Kolyvagin's Conjecture for Specific Higher Rank Elliptic Curves

William Stein*

March 26, 2011

Abstract

We study Heegner points and Kolyvagin classes for elliptic curves over $\mathbb{Q}$, with special focus on curves that have analytic rank at least 2. We reinterpret Kolyvagin's "derived classes" construction in the context of divisors on modular curves directly in characteristic ℓ, and prove compatibility and multiplicity one results. We use these results to give the first complete algorithm for explicitly computing (certain) Kolyvagin classes, and thus verify a conjecture of Kolyvagin for some specific elliptic curves.

1 Introduction

A *higher rank* elliptic curve is an elliptic curve E over $\mathbb{Q}$ of analytic rank at least 2. Let K be a quadratic imaginary field such that each prime dividing the conductor of E splits in K. This paper is about the Galois cohomology classes $\tau_{c,p^n} \in \mathrm{H}^1(K, E[p^n])$ defined by Kolyvagin (see, e.g., [Kol88a, Gro91, McC91]). Our main motivation is the explicit study of these classes on higher rank elliptic curves, inspired by the results of [Ste10, BS11] and open conjectures of Kolyvagin (see [Kol91, ÇW08]). In particular, consider Conjecture A of [Kol91, pg. 255]:

Conjecture 1.1 (Kolyvagin)**.** *For each prime p, there is some n and squarefree product $c = \prod p_i$ of primes that are inert in K with $p^n \mid \gcd(a_{p_i}, p_i + 1)$ such that $\tau_{c,p^n} \neq 0$.*

For elliptic curves with analytic rank ≤ 1 over K, this conjecture with $c = 1$ follows from [GZ86], but for higher rank curves the conjecture is wide open, and we have only computational data.

The goal of this paper is to shed some light on Conjecture 1.1 by making it more explicit and computing many examples, as follows. Let p^n and c be as in Conjecture 1.1 We adapt Kolyvagin's construction to define elements in $E(\mathbb{F}_{\ell^2}) \otimes (\mathbb{Z}/p^n\mathbb{Z})$, then give an algorithm to compute these elements in many cases. When one of these elements is nonzero, the corresponding Kolyvagin cohomology class τ_{c,p^n} is also nonzero, which allows us to verify, in several specific examples, Conjecture 1.1. This is significant because until now this conjecture had not been verified in even a single case. In particular, we present a powerful and fairly general approach to explicitly computing information about particular classes $\tau_{c,p^n} \in \mathrm{H}^1(K, A_f[p^n])$ for a modular abelian varieties A_f, squarefree integer c and prime power p^n. Thus, our results provide further motivation and much needed tools for studying Heegner points in the context of higher rank elliptic curves

*The work was supported by NSF grant 0555776 and the Clay Mathematics Institute.

and modular abelian varieties. Moreover, we provide new algorithms for computing with Selmer groups of elliptic curves, which exploit different methods than explicit n-descent for small n (see [Cre97, §3.5] and [CFO+08]) or explicit Iwasawa theory as in [SW11].

Our approach is inspired by groundbreaking work of Cornut, Vatsal, Gross, Jetchev-Kane, and Mazur (see [JK10, Cor02, Vat02]), in which they establish nontriviality results about Heegner points. Our new idea is simple: *use rational quaternion algebras to give an explicit description of the Kolyvagin derived classes construction modulo an auxiliary prime ℓ that is inert in the quadratic imaginary field K* (see Section 6). Many of the objects we use play a central role in the work of Cornut mentioned above. We hope that some of our techniques may also be useful for exploring and refining other ideas related to extra structure on higher rank elliptic curves arising from Heegner points.

The Birch and Swinnerton-Dyer conjectural rank formula (see Conjecture 3.1 below) asserts that $\mathrm{ord}_{s=1} L(E,s) = \mathrm{rank}(E(\mathbb{Q}))$. This conjecture is a theorem when E is an elliptic curve over $\mathbb{Q}$ of analytic rank ≤ 1 (see [BCDT01, GZ86, Kol88b] and Theorem 3.2 below). In sharp contrast, when E is a higher rank curve, the BSD conjecture remains shrouded in mystery, as do potential generalizations of the Gross-Zagier formula (see, e.g., [Ste10]). Unfortunately, the many exciting generalizations of the Gross-Zagier formula to other settings (see [BY09, Zha01, Zha04, YZZ11]) so far seem to yield little new insight in the higher rank case. As explained in [Ste10], Kolyvagin classes are potentially relevant to a search for a generalization of the Gross-Zagier formula that treats higher derivatives. Such a generalization is an incredibly difficult open problem and anything that might shed light on it is worth investigating. So far, finding a plausibly-provable conjecture has remained elusive.

The explicit examples in Section 8 involve rank 2 curves (instead of curves of rank ≥ 3), since the notation and computations are substantially simpler when the rank is 2. The theory and algorithms we develop apply to elliptic curves of any rank, and also to modular abelian varieties. It is thus possible to study many more general situations using our approach (see Section 9).

This paper is structured as follows. In Section 2 we give an outline of our main algorithm. Next in Section 3 we recall the BSD conjecture and give some examples, which motivate our paper. In Section 4 we recall the definition of Heegner points. In Section 5 we introduce Kolyvagin classes, make some observations, and discuss reduction of Heegner points modulo a prime over ℓ. In Section 6 we make the action of Galois on certain objects in characteristic ℓ more explicit and prove a compatibility result. In Section 7 we explain in more detail how our algorithm for computing reductions of Kolyvagin classes works. We combine our above results to obtain an algorithm to compute Kolyvagin classes, which we apply in Section 8, in which we discuss the implementation of our algorithm, tables we obtained by running it, and state some results inspired by this data. Finally, Section 9 discusses a range of related future projects.

Acknowledgement: The author would like to thank Jennifer Balakrishnan, Ralph Greenberg, Benedict Gross, Ben Howard, David Kohel, Dimitar Jetchev, Barry Mazur, Ken Ribet, Karl Rubin, Justin Walker, and Jared Weinstein for helpful discussions.

1.1 Notation and terminology

We use $\cong$ to denote a canonical isomorphism and $\approx$ to denote a noncanonical one. Unless otherwise stated, all tensor products are over $\mathbb{Z}$. We always let p, q, ℓ denote *odd* prime numbers, E an elliptic curve over $\mathbb{Q}$, and K a quadratic imaginary field such that

each prime dividing the conductor N of E splits in K. Let a_n denote the nth Dirichlet series coefficient of the L-series $L(E/\mathbb{Q}, s)$ associated to E.

2 Reducing Kolyvagin Classes

As above, let E be an elliptic curve over $\mathbb{Q}$, let K be a quadratic imaginary field such that each prime dividing the conductor N of E splits in K, let p^n be an odd prime power. Let c be a squarefree product of primes that are inert in K such that for each prime $q \mid c$ we have $p^n \mid \gcd(a_q, q+1)$, where $a_q = q + 1 - \#E(\mathbb{F}_q)$. Let K_c be the ring (not ray!) class extension of K associated to c, and let σ_i be a choice of generator of $\mathrm{Gal}(K_c/K_{c/p_i})$ for each prime divisor $p_i \mid c$, and let $\sigma = (\ldots, \sigma_i, \ldots)$. As explained in Section 5 below, Kolyvagin uses Heegner points to construct a point $P_{c,\sigma} \in E(K_c)$ such that $[P_{c,\sigma}] \in (E(K_c) \otimes \mathbb{Z}/p^n\mathbb{Z})^{\mathrm{Gal}(K_c/K)}$. Under suitable hypothesis on p (e.g., the p-adic representation $\rho_{E,p}$ is surjective), Kolyvagin then uses $P_{c,\sigma}$ to define a cohomology class $\tau_{c,p^n} \in \mathrm{H}^1(K, E[p^n])$ characterized by

$$\delta([P_{c,\sigma}]) = \mathrm{res}_{K,K_c}(\tau_{c,p^n}) \in H^1(K_c, E[p^n])^{\mathrm{Gal}(K_c/K)},$$

where δ is the connecting homomorphism of Galois cohomology. (The class τ_{c,p^n} also depends on the choice of σ, but we surpress this in our notation.)

