	5	238	16319	131	118	149, 233, 389, 503	137, 179, 227, 257
709a1	-67	3	5	238	16301	133	109	179, 197, 233, 353	137, 239, 281, 503
709a1	-163	3	5	238	16883	138	107	233, 239, 353, 479	59, 137, 149, 257
718b1	-7	3	5	360	15137	122	100	41, 47, 131, 167	101, 251, 353, 839
997c1	-19	3	41	3328	8297	66	63	179, 227, 269, 449	113, 173, 383, 677
997c1	-67	3	41	3328	8231	76	61	179, 191, 311, 347	113, 197, 383, 647

Table 3.3: Data about normalized elements $\tau_{c,\sigma} \in \mathrm{Sel}^{(q)}(E/\mathbb{Q})$ (part 1 of 2)

E	D	q	ℓ_1	ℓ_2	$\tau_{c,\sigma}$	#	at most first 10 primes c
389a1	-7	3	5	17	$(0,0)$	87	173, 227, 269, 479, 509, 761, 797, 929, 1013, 1181
					$(0,1)$	30	503, 773, 1049, 1193, 1487, 2897, 3359, 4157, 5333, 5843
					$(1,0)$	35	41, 83, 857, 1151, 1553, 1637, 1907, 2141, 2393, 2441
					$(1,1)$	34	59, 587, 941, 1307, 1571, 1721, 2273, 2399, 3407, 3797
					$(1,2)$	27	1091, 1217, 1931, 2579, 3191, 3779, 4493, 5477, 6011, 6173
389a1	-7	3	5	41	$(0,0)$	75	17, 173, 227, 269, 479, 509, 761, 797, 929, 1013
					$(0,1)$	25	503, 773, 1049, 1193, 1487, 2897, 3359, 4157, 5333, 5843
					$(1,0)$	27	83, 857, 1151, 1553, 1637, 1907, 2141, 2393, 2441, 2477
					$(1,1)$	29	59, 587, 941, 1307, 1571, 1721, 2273, 2399, 3407, 3797
					$(1,2)$	19	1091, 1217, 1931, 2579, 3191, 3779, 4493, 5477, 6011, 6173
389a1	-67	3	5	41	$(0,0)$	95	113, 281, 587, 857, 1013, 1049, 1187, 1481, 1571, 1583
					$(0,1)$	25	347, 503, 683, 929, 1319, 1487, 2129, 2687, 3947, 4157
					$(1,0)$	34	53, 653, 1151, 1553, 1907, 2207, 2393, 2417, 2423, 3167
					$(1,1)$	26	233, 599, 1181, 1217, 1409, 2657, 3779, 4019, 5387, 5477
					$(1,2)$	30	941, 1307, 1709, 1721, 2339, 2549, 2909, 3467, 3797, 3821
433a1	-8	5	79	199	$(0,0)$	11	1319, 2269, 2549, 3079, 3319, 4349, 4759, 4799, 6949, 7879
					$(0,1)$	3	6719, 8389, 8669
					$(1,0)$	3	1879, 4549, 6679
					$(1,1)$	4	1669, 2879, 5119, 5399
					$(1,2)$	3	5839, 6029, 9949
					$(1,3)$	6	2239, 3389, 4079, 5639, 7589, 11149
					$(1,4)$	9	389, 1039, 2309, 2749, 4789, 6599, 7669, 9349, 9679
433a1	-11	3	17	41	$(0,0)$	63	239, 293, 359, 503, 563, 659, 761, 821, 1097, 1217
					$(0,1)$	21	131, 677, 1031, 1427, 1601, 1979, 2129, 2213, 3797, 4451
					$(1,0)$	19	281, 479, 857, 1019, 1949, 2207, 2309, 2609, 4421, 5147
					$(1,1)$	36	83, 107, 701, 941, 953, 1091, 1223, 1667, 1913, 2087
					$(1,2)$	26	197, 263, 431, 887, 2741, 2837, 3137, 3209, 3659, 3803
563a1	-163	3	17	23	$(0,0)$	88	137, 311, 887, 929, 953, 1217, 1223, 1367, 1583, 1733
					$(0,1)$	28	293, 983, 1433, 1553, 2213, 2843, 3923, 4397, 4691, 5927
					$(1,0)$	26	521, 569, 587, 863, 1289, 1427, 1637, 3167, 3863, 4481
					$(1,1)$	31	59, 269, 353, 509, 977, 1709, 1979, 2399, 2801, 3413
					$(1,2)$	32	191, 317, 761, 827, 1283, 1409, 1871, 3779, 3911, 4049