We introduce yet another prime ℓ that is also inert in K and fix a prime λ of K_c over ℓ. Reduction modulo λ induces a homomorphism $E(K_c) \otimes \mathbb{Z}/p^n\mathbb{Z} \to E(\mathbb{F}_{\ell^2}) \otimes \mathbb{Z}/p^n\mathbb{Z}$. Using Algorithm 2.1 below when $n = 1$, we compute the image z of $[P_{c,\sigma}]$ under the reduction map. When $z \neq 0$, we conclude that $\tau_{c,p}$ is also nonzero.

Algorithm 2.1.

- INPUT: *E, K, p, ℓ, c, σ, as above.*
- OUTPUT: *The (well-defined) image of $[P_{c,\sigma}]$ in $E(\mathbb{F}_{\ell^2}) \otimes (\mathbb{Z}/p\mathbb{Z})$, via reduction modulo any prime over ℓ (it does not matter which), up to some fixed nonzero scalar that is independent of c. We can compute the image of many different $P_{c,\sigma}$ with respect to a consistent choice of map.*

1. Use rational quaternion algebras and theta series of quadratic forms to directly compute a supersingular point $\overline{x}_1 \in X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}}$ that is the reduction modulo λ of a choice of Heegner point $x_1 \in X_0(N)(K_1)$. (See Section 7.1.)

2. Apply a mod ℓ analogue of Kolyvagin's construction to directly obtain the reduction $\overline{Q}_{c,\sigma}$ of the "Kolyvagin derived divisor" attached to x_c as an element of $\mathrm{Div}(X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}})$. (See Sections 6 and 7.2.) Computing $\overline{Q}_{c,\sigma}$ closely resembles computing the image $T_c(\overline{x}_1)$ of $\overline{x}_1$ under the Hecke operator T_c using Equation (6.1), but with an appropriate choice of weighting of each summand.

3. Use linear algebra combined with refinements of results of Cornut, Ihara and Ribet (see Section 7.4) and a multiplicity one theorem (see Theorem 7.14 below) to compute a fixed nonzero scalar multiple of the image of $\overline{Q}_{c,\sigma}$, hence of $P_{c,\sigma}$, under the homomorphism of Hecke modules

$$\mathrm{Div}(X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}}) \otimes (\mathbb{Z}/p\mathbb{Z}) \to E(\mathbb{F}_{\ell^2}) \otimes (\mathbb{Z}/p\mathbb{Z}). \tag{2.1}$$

Remark 2.2. We emphasize that the steps of Algorithm 2.1 can all be done purely algebraically, without recourse to any numerical approximations. This contrasts with the approach of [JLS09], which provides numerical *evidence* for Kolyvagin's conjecture in one case, *without* proof. In theory the approach of [JLS09] can likely be made rigorous, but this has not been done in practice in any case, though see [Bra10] which is a step in that direction. The approach of [JLS09] can be faster for an elliptic curve with large conductor (with c *very small*); it is much worse for large c than Algorithm 2.1 (e.g., $c > 100$ would be incredibly hard).

Remark 2.3. Suppose we are only interested in verifying that the image under (2.1) of $\overline{Q}_{c,\sigma}$ is *nonzero*. Instead of the linear algebra of Step 3, we might be able to use that (2.1) is a $\mathbb{T}$-module homomorphism, where $\mathbb{T}$ is the Hecke algebra; if $\mathbb{T}\overline{Q}_{c,\sigma}$ has sufficiently large dimension, so that it cannot be contained in the nontrivial kernel, then we are done. If we take this approach and it works, we do not need to compute (2.1) at all. However, in some cases this approach cannot work, e.g., we could run into trouble if there are other elliptic curves of larger rank also of level N.

Remark 2.4. Algorithm 2.1 only computes the reduction of $P_{c,\sigma}$ up to a fixed nonzero scalar, which is enough to show that $\delta(P_{c,\sigma}) \neq 0$. The point $P_{c,\sigma}$ could in principle be normalized by finding $P_{c,\sigma}$ exactly via a numerical computation, using [JLS09] for one choice of c for which the image of $P_{c,\sigma}$ in $E(\mathbb{F}_\ell) \otimes (\mathbb{Z}/p\mathbb{Z})$ is nonzero.

To make the steps of Algorithm 2.1 explicit and machine computable, we view $\mathrm{Div}(X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}})$ noncanonically as the set of right ideal classes in an Eichler order R of level N in the (unique up to isomorphism) rational quaternion algebra ramified at ℓ and ∞, which we compute as explained in [Piz80, Koh01, Koh97, Ste09]. By computing representation numbers of ternary quadratic forms associated to left orders, we find the right R-ideals I whose left order admits an optimal embedding of the ring of integers $\mathcal{O}_K$ of K; this is the trick we use to compute the reduction $\overline{x}_1 \in X_0(N)(\mathbb{F}_{\ell^2})$ of x_1 modulo a prime over ℓ without ever computing x_1 itself. Then we use $\overline{x}_1$ and a parametrization of the right ideals $J \subset I$ such that $I/J \cong (\mathbb{Z}/c\mathbb{Z})^2$ to directly compute the reduction $\overline{Q}_{c,\sigma}$ (see Theorem 7.8 below). An implementation of the algorithm is included in Sage [S$^+$11].

3 The Birch and Swinnerton-Dyer Conjecture

The BSD conjecture is the main motivation for this paper, so we spend a page recalling it and emphasizing our ignorance. First we state the conjecture, then state the main theorem about it, and finish with some remarks about a curve of rank 4 and another of rank 2.

Let E be an elliptic curve over $\mathbb{Q}$. By [BCDT01, Wil95] the L-series

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

attached to E extends to a holomorphic function on all of $\mathbb{C}$, hence the nonnegative integer

$$r_{\mathrm{an}}(E/\mathbb{Q}) = \mathrm{ord}_{s=1} L(E, s) \geq 0$$

is defined. The BSD conjecture was first introduced by Birch and Swinnerton-Dyer in the 1960s motivated by computer computations, and was later formulated for abelian varieties over number fields (see [Bir65, Bir71, Mil72, Tat66, Wil00]).

Conjecture 3.1 (Birch and Swinnerton-Dyer)**.** *For any elliptic curve E defined over $\mathbb{Q}$ we have*

$$\operatorname{rank} E(\mathbb{Q}) = r_{\mathrm{an}}(E/\mathbb{Q}).$$

There is also a conjectural formula of Birch and Swinnerton-Dyer for the leading coefficient of the series expansion of $L(E,s)$ about $s=1$ (see [Lan91, III, §5] for a general formulation). This formula has now been computationally verified in many cases; see [GJP+09, Mil10] where the formula is fully proved for all curves with rank ≤ 1 and conductor ≤ 5000.

Results of Kolyvagin, Gross-Zagier, and Bump-Friedberg-Hoffstein (see, e.g., [BFH90, GZ86, Kol88b]) imply the following theorem.

Theorem 3.2. *Conjecture 3.1 is true for elliptic curves E with $\operatorname{ord}_{s=1} L(E,s) \leq 1$.*

As mentioned in the introduction, Conjecture 3.1 remains completely open when $\operatorname{ord}_{s=1} L(E,s) \geq 2$. As evidence for Conjecture 3.1, we have tables of specific rank 2 and 3 curves for which the conjecture is known (see, e.g., [Crea, SW02]), and assurances that many curves have analytic rank ≤ 1 (see [BS10]). There is not a single example of a curve of rank ≥ 4 for which the conjecture has been verified. Rank 4 is difficult not because of the complexity of doing computations, but because there is, as of now, no known *algorithm* (no matter how slow) that can be used to show that $r_{\mathrm{an}}(E/\mathbb{Q}) \geq 4$.

Example 3.3. Let E be the elliptic curve $y^2 + xy = x^3 - x^2 - 79x + 289$. A 2-descent (using [Creb, S+11]) and point search proves that E has algebraic rank 4, with generators $(-9,19), (-8,23), (-7,25), (4,-7)$. Applying the methods of [Cre97, Dok04] and the Gross-Zagier formula, we see that $L(E,1) = L'(E,1) = 0$, $L''(E,1)$ is *very close* to 0, and $L^{(4)}(E,1) = 214.65233\ldots$. But showing that $L''(E,1) = 0$ (which would imply Conjecture 3.1 for E) is an unsolved problem.

Assume that E is an elliptic curve with $\operatorname{ord}_{s=1} L(E,s) = 2$. Then Conjecture 3.1 asserts that $\operatorname{rank} E(\mathbb{Q}) = 2$. In the explicit examples Section 8, the Birch and Swinnerton-Dyer formula predicts that $\#Ш(E/\mathbb{Q}) = 1$, though in fact $Ш(E/\mathbb{Q})$ is not known to be finite for any of these curves (or indeed, for any curve of rank ≥ 2). The best that has been done at present for a general rank 2 curve is to verify that $Ш(E/\mathbb{Q})[p] = 0$ for (finitely) many specific p, e.g., using the algorithm of [SW11]. See the recent work of [CLS09, CLS10] on CM elliptic curves of rank 2. Also, for the rank 2 elliptic curve of conductor 389, the author used modular symbols, p-adic L-series, p-adic heights, Iwasawa theory, and results of Kato and Schneider to show that $Ш(E/\mathbb{Q})[p] = 0$ for all primes $p < 2466$, except possibly the supersingular primes $p = 107$, 599, and 1049, for which the approach of [SW11] should work, but take much longer.

4 Quadratic Imaginary Fields and Heegner Points

In this section we recall the definition of Heegner points over ring class fields, and explain how they behave under taking traces. We will use these points in the next section to construct derived Galois equivariant classes.

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N, and let $\pi_E : X_0(N) \to E$ be a fixed choice of minimal modular parametrization. The main theorem of [BFH90] implies that there exists infinitely many quadratic imaginary fields $K = \mathbb{Q}(\sqrt{D})$ of discriminant $D \leq -5$ such that each prime dividing N splits in K. Fix any such K.

Fix an odd prime power p^n with $n \geq 1$. Let $c = \prod p_i$ be any product of prime numbers p_i that are each inert in K, coprime to ND, and such that

$$p^n \mid \gcd(a_{p_i}, p_i + 1),$$

for each i. Let K_c be the ring class field associated to the conductor c. As explained in [Gro91, pg. 238], the field K_c is an abelian extension of the Hilbert class field K_1 of K, is unramified outside c, and is contained in the ray class field associated to c. Moreover, the reciprocity map of class field theory induces a canonical isomorphism

$$\mathrm{Gal}(K_c/K_1) \cong (\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times, \tag{4.1}$$

where $\mathcal{O}_K$ is the ring of integer of K (see Proposition 6.2 below). Let $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ be the order in $\mathcal{O}_K$ of conductor c. Each prime dividing N splits in K, so we can fix a *choice* $\mathfrak{n}$ of ideal in $\mathcal{O}_K$ with $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$.

The Heegner point associated to c is

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

which has image

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

Remark 4.1. There are many possible choices of $\mathfrak{n}$ in the definition above, which are parametrized by the different choices of prime ideals of $\mathcal{O}_K$ over the prime divisors of N. These different choices are permuted by the action of the Atkin-Lehner operators. The Atkin-Lehner operators act as ± 1 on E, so y_c is well-defined up to sign, independent of the choice of $\mathfrak{n}$. See [Wat06] or [Coh07, Thm. 8.7.7] for an explicit description of the Atkin-Lehner action on Heegner points.

Motivated by the problem of constructing elements of $E(\mathbb{Q})$, it is natural to apply a trace map to y_c.

Proposition 4.2 (The Distribution Relation)**.** *We have* $\mathrm{Tr}_{K_c/K_1}(y_c) = a_c \cdot y_1 \in E(K_1)$. *More generally for each prime* $q \mid c$*, we have* $\mathrm{Tr}_{K_c/K_{c/q}}(y_c) = a_q \cdot y_{c/q} \in E(K_{c/q})$.

Proof. See [Gro84, §6] or [JK10, Lem. 5.2]. The key idea is that if T_c is the cth Hecke operator, then we have the following equality of divisors on $X_0(N)$:

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

To complete the proof, take the image of both sides in E and use that the Hecke operator T_c acts as a_c on E. □

Suppose E is a higher rank curve. The Gross-Zagier theorem [GZ86, §5.2] implies that the height of $\mathrm{Tr}_{K_1/K}(y_1) \in E(K)$ is a nonzero multiple of $L'(E/K, 1)$. However, $L(E/K, s) = L(E/\mathbb{Q}, s) \cdot L(E^D/\mathbb{Q}, s)$, and we assumed that $\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) \geq 2$, so $L'(E/K, 1) = 0$. Thus for all c,

$$\mathrm{Tr}_{K_c/K}(y_c) = \mathrm{Tr}_{K_1/K}(a_c y_1) \in E(K)_{\mathrm{tor}}. \tag{4.2}$$

Thus the traces of y_c are never non-torsion elements of the higher rank Mordell-group $E(\mathbb{Q})$.

5 Derived Points and Cohomology Classes, and their Reduction Modulo ℓ

In this section, we assume that p is an odd prime such that the p-adic representation $\rho_{E,p}$ is surjective.

In Section 5.1 we construct Kolyvagin's derived classes associated to Heegner points, then use these in Section 5.2 to construct Galois invariant classes. In Section 5.3 we explain how to reduce these classes modulo ℓ, and note that if the reduction is ever nonzero, then so is the class. Section 5.4 contains some consequences of nontriviality in the special case when E has analytic rank 2.

5.1 Derived points

Let p^n be a power of p, and let $c = p_1 \cdots p_t$ be a squarefree product of inert primes p_i such that $p^n \mid \gcd(a_{p_i}, p_i + 1)$. We recall the construction of Kolyvagin classes here, since it is important to emphasize the precise dependence on choice of generator of the Galois group, which impacts our algorithm. Also, we will make some remarks about this construction that appear to not be in the literature.

Let $[y_c]$ denote the image of y_c in $E(K_c) \otimes (\mathbb{Z}/p^n\mathbb{Z})$. Let q be a prime divisor of c. The Galois group $\mathrm{Gal}(K_c/K_{c/q})$ is cyclic of order $q+1$. Fix a choice of generator $\sigma = \sigma_q \in \mathrm{Gal}(K_c/K_{c/q})$, let

$$P = \sum_{i=1}^{q} i\sigma^i(y_c) \in E(K_c),$$

and let $[P]$ denote the image of P in $E(K_c) \otimes (\mathbb{Z}/p^n\mathbb{Z})$, so

$$[P] = \sum_{i \in \mathbb{Z}/(q+1)\mathbb{Z}} i\sigma^i([y_c]). \tag{5.1}$$

Proposition 5.1. *As above, assume that $p^n \mid \gcd(a_q, q+1)$. Then*

$$[P] \in (E(K_c) \otimes (\mathbb{Z}/p^n\mathbb{Z}))^{\mathrm{Gal}(K_c/K_{c/q})}.$$

Proof. Applying our choice of generator σ of $\mathrm{Gal}(K_c/K_{c/q})$ to P, we have

$$\sigma([P]) = \sum_{i \in \mathbb{Z}/(c+1)\mathbb{Z}} \sigma i\sigma^i([y_c]) = \sum_{i \in \mathbb{Z}/(c+1)\mathbb{Z}} i\sigma^{i+1}([y_c]) \tag{5.2}$$

$$= \sum_{i \in \mathbb{Z}/(c+1)\mathbb{Z}} (i-1)\sigma^i([y_c]) = [P] - \mathrm{Tr}_{K_c/K_{c/q}}([y_c]) = [P]. \tag{5.3}$$

The first equality in (5.3) is because $p^n \mid q+1$, so we can enumerate the elements of $\mathbb{Z}/(q+1)\mathbb{Z}$ in any way we want (in fact, the notation we are using above only makes sense because $p^n \mid q+1$). The final equality in (5.3) holds since $p^n \mid a_q$ and $\mathrm{Tr}_{K_c/K_{c/q}}(y_c) = a_q y_{c/q}$, by Proposition 4.2. □