Table 3.4: Data about normalized elements $\tau_{c,\sigma} \in \mathrm{Sel}^{(q)}(E/\mathbb{Q})$ (part 2 of 2)

E	D	q	ℓ_1	ℓ_2	$\tau_{c,\sigma}$	#	at most first 10 primes c
571b1	-7	7	97	167	$(0,0)$	9	503, 937, 1511, 3989, 4157, 4507, 6691, 7349, 9421
					$(0,1)$	2	2239, 7489
					$(1,0)$	6	1063, 1861, 2141, 2309, 5039, 8581
					$(1,1)$	2	349, 9547
					$(1,2)$	2	5417, 6131
					$(1,3)$	4	881, 1931, 2099, 5683
					$(1,4)$	2	839, 1483
					$(1,5)$	2	3163, 6229
					$(1,6)$	2	2953, 6719
571b1	-19	7	97	167	$(0,0)$	4	2309, 2953, 4157, 7349
					$(0,1)$	1	7489
					$(1,0)$	4	1063, 1861, 2141, 8581
					$(1,1)$	2	3989, 10639
					$(1,2)$	3	5417, 6131, 9883
					$(1,3)$	2	1931, 5683
					$(1,4)$	2	839, 1511
					$(1,5)$	1	6691
					$(1,6)$	2	6719, 10331
709a1	-7	3	5	47	$(0,0)$	62	257, 269, 419, 593, 839, 857, 881, 929, 971, 1433
					$(0,1)$	17	479, 1091, 1319, 1553, 2243, 4049, 4259, 4289, 4973, 5519
					$(1,0)$	30	503, 647, 677, 1049, 1151, 1181, 1301, 1613, 1697, 2267
					$(1,1)$	16	353, 521, 563, 1097, 1427, 1637, 1949, 2579, 2621, 2687
					$(1,2)$	22	59, 83, 227, 773, 983, 1259, 2897, 2939, 3779, 4721

Table 3.5: Data about **non-scaled** elements $\tau_{c,\sigma} \in \mathrm{Sel}^{(q)}(E/\mathbb{Q})$ (part 1 of 2)