For each prime $p_i \mid c$, make a choice σ_i of generator for $\mathrm{Gal}(K_c/K_{c/p_i})$, and let $\sigma = (\sigma_1, \ldots, \sigma_t)$ be the tuple of those choices. Let

$$D_{c,\sigma} = \prod_{j=1}^{t} \sum_{i=1}^{p_j} i\sigma_j^i \in \mathbb{Z}[\mathrm{Gal}(K_c/K_1)],$$

and let

$$[P_{c,\sigma}] = \mathrm{Tr}_{K_1/K}(D_{c,\sigma}([y_c])) \in (E(K_c) \otimes (\mathbb{Z}/p^n\mathbb{Z}))^{\mathrm{Gal}(K_c/K)}. \tag{5.4}$$

Remark 5.2. If we replace the hypothesis that $p^n \mid \gcd(a_q, q+1)$ with the hypothesis that $p^n \mid q+1$ and E has analytic rank ≥ 2, then we still have that $[P_{c,\sigma}] \in (E(K_c) \otimes (\mathbb{Z}/p^n\mathbb{Z}))^{\mathrm{Gal}(K_c/K)}$. This is because $\mathrm{Tr}_{K_1/K}(y_1)$ is torsion and p is coprime to torsion, so the proof of Proposition 5.1 still goes through, but with an "obstruction" of $a_c y_1$, which vanishes upon taking a trace because of Equation (4.2).

Remark 5.3. The construction also generalizes if we replace the prime power p^n by the ideal I in $\mathbb{Z}$ generated by all a_q and $q+1$ for primes $q \mid c$, and we obtain

$$[P_{c,\sigma}] \in (E(K_c) \otimes (\mathbb{Z}/I))^{\mathrm{Gal}(K_c/K)}.$$

More generally, consider the modular Jacobian $J = J_0(N)$, and let I be the ideal of the Hecke algebra $\mathbb{T}$ generated by all T_q and $q+1$, for prime $q \mid c$. Then the above construction with x_c (instead of y_c) defines a class

$$[R_{c,\sigma}] = \mathrm{Tr}_{K_1/K}(D_{c,\sigma}([x_c])) \in (J(K_c) \otimes_{\mathbb{T}} (\mathbb{T}/I))^{\mathrm{Gal}(K_c/K)}$$

that maps to $[P_{c,\sigma}]$ under the natural map.

The next lemma explains how replacing σ_i by a different generator of $\mathrm{Gal}(K_c/K_{c/p_i})$ changes $[P_{c,\sigma}]$ by multiplication by an element of $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Lemma 5.4. *For every $j \in (\mathbb{Z}/(p_i+1)\mathbb{Z})^\times$, we have $[P_{c,(\ldots,\sigma_i^j,\ldots)}] = \frac{1}{j}[P_{c,\sigma}]$.*

Proof. Writing $q = p_i$ and $s = \sigma_i$, we have in $(\mathbb{Z}/(q+1)\mathbb{Z})[\mathrm{Gal}(K_c/K)]$ that

$$\sum_{i \,\in\, \mathbb{Z}/(q+1)\mathbb{Z}} i s^{ji} = \sum_{i \,\in\, \mathbb{Z}/(q+1)\mathbb{Z}} \frac{i}{j} s^i = \frac{1}{j} \cdot \sum_{i \,\in\, \mathbb{Z}/(q+1)\mathbb{Z}} i s^i.$$

□

Lemma 5.5. *If E has analytic rank r over $\mathbb{Q}$ and c is a product of t primes, then $\tau([P_{c,\sigma}]) = (-1)^{r+t+1}[P_{c,\sigma}]$. In particular, if $r+t$ is odd, then*

$$[P_{c,\sigma}] \in (E(K_c) \otimes (\mathbb{Z}/p^n\mathbb{Z}))^{\mathrm{Gal}(K_c/\mathbb{Q})}.$$

Proof. This is just [Gro91, Prop. 5.4(1)], which is proved by noting ([Gro91, Prop. 5.3]) 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 and we have that $\tau(y_c) = (-1)^{r+1}\sigma'(y_c) + (\text{torsion})$ for some $\sigma' \in \mathrm{Gal}(K_c/K)$. Thus $\tau([y_c]) = (-1)^{r+1}\sigma'([y_c])$, since p is coprime to any torsion. When $c = p_1 \cdots p_t$ is a product of t distinct primes, we have (using Lemma 5.4) that $\tau([P_{c,\sigma}]) = (-1)^{r+1}(-1)^t[P_{c,\sigma}]$. □

Remark 5.6. Following [How04, §1.2], we could alternatively encode the dependence on the choice of σ in a tensor product. Suppose for simplicity that c is prime. Consider the element

$$\sigma \otimes [P_{c,\sigma}] \in \mathrm{Gal}(K_c/K_1) \otimes (E(K_c) \otimes (\mathbb{Z}/p^n\mathbb{Z}))^{\mathrm{Gal}(K_c/K)}.$$

This element does not depend on the choice of generator σ because for any $j \in (\mathbb{Z}/(c+1)\mathbb{Z})^\times$, if we define the element instead using the generator σ^j, by Lemma 5.4, we obtain

$$\sigma^j \otimes [P_{c,\sigma^j}] = \sigma^j \otimes \frac{1}{j}[P_{c,\sigma}] = (\sigma^j)^{1/j} \otimes [P_{c,\sigma}] = \sigma \otimes [P_{c,\sigma}],$$

where by $1/j$ we mean that element $j' \in \mathbb{Z}/p^n\mathbb{Z}$ such that $j'j = 1$. This generalizes to composite c by replacing $\mathrm{Gal}(K_c/K_1)$ by the tensor product $\bigotimes_{p_i \mid c} \mathrm{Gal}(K_c/K_{c/p_i})$.

Remark 5.7. We can define $[P_{c,\sigma}]$ without the hypothesis that each σ_i is a generator of $\mathrm{Gal}(K_c/K_{c/p_i})$. If we try to use exactly the definition given above, then the resulting $[P_{c,\sigma}]$ need not be $\mathrm{Gal}(K_c/K)$-equivariant, so we must modify the definition slightly. Let K' be the biggest subfield of K_c that is fixed by all σ_i, and let k_i (which divides p_i+1) be the order of σ_i. Let $[P] = \prod_{i=1}^{t} \sum_{j=1}^{k_i} j\sigma_i^j(y_c)$. Then the same argument as in Proposition 5.1 shows that $[P] \in (E(K_c) \otimes (\mathbb{Z}/p^n\mathbb{Z}))^{\mathrm{Gal}(K_c/K')}$, and we let

$$[P_{c,\sigma}] = \mathrm{Tr}_{K'/K}([P]) \in (E(K_c) \otimes (\mathbb{Z}/p^n\mathbb{Z}))^{\mathrm{Gal}(K_c/K)}.$$

For example, if $c \neq 1$ and all $\sigma_i = 1$, then $[P_{c,\sigma}] = [a_c \cdot y_K] = 0$, since $p^n \mid a_c$.

For any multiple k of p^n, we have the following identity of polynomials:

$$\sum_{j=1}^{k-1} jX^j = \sum_{i=0}^{\frac{k}{p^n}-1} X^{p^n \cdot i} \cdot \left(\sum_{j=1}^{p^n-1} jX^j \right) \in (\mathbb{Z}/p^n\mathbb{Z})[X]. \tag{5.5}$$

Thus in the above construction, if we choose each σ_i to be of order exactly p^n, then we get (up to scaling by a unit) the same element $[P_{c,\sigma}]$ as if each σ_i is a generator of $\mathrm{Gal}(K_c/K_{c/p_i})$. The factorization (5.5) thus means we can alternatively view the Kolyvagin derived point construction as follows. Let K_c' be the compositum of the degree p^n subfields of each K_{p_i} for the primes $p_i \mid c$. If

$$D = \prod_{p_i \mid c} \sum_{j=1}^{p^n-1} j\sigma_i^j \in \mathbb{Z}[\mathrm{Gal}(K_c'/K_1)],$$

then

$$[P_{c,\sigma}] = \mathrm{Tr}_{K_1/K}([D(\mathrm{Tr}_{K_c/K_c'}(y_c))]).$$

5.2 Derived cohomology classes

As explained in [Gro91, §4], under our hypothesis that $\rho_{E,p}$ is surjective, the map

$$\mathrm{H}^1(K, E[p^n]) \to \mathrm{H}^1(K_c, E[p^n])^{\mathrm{Gal}(K_c/K)}$$

is an isomorphism, so $[P_{c,\sigma}]$ uniquely determines a cohomology class

$$\tau_{c,p^n} \in \mathrm{H}^1(K, E[p^n]).$$

In the rest of this short section, we make an additional observation in the special case when $r_{\mathrm{an}}(E/\mathbb{Q}) = 2$ and c is prime, since this is the situation for our data in Section 8.

Let $\mathrm{res} : \mathrm{H}^1(\mathbb{Q}, E[p^n]) \to \mathrm{H}^1(K_c, E[p^n])$ be the restriction map and δ the connecting homomorphism. Restricting res to Selmer groups, we obtain a commutative diagram:

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

The following proposition *defines* an element τ_{c,p^n} in the Selmer group $\mathrm{Sel}^{(p^n)}(E/\mathbb{Q})$, not just in $\mathrm{H}^1(K, E[p^n])$ as above.

Proposition 5.8. *If c is prime and $r_{\mathrm{an}}(E/\mathbb{Q}) = 2$, then $\tau_{c,p^n} \in \mathrm{Sel}^{(p^n)}(E/\mathbb{Q})$.*

Proof. Since $r_{\mathrm{an}}(E/\mathbb{Q})$ is even and c is prime, Lemma 5.5 implies that $\delta([P_{c,\sigma}]) \in \mathrm{H}^1(K_c, E[p^n])^{\mathrm{Gal}(K_c/\mathbb{Q})}$. That the image of τ_{c,p^n} in $\mathrm{H}^1(\mathbb{Q}, E)[p^n]$ is locally trivially (hence in $\mathrm{Sel}^{(p^n)}(E/\mathbb{Q})$) follows from [Gro91, Prop. 6.2] with $n = c$ and $m = 1$, since $L'(E/K, 1) = 0$ hence y_K is torsion. □

5.3 Reduction modulo ℓ

The following lemma will be helpful when reducing the computation of τ_{c,p^n} to linear algebra (see Section 7.4). Below we will consider $M = E(\mathbb{F}_{\ell^2}) \otimes (\mathbb{Z}/p^n\mathbb{Z})$ as a module for the action of the nontrivial element $\mathrm{Frob}_\ell \in \mathrm{Gal}(\mathbb{F}_{\ell^2}/\mathbb{F}_\ell)$; we write M^- for the eigenspace of M on which Frob_ℓ acts by -1.

Lemma 5.9. *Let $p^n > 1$ be an odd prime power and let ℓ be a prime such that $p^n \mid \gcd(a_\ell, \ell + 1)$. Then the groups $E(\mathbb{F}_\ell) \otimes (\mathbb{Z}/p^n\mathbb{Z})$ and $(E(\mathbb{F}_{\ell^2}) \otimes (\mathbb{Z}/p^n\mathbb{Z}))^-$ are each cyclic of order p^n.*

Proof. (See [Ste10, Lem. 5.1].) We have

$$p^n \mid \gcd(a_\ell, \ell + 1) \mid \ell + 1 - a_\ell = \#E(\mathbb{F}_\ell).$$

If $E(\mathbb{F}_\ell)[p]$ is noncyclic, then nondegeneracy of the Weil pairing implies that $\mu_p \subset \mathbb{F}_\ell^\times$, so $p \mid \ell - 1$, hence $p \mid \gcd(\ell - 1, \ell + 1) = 2$, which contradicts that p is odd. Thus $E(\mathbb{F}_\ell)[p]$ is cyclic, so the p-primary part of $E(\mathbb{F}_\ell)$ is cyclic of order divisible by p^n. For the second group, apply the above argument to the quadratic twist of E with trace of Frobenius $-a_\ell$, and note that p^n also divides $\gcd(-a_\ell, \ell + 1)$. □

For any prime $\ell \nmid c$ that is inert in K, let λ be a prime ideal over ℓ in the ring of integers of the ring class field K_c. Define

$$z_{c,\sigma,\ell} \;=\; [P_{c,\sigma}] \pmod{\lambda} \in E(\mathbb{F}_{\ell^2}) \otimes (\mathbb{Z}/p^n\mathbb{Z}), \tag{5.6}$$

which is well defined, independent of the choice of λ. See [Ste10, Prop. 5.4] for the proof that $z_{c,\sigma,\ell}$ is well defined; the reason is that changing λ corresponds to acting on $[P_{c,\sigma}]$ by an automorphism, which does nothing since $[P_{c,\sigma}]$ is $\mathrm{Gal}(K_c/K)$-equivariant. Also, note that by Lemma 5.5, if $r_{\mathrm{an}}(E/\mathbb{Q}) + t$ is odd, then $z_{c,\sigma,\ell} \in E(\mathbb{F}_\ell) \otimes (\mathbb{Z}/p^n\mathbb{Z})$; if it is even, then $z_{c,\sigma,\ell} \in (E(\mathbb{F}_{\ell^2}) \otimes (\mathbb{Z}/p^n\mathbb{Z}))^-$, where the $-$ is for the action of the involution Frob_ℓ.

5.4 Consequences of nontriviality of the elements

We continue with the same notation and running assumptions as above. The first lemma below links verifying that $z_{c,\sigma,\ell} \neq 0$ to verifying Kolyvagin's Conjecture A [Kol91, pg. 255] (see Conjecture 1.1 above).

Lemma 5.10. *Suppose c is a squarefree product of inert primes q with $p^n \mid \gcd(a_q, q+1)$. If $z_{c,\sigma,\ell} \neq 0$, then $\tau_{c,p^n} \neq 0$.*

Proof. The nonzero element $z_{c,\sigma,\ell}$ is the image of $[P_{c,\sigma}]$ under the homomorphism

$$E(K_c) \otimes (\mathbb{Z}/p^n\mathbb{Z}) \longrightarrow E(\mathbb{F}_{\ell^2}) \otimes (\mathbb{Z}/p^n\mathbb{Z})$$

induced by reduction modulo a choice of prime ideal λ over ℓ. Thus if $z_{c,\sigma,\ell} \neq 0$, then $[P_{c,\sigma}] \neq 0$, so $\tau_{c,p^n} = \delta([P_{c,\sigma}]) \neq 0$, since δ is injective. □

Theorem 5.11. *Suppose $r_{\mathrm{an}}(E/\mathbb{Q}) = 2$ and that there exists inert primes c, ℓ (as above) such that $z_{c,\sigma,\ell} \neq 0$. Then*

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

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

Proof. If $z_{c,\sigma,\ell} \neq 0$ then by Lemma 5.10, the Kolyvagin cohomology class $\tau_{c,p} \in \mathrm{H}^1(K, E[p])$ is nonzero, so Kolyvagin's Conjecture A [Kol91, pg. 255] is true. The desired conclusion then follows from [Ste10, Thm 4.2] (which is mainly a restatement of the main theorem of [Kol91]). □

For example, suppose E is a curve with $r_{\mathrm{an}}(E) = \operatorname{rank}(E(\mathbb{Q})) = 2$, that $Ш(E/\mathbb{Q})[2] = 0$ and that $\rho_{E,p}$ is surjective for all odd primes p. If we could somehow prove that for every prime p, there is a c with $z_{c,\sigma,\ell} \neq 0$, then Theorem 5.11 would imply that $Ш(E/\mathbb{Q}) = 0$. This would be an extremely deep result, since at present it is an open problem to prove unconditionally that the set of all pairs

$$\{(E, p) : Ш(E/\mathbb{Q})(p) \text{ is finite and } \operatorname{rank}(E) \geq 2\}$$

is infinite!