E	D	q	ℓ_1	ℓ_2	$\tau_{c,\sigma}$	#	at most first 13 primes c
389a1	-7	3	5	17	$(0,0)$	87	173, 227, 269, 479, 509, 761, 797, 929, 1013, 1181, 1319, 1511, 1601
					$(0,1)$	15	1487, 2897, 3359, 4157, 5843, 6317, 6653, 6803, 7229, 7901, 8237, 9551, 10559
					$(0,2)$	15	503, 773, 1049, 1193, 5333, 6971, 8069, 9371, 9623, 10457, 11483, 11681, 13151
					$(1,0)$	21	41, 83, 857, 1553, 1637, 2393, 2441, 2477, 3167, 4217, 6053, 6221, 7103
					$(1,1)$	16	1307, 1571, 1721, 2399, 3407, 4091, 4721, 5171, 6389, 6977, 7451, 8501, 8627
					$(1,2)$	17	1217, 3191, 3779, 5477, 6011, 6173, 6947, 8363, 8951, 9173, 9929, 11087, 11927
					$(2,0)$	14	1151, 1907, 2141, 3461, 3617, 6257, 7019, 7727, 10463, 10589, 11171, 12101, 12983
					$(2,1)$	10	1091, 1931, 2579, 4493, 8039, 10163, 10433, 13313, 13331, 14621
					$(2,2)$	18	59, 587, 941, 2273, 3797, 4457, 4751, 4973, 5309, 6569, 7817, 8111, 8123
389a1	-7	3	5	41	$(0,0)$	75	17, 173, 227, 269, 479, 509, 761, 797, 929, 1013, 1181, 1319, 1511
					$(0,1)$	13	1487, 2897, 3359, 4157, 5843, 6317, 6653, 6803, 7229, 7901, 8237, 9551, 10559
					$(0,2)$	12	503, 773, 1049, 1193, 5333, 6971, 8069, 9371, 9623, 10457, 11483, 11681
					$(1,0)$	16	83, 857, 1553, 1637, 2393, 2441, 2477, 3167, 4217, 6053, 6221, 7103, 8573
					$(1,1)$	14	1307, 1571, 1721, 2399, 3407, 4091, 4721, 5171, 6389, 6977, 7451, 8501, 8627
					$(1,2)$	12	1217, 3191, 3779, 5477, 6011, 6173, 6947, 8363, 8951, 9173, 9929, 11087
					$(2,0)$	11	1151, 1907, 2141, 3461, 3617, 6257, 7019, 7727, 10463, 10589, 11171
					$(2,1)$	7	1091, 1931, 2579, 4493, 8039, 10163, 10433
					$(2,2)$	15	59, 587, 941, 2273, 3797, 4457, 4751, 4973, 5309, 6569, 7817, 8111, 8123
389a1	-67	3	5	41	$(0,0)$	95	113, 281, 587, 857, 1013, 1049, 1187, 1481, 1571, 1583, 1811, 1889, 2531
					$(0,1)$	10	347, 503, 683, 929, 1487, 4157, 5639, 13649, 14051, 14969
					$(0,2)$	15	1319, 2129, 2687, 3947, 4583, 4673, 5867, 6551, 6653, 7109, 8807, 9371, 10259
					$(1,0)$	16	53, 1151, 1553, 2417, 2423, 3167, 3461, 5279, 5741, 7583, 8741, 8819, 9521
					$(1,1)$	13	233, 1217, 2657, 3779, 5387, 7649, 7757, 8039, 9041, 10973, 12659, 14879, 15053
					$(1,2)$	12	1721, 3467, 3821, 5171, 5231, 6143, 10331, 13613, 14033, 14321, 14669, 14717
					$(2,0)$	18	653, 1907, 2207, 2393, 3617, 4229, 4253, 4937, 5471, 6221, 7019, 7547, 7643
					$(2,1)$	18	941, 1307, 1709, 2339, 2549, 2909, 3797, 4463, 5237, 6779, 7481, 8627, 8849
					$(2,2)$	13	599, 1181, 1409, 4019, 5477, 7331, 8093, 8243, 11087, 11489, 12263, 12671, 15083
433a1	-8	5	79	199	$(0,0)$	11	1319, 2269, 2549, 3079, 3319, 4349, 4759, 4799, 6949, 7879, 11069
					$(0,1)$	1	8669
					$(0,2)$	0	
					$(0,3)$	0	
					$(0,4)$	2	6719, 8389
					$(1,0)$	2	1879, 6679
					$(1,1)$	2	1669, 5119
					$(1,2)$	1	6029
					$(1,3)$	0	
					$(1,4)$	2	389, 2749
					$(2,0)$	1	4549
					$(2,1)$	2	3389, 11149
					$(2,2)$	0	
					$(2,3)$	1	6599
					$(2,4)$	1	9949
					$(3,0)$	0	
					$(3,1)$	1	5839
					$(3,2)$	6	1039, 2309, 4789, 7669, 9349, 9679
					$(3,3)$	1	2879
					$(3,4)$	1	5639
					$(4,0)$	0	
					$(4,1)$	0	
					$(4,2)$	3	2239, 4079, 7589
					$(4,3)$	0	
					$(4,4)$	1	5399

Table 3.6: Data about **non-scaled** elements $\tau_{c,\sigma} \in \mathrm{Sel}^{(q)}(E/\mathbb{Q})$ (part 2 of 2)