6 The Action of Galois and Reduction of Heegner Points Modulo ℓ

In this section, we prove a result (Theorem 6.6) that is crucial to giving a variant of Kolyvagin's derived points construction directly in characteristic ℓ, which is the main input to Algorithm 2.1. Note that the results in this section are on the level of the modular curve $X_0(N)$, and make no reference to a specific choice of elliptic curve over $\mathbb{Q}$ of conductor N, so they are equally useful in studying modular abelian varieties.

Theorem 6.6 below asserts that there is a compatible action of $\mathrm{Gal}(K_c/K_1)$ on two objects. Everything in the current paragraph will be made precise in Section 6.1 below. Let N be a positive integer and K a quadratic imaginary field such that each prime dividing N splits in K. Fix a choice of Heegner point $x_1 \in X_0(N)(K_1)$. For any square-free product c of primes that are inert in K, consider the support S of the divisor $T_c(x_1) \in \mathrm{Div}(X_0(N))$, where T_c is the cth Hecke operator. The Galois group $\mathrm{Gal}(K_c/K_1)$ acts transitively on S. Fix an inert prime $\ell \nmid c$ and a choice of prime λ of $\overline{\mathbb{Z}}$ over ℓ. Let $\mathbf{E}_1$ be the reduction mod λ of the enhanced elliptic curve corresponding to x_1, and consider the Eichler order $R = \mathrm{End}(\mathbf{E}_1)$. Also, as explained in Proposition 6.2, use class field theory to identify $\mathrm{Gal}(K_c/K_1)$ with $(\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times$. For $x \in S$, represent $x \pmod{\lambda}$ by a right ideal class in R. Then Theorem 6.6 below asserts that *the action of* $\mathrm{Gal}(K_c/K_1)$ *on S is compatible with the action of* $(\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times$ *on the set of right ideals of R/cR of index c^2*. This result is somewhat complicated to state and prove, but we are amply compensated with an alternative interpretation of Kolyvagin's derived points construction.

In Section 6.1 we state our main result, then in Section 6.2 we prove it by deriving certain transformation rules for right ideals. We emphasize that in the arguments below, c is an arbitrary squarefree product of inert primes, and K is allowed to have arbitrary class number.

Remark 6.1. Reduction and the Galois action is also considered in [Cor02, §3.3], but via an adelic formulation that is less explicit and amenable to computation.

6.1 Notation and statement of theorem

In Section 6.1.1 we explain how Galois and Hecke operators act on higher Heegner points. In order to see the reduction of these points modulo ℓ, in Section 6.1.2 we introduce enhanced supersingular elliptic curves, and describe how they relate to points on modular curves. In Section 6.1.3, we explain how the Hecke operators act on divisors on enhanced curves, which will be used later in the proof of our main theorem. Finally, in Section 6.1.4 we precisely state the main theorem of this section, which is critical in reinterpreting Kolyvagin's derived classes operator in characteristic ℓ.

6.1.1 Galois and Hecke actions on Heegner points

Let N, K, c, and K_c be as above, and let $D = \mathrm{disc}(\mathcal{O}_K)$. Let $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ be the order of conductor c. Let $\mathfrak{n}$ be a choice of ideal in $\mathcal{O}_K$ with $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$, and let $\mathfrak{n}_c = \mathfrak{n} \cap \mathcal{O}_c$. As in [Gro84], for any order $\mathcal{O}$ (of conductor coprime to N) and any fractional $\mathcal{O}$-ideals $\mathfrak{m}$ and $\mathfrak{a}$, let $(\mathcal{O}, \mathfrak{m}, [\mathfrak{a}])$ denote the Heegner point $(\mathbb{C}/\mathfrak{a}, \mathfrak{m}^{-1}\mathfrak{a}/\mathfrak{a}) \in X_0(N)$, with endomorphism ring the order $\mathcal{O}$. In particular, let

$$x_c = (\mathcal{O}_c, \mathfrak{n}_c, [\mathcal{O}_c]) \in X_0(N)(K_c).$$

The elements of $(\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times$ are in bijection with the lines through the origin in the plane $\mathcal{O}_K/c\mathcal{O}_K \approx (\mathbb{Z}/c\mathbb{Z})^2$. These lines are in bijection with the sublattices of $\mathcal{O}_K$ of index c. The aforementioned sublattices are fractional $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ ideals, and each one represents an element of the kernel of the natural map $\mathrm{Cl}(\mathcal{O}_c) \to \mathrm{Cl}(\mathcal{O}_K)$.

Proposition 6.2. *We have a commutative diagram of abelian groups:*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}(K_c/K_1) & \longrightarrow & \mathrm{Gal}(K_c/K) & \longrightarrow & \mathrm{Gal}(K_1/K) & \longrightarrow & 1 \\
 & & \downarrow \cong & & \theta \downarrow \cong & & \downarrow \cong & & \\
1 & \longrightarrow & (\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times & \longrightarrow & \mathrm{Cl}(\mathcal{O}_c) & \longrightarrow & \mathrm{Cl}(\mathcal{O}_K) & \longrightarrow & 1,
\end{array}$$

where the rightmost two vertical isomorphisms are induced by the Artin reciprocity map of class field theory, and the bottom row involves the bijections mentioned above.

Proof. This is standard; see, e.g., [Gro91, §3]. □

As explained in [Gro84, §4, (4.2)], for $[\mathfrak{b}] \in \mathrm{Cl}(\mathcal{O}_c)$, we have

$$(\mathcal{O}_c, \mathfrak{n}_c, \mathfrak{a})^{\theta(\mathfrak{b})} = (\mathcal{O}_c, \mathfrak{n}_c, \mathfrak{a}\mathfrak{b}^{-1}).$$

Also [Gro84, §6], we have

$$T_c(x_1) = T_c((\mathcal{O}_K, \mathfrak{n}, \mathcal{O}_K)) = \sum_{\mathfrak{b} \subset \mathcal{O}_K} (\mathcal{O}_c, \mathfrak{n}_c, \mathfrak{b}) \in \mathrm{Div}(X_0(N)), \tag{6.1}$$

where the sum is over *sublattices* $\mathfrak{b} \subset \mathcal{O}_K$ of index c.

Remark 6.3. We emphasize: the $\mathfrak{b}$ are not *ideals* of $\mathcal{O}_K$, but merely ideals of $\mathcal{O}_c$! If they were ideals of $\mathcal{O}_K$, they would have norm $c = \#(\mathcal{O}_K/\mathfrak{b})$, but c is a product of distinct inert primes, so there are no ideals of $\mathcal{O}_K$ of norm c.

6.1.2 Enhanced supersingular elliptic curves in characteristic ℓ

We consider enhanced elliptic curves $\mathbf{E} = (E, C)$, where E is an elliptic curve and $C \subset E$ is a cyclic subgroup of order N. The terminology *enhanced elliptic curves* is used in [Rib90a, §3].

Recall that we fixed above an inert prime $\ell \nmid c$ and a prime λ of $\overline{\mathbb{Z}}$ over ℓ. The set $X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}}$ of supersingular points on the mod λ reduction of $X_0(N)$ is the set of isomorphism classes of enhanced elliptic curves $\mathbf{E} = (E, C)$, where E is a supersingular elliptic curve over $\mathbb{F}_{\ell^2}$ and $C \subset E$ is a cyclic subgroup of order N.

Let $[\mathbf{E}_1] = x_1 \in X_0(N)(K_1)$, so $\mathbf{E}_1$ is a representative enhanced elliptic curve corresponding to the Heegner point x_1. Since $\mathfrak{n}$ is an $\mathcal{O}_K$-ideal, we have $\mathcal{O}_K = \mathrm{End}(\mathbf{E}_1)$, so we obtain an inclusion

$$\mathcal{O}_K = \mathrm{End}(\mathbf{E}_1) \hookrightarrow \mathrm{End}(\overline{\mathbf{E}}_1). \tag{6.2}$$

Remark 6.4. To see that Equation (6.2) is injective, note that by [ST68, Lem. 2], reduction modulo the prime λ of $\overline{\mathbb{Z}}$ induces an isomorphism $E_1[p^n] \xrightarrow{\cong} \overline{E}_1[p^n]$ for any prime power p^n with $p \neq \ell$ and p a prime of good reduction for E_1 (the lemma only asserts the map is surjective, but it is a map between finite groups of the same order, hence is an isomorphism). If $\varphi \in \mathrm{End}(\mathbf{E}_1)$ acts as 0 on $\overline{\mathbf{E}}_1$, then it acts as 0 on $\overline{E}_1[p^\infty]$, hence acts as 0 on $E_1[p^\infty]$, hence is 0 (since endomorphisms have finite degree).

The following lemma implies that

$$[\overline{\mathbf{E}}_1] \in X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}}.$$

Lemma 6.5. *Suppose F is an elliptic curve defined over an extension M of K and that F has CM by an order $\mathcal{O}$ of K. Suppose that $\ell \in \mathbb{Z}$ is a prime that is inert in K such that $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$. Let λ be a prime of M lying over ℓ and assume F has good reduction at λ, and let k be residue field modulo λ. Then the reduction F_k of F modulo λ is a supersingular elliptic curve.*

Proof. This is well known (see [Lan87, Ch. 10, §4, Thm. 10, Case 1] and [Sil94, Exercise 2.30]), but for the convenience of the reader we give a more conceptual proof than the ones cited above. It follows from the definition of F_k in terms of Néron models that $\mathcal{O}$ acts (functorially) on F_k. Moreover, because $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$, the ℓ-torsion subgroup $F_k[\ell] = F_k(\overline{\mathbb{F}}_\ell)[\ell]$ is a vector space over the finite field $\mathcal{O}_K/(\ell) \approx \mathbb{F}_{\ell^2}$. Thus $d = \dim_{\mathbb{F}_\ell} F_k[\ell]$ is even. Since F_k is an elliptic curve over a finite field of characteristic ℓ, we have $d \leq 1$, so $d = 0$, hence F_k is supersingular. □

We view $X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}}$ as explained in [Rib90a, §3], especially [Rib90a, Rmk. 3.5, pg 441], which builds on work of Deuring and Shimura. The endomorphism ring $R = \mathrm{End}(\overline{\mathbf{E}}_1)$ is an Eichler order of level N in the (unique up to isomorphism) rational quaternion algebra B ramified at ℓ and ∞. We have a bijection

$$X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}} \xrightarrow{\cong} \{ \text{ right fractional ideal classes in } R \}, \tag{6.3}$$

where two (nonzero) fractional right R-ideals $I, J \subset B$ are equivalent if there exists $\alpha \in B$ such that $\alpha I = J$. For any enhanced elliptic curve $\mathbf{F}$, endow $\mathrm{Hom}(\overline{\mathbf{E}}_1, \mathbf{F})$ with the structure of right R-module as follows: for $\varphi \in \mathrm{Hom}(\overline{\mathbf{E}}_1, \mathbf{F})$ and $r \in R$ we put $\varphi.r = \varphi \circ r$. This bijection sends $[\mathbf{F}]$ to the class of a right R-ideal that is isomorphic as a right R-module to the right R-module $\mathrm{Hom}(\overline{\mathbf{E}}_1, \mathbf{F})$. Also, we see that the right R-module $\mathrm{Hom}(\overline{\mathbf{E}}_1, \mathbf{F})$ is isomorphic to *some* right R-ideal I as follows. By [Mes86,

§2.4, pg. 223] or [Rib90a, Lem. 3.17], there exists an isogeny $\psi : \mathbf{F} \to \overline{\mathbf{E}}_1$. Using such an isogeny, we obtain an embedding

$$\mathrm{Hom}(\overline{\mathbf{E}}_1, \mathbf{F}) \hookrightarrow \mathrm{End}(\overline{\mathbf{E}}_1) = R$$

given by $\varphi \mapsto \psi \circ \varphi$, and the right ideal I is the image of $\mathrm{Hom}(\overline{\mathbf{E}}_1, \mathbf{F})$ under this embedding. Making a different choice of isogeny ψ replaces I by an equivalent right ideal.

6.1.3 Action of Hecke operators on supersingular divisors

The Hecke operators T_n act on $\mathrm{Div}(X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}})$, as explained in [Rib90a, pg. 443–445], and this action translates to an action on the free abelian group on the right R-ideal classes via the bijection (6.3) above, as explained in, e.g., [Koh01, §3.2]. For n any integer coprime to ℓN, we have

$$T_n([I]) = \sum_{J \subset I} [J], \tag{6.4}$$

where the sum is over right R ideals $J \subset I$ with $I/J \approx (\mathbb{Z}/n\mathbb{Z})^2$. We apply (6.4) to obtain a more explicit description of the image of the unit ideal (which corresponds to the reduction of x_1) under the Hecke operator T_c. Let

$$\overline{R} = R \otimes (\mathbb{Z}/c\mathbb{Z}) \cong R/cR.$$

Since c is coprime to N and coprime to the unique finite prime ℓ that ramifies in B, we have $R \otimes \mathbb{Z}_c \approx M_2(\mathbb{Z}_c)$, hence

$$\overline{R} \approx M_2(\mathbb{Z}/c\mathbb{Z}) \cong \bigoplus_{\text{primes } p|c} M_2(\mathbb{F}_p).$$

For any right ideal $I \subset \overline{R}$, let $\tilde{I}$ denote the inverse image of I in R under the natural surjection $R \to \overline{R}$. The right ideals of $\overline{R}$ correspond to the right ideals of R that contain cR, so the Hecke operator T_c acts on the unit ideal R via

$$T_c([R]) = \sum_{\substack{\text{right ideals } I \subset \overline{R} \\ \text{with } \overline{R}/I \approx (\mathbb{Z}/c\mathbb{Z})^2}} [\tilde{I}]. \tag{6.5}$$

More generally, for any right R-ideal J with $[R : J]$ coprime to c, we have

$$T_c([J]) = \sum_{\substack{\text{right ideals } I \subset \overline{R} \\ \text{with } \overline{R}/I \approx (\mathbb{Z}/c\mathbb{Z})^2}} [\tilde{I} \cap J].$$

6.1.4 Statement of the main theorem

As in the diagram of Proposition 6.2 above, let $[\mathfrak{a}] \in \ker(\mathrm{Cl}(\mathcal{O}_c) \to \mathrm{Cl}(\mathcal{O}_K))$ be an ideal class, and let $[\alpha] \in (\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times$ be the corresponding element, so $\alpha \in \mathcal{O}_K$. By replacing $\mathfrak{a}$ by an equivalent ideal, we may assume that $\mathfrak{a} = \mathbb{Z}\alpha + c\mathcal{O}_K$. Suppose $[\mathfrak{b}] \in \ker(\mathrm{Cl}(\mathcal{O}_c) \to \mathrm{Cl}(\mathcal{O}_K))$ is another ideal class, with corresponding element $[\beta]$, and let $\theta_{[\mathfrak{b}]} \in \mathrm{Gal}(K_c/K_1)$ be the corresponding automorphism. Let $I_\mathfrak{b} \subset \overline{R}$ be a right ideal such that

$$(\mathcal{O}_c, \mathfrak{n}_c, \mathfrak{b}) \mapsto [\tilde{I}_\mathfrak{b}] \tag{6.6}$$

under composition of reduction modulo λ with the equivalence (6.3) above. There is such a right ideal $I_{\mathfrak{b}}$ because $(\mathcal{O}_c, \mathfrak{n}_c, \mathfrak{b})$ is in the support of $T_c(x_1)$, and $[\tilde{I}_{\mathfrak{b}}]$ is in the support of $T_c(x_1 \pmod{\lambda})$ (see Equation (6.1)).

The group $\mathrm{Gal}(K_c/K_1)$ does *not* act naturally on

$$X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}} = X_0(N)(\mathcal{O}_{K_c}/\lambda)^{\mathrm{ss}},$$

since $\ell\mathcal{O}_K$ splits as a product of many primes (of which λ is one of them); of course, the "useless" decomposition subgroup of $\mathrm{Gal}(K_c/K_1)$ associated to λ (which has order 1!) does naturally act. However, as we will now see, $\mathrm{Gal}(K_c/K_1)$ acts naturally on a subset of the right ideals of $\overline{R}$. The challenge is that we need to compute what happens if we take $x_c \in X_0(N)(K_c)$, act by Galois, then map the result to $X_0(N)(\mathbb{F}_{\ell^2})$, and we can do this explicitly by instead considering the action of $\mathrm{Gal}(K_c/K_1)$ on index c^2 ideals in $\overline{R}$.