E	D	q	ℓ_1	ℓ_2	$\tau_{c,\sigma}$	#	at most first 13 primes c
433a1	-11	3	17	41	$(0,0)$	63	239, 293, 359, 503, 563, 659, 761, 821, 1097, 1217, 1319, 1487, 1613
					$(0,1)$	11	131, 677, 1031, 1979, 2213, 3797, 4451, 5939, 9437, 9473, 11483
					$(0,2)$	10	1427, 1601, 2129, 4517, 5189, 5507, 5711, 5741, 9257, 10247
					$(1,0)$	13	281, 479, 857, 1949, 2207, 2309, 2609, 4421, 5147, 5297, 5519, 10067, 10691
					$(1,1)$	19	107, 701, 941, 1091, 2087, 2969, 3119, 3527, 4133, 4583, 5279, 5309, 7127
					$(1,2)$	17	197, 431, 887, 2741, 2837, 3209, 3659, 3803, 4241, 4253, 4523, 6701, 7229
					$(2,0)$	6	1019, 5231, 5639, 7211, 9467, 10457
					$(2,1)$	9	263, 3137, 6269, 6299, 7829, 8147, 8861, 9941, 10589
					$(2,2)$	17	83, 953, 1223, 1667, 1913, 2459, 2591, 3533, 4157, 6113, 6221, 6761, 7487
563a1	-163	3	17	23	$(0,0)$	88	137, 311, 887, 929, 953, 1217, 1223, 1367, 1583, 1733, 1811, 1907, 2243
					$(0,1)$	15	983, 2843, 4397, 5927, 6389, 6869, 7949, 8093, 8363, 8669, 8753, 11159, 11489
					$(0,2)$	13	293, 1433, 1553, 2213, 3923, 4691, 7673, 8273, 11069, 11243, 12569, 14699, 15149
					$(1,0)$	12	521, 587, 1637, 4583, 5507, 6449, 8429, 11969, 12161, 12959, 13649, 13907
					$(1,1)$	12	59, 353, 977, 1979, 2399, 2801, 3413, 4217, 4241, 6701, 10289, 10709
					$(1,2)$	14	191, 761, 827, 3911, 4391, 6863, 8111, 9419, 9491, 9521, 10133, 12491, 13751
					$(2,0)$	14	569, 863, 1289, 1427, 3167, 3863, 4481, 4793, 4799, 6323, 6983, 7703, 10067
					$(2,1)$	18	317, 1283, 1409, 1871, 3779, 4049, 4673, 5783, 6143, 6317, 6971, 9341, 9803
					$(2,2)$	19	269, 509, 1709, 3617, 4283, 4721, 6551, 7727, 9371, 9887, 10301, 10391, 12497
709a1	-7	3	5	47	$(0,0)$	62	257, 269, 419, 593, 839, 857, 881, 929, 971, 1433, 1487, 1511, 1571
					$(0,1)$	7	479, 1091, 4259, 5519, 6299, 6359, 7481
					$(0,2)$	10	1319, 1553, 2243, 4049, 4289, 4973, 5843, 5927, 6053, 6803
					$(1,0)$	16	647, 1049, 1151, 1181, 1697, 2957, 3449, 4283, 4637, 5879, 6047, 7187, 7229
					$(1,1)$	10	353, 563, 1097, 1427, 1637, 2621, 2687, 3191, 5897, 6221
					$(1,2)$	7	59, 227, 1259, 4721, 4919, 7829, 7937
					$(2,0)$	14	503, 677, 1301, 1613, 2267, 2693, 2903, 3491, 3671, 4217, 5393, 8627, 9467
					$(2,1)$	15	83, 773, 983, 2897, 2939, 3779, 4751, 5381, 6173, 6317, 6737, 6977, 8123
					$(2,2)$	6	521, 1949, 2579, 3659, 6011, 7649

References

[AS05] A. Agashe and W. Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484 (electronic), With an appendix by J. Cremona and B. Mazur. MR 2085902

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

[Cor] Christophe Cornut, *Mazur's conjecture on higher heegner points.*

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

[JK09] Dimitar Jetchev and Ben Kane, *Equidistribution of Heegner Points and Ternary Quadratic Forms.*

[KL89] V. A. Kolyvagin and D. Y. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Algebra i Analiz **1** (1989), no. 5, 171–196.

[Kol91] V. A. Kolyvagin, *On the structure of Shafarevich-Tate groups*, Algebraic geometry (Chicago, IL, 1989), Springer, Berlin, 1991, pp. 94–121.

[Piz80] A. Pizer, *An algorithm for computing modular forms on* $\Gamma_0(N)$, J. Algebra **64** (1980), no. 2, 340–390.

[Ste09] William Stein, *Toward a Generalization of the Gross-Zagier Conjecture*, `http://wstein.org/papers/stein-ggz/`.