Equation (6.2) asserts that given our choice of λ there is an inclusion $\mathcal{O}_K \hookrightarrow R$, which we fix and use to define a right action of $\mathrm{Gal}(K_c/K_1)$ on certain right ideals in $\overline{R}$. For $\alpha \in \mathcal{O}_K$, let $\overline{\alpha}$ denote the image of α in $\overline{R}$. If $\sigma \in \mathrm{Gal}(K_c/K_1)$ corresponds to $[\alpha] \in (\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times$, make σ act on the right on the set of right ideals I of $\overline{R}$ with $\overline{R}/I \approx (\mathbb{Z}/c\mathbb{Z})^2$ by $I^\sigma = \overline{\alpha}^{-1}I$. Finally, we state the main result of this section, which asserts that the natural right action of $\mathrm{Gal}(K_c/K_1)$ on the support of $T_c(x_1)$ in $\mathrm{Div}(X_0(N)/K_c)$ is compatible with the right action of $\mathrm{Gal}(K_c/K_1)$ that we just defined. We will prove this theorem in Section 6.2 below.

Theorem 6.6. *Let $\sigma \in \mathrm{Gal}(K_c/K_1)$, $[\mathfrak{b}] \in \ker(\mathrm{Cl}(\mathcal{O}_c) \to \mathrm{Cl}(\mathcal{O}_K))$, and let $[\tilde{I}_{\mathfrak{b}}]$ correspond to $(\mathcal{O}_c, \mathfrak{n}_c, \mathfrak{b}) \pmod{\lambda}$ as in Equation 6.6 above. Then*

$$(\mathcal{O}_c, \mathfrak{n}_c, \mathfrak{b})^\sigma \pmod{\lambda} \quad = \quad [\widetilde{I_{\mathfrak{b}}^\sigma}].$$

6.2 Proof of Theorem 6.6

This section is devoted to giving a proof of Theorem 6.6. When $c = 1$ the relevant objects all have cardinality 1 and the statement is trivial, so for the rest of this section we assume that $c > 1$. The strategy of the proof is to reinterpret the ideal $I_{\mathfrak{b}}$ as the right annihilator of a certain left ideal, and observe that this left ideal behaves sensibly under the action of Galois. (The proof is long because we are not sneaking any important details under the rug.)

We may assume that the representative fractional ideal $\mathfrak{b}$ is a sublattice of $\mathcal{O}_K$ of index c. Let $\mathbf{E}_1$ be the enhanced elliptic curve corresponding to the triple $(\mathcal{O}_K, \mathfrak{n}, [\mathcal{O}_K])$ and let $\mathbf{E}_{\mathfrak{b}}$ be the enhanced elliptic curve corresponding to the triple $(\mathcal{O}_c, \mathfrak{n}_c, [\mathfrak{b}])$. Let $\psi_{\mathfrak{b}} : \mathbf{E}_{\mathfrak{b}} \to \mathbf{E}_1$ be the isogeny of degree c given by the map $\mathbb{C}/\mathfrak{b} \to \mathbb{C}/\mathcal{O}_K$ that is multiplication by 1 on tangent spaces. The complementary (or dual) isogeny $\hat{\psi}_{\mathfrak{b}} : \mathbf{E}_1 \to \mathbf{E}_{\mathfrak{b}}$ is then given by the map $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathfrak{b}$ induced by multiplication by c on $\mathbb{C}$. As in Section 6.1.2, we use $\psi_{\mathfrak{b}} \pmod{\lambda}$ to define a specific R-ideal $I_{\mathfrak{b}} \subset R = \mathrm{End}(\overline{\mathbf{E}}_1)$ that corresponds to $[\overline{\mathbf{E}}_{\mathfrak{b}}] \in X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}}$. More precisely, the ideal $I_{\mathfrak{b}}$ is the image of $\mathrm{Hom}(\overline{\mathbf{E}}_1, \overline{\mathbf{E}}_{\mathfrak{b}})$ in R via the map $\vartheta \mapsto \overline{\psi}_{\mathfrak{b}} \circ \vartheta$, i.e.,

$$I_{\mathfrak{b}} = \{\overline{\psi}_{\mathfrak{b}} \circ \vartheta \ : \ \vartheta : \overline{\mathbf{E}}_1 \to \overline{\mathbf{E}}_{\mathfrak{b}}\} \subset R = \mathrm{End}(\overline{\mathbf{E}}_1).$$

The following lemma follows immediately from the definitions given in Section 6.1:

Lemma 6.7. *Under our fixed choices of maps and prime λ, we have*

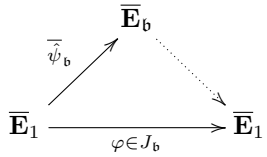
$$[\mathbf{E}_{\mathfrak{b}}] \pmod{\lambda} \quad \longleftrightarrow \quad [I_{\mathfrak{b}}],$$

where $I_{\mathfrak{b}}$ is defined as above.

Proposition 6.10 below characterizes $I_\mathfrak{b}$ as an annihilator of a left R-ideal, which will be easier to work with. Let

$$J_\mathfrak{b} = \{\varphi \in R : \varphi(\ker(\overline{\hat{\psi}}_\mathfrak{b})) = 0\},$$

which is a left R-ideal. Thus $J_\mathfrak{b}$ is the left ideal of all endomorphisms of $\overline{\mathbf{E}}_1$ that factor through the homomorphism $\overline{\hat{\psi}}_\mathfrak{b} : \overline{\mathbf{E}}_1 \to \overline{\mathbf{E}}_\mathfrak{b}$:



We will use the following lemma to compute the quotient abelian group $R/J_\mathfrak{b}$.

Lemma 6.8. *The natural map $R \to \mathrm{End}(\overline{E}_1[c])$ is surjective.*

Proof. It suffices to prove that for each prime $p \mid c$, the map

$$\varphi : R \otimes \mathbb{F}_p \to \mathrm{End}(\overline{E}_1[p]) \tag{6.7}$$

is surjective. Since R is an Eichler order of level N, N is coprime to c and $p \mid c$, we have $R \otimes \mathbb{F}_p = \mathrm{End}(\overline{E}_1) \otimes \mathbb{F}_p$. Also, since $p \neq \ell$, we have $\mathrm{End}(\overline{E}_1[p]) \approx \mathrm{End}(\mathbb{F}_p \oplus \mathbb{F}_p) \cong M_2(\mathbb{F}_p)$, and since $\overline{E}_1$ is a supersingular elliptic curve, $\dim_{\mathbb{F}_p}(R \otimes \mathbb{F}_p) = \mathrm{rank}_\mathbb{Z} R = 4$, so by a dimension count it suffices to prove that φ is injective. Suppose $\overline{f} = f \otimes 1 \in R \otimes \mathbb{F}_p$ is a nonzero element of $\ker(\varphi)$, with $f \in \mathrm{End}(\overline{E}_1)$. Then f acts as 0 on $\overline{E}_1[p]$, so f factors through multiplication by p, which means that there exists $g \in \mathrm{End}(\overline{E}_1)$ with $f = pg$. But then $\overline{f} = pg \otimes 1 = g \otimes p = g \otimes 0 = 0$, a contradiction. We conclude that φ is injective, hence surjective. □

Lemma 6.9. *We have $R/J_\mathfrak{b} \approx (\mathbb{Z}/c\mathbb{Z})^2$, where we view both sides as quotients of additive abelian groups.*

Proof. We prove this lemma by using Lemma 6.8 to reinterpret the assertion as a statement in $M_2(\mathbb{Z}/c\mathbb{Z})$, then use linear algebra modulo prime divisors of c to count dimensions. The kernel $D = \ker(\overline{\hat{\psi}}_\mathfrak{b}) \subset \overline{E}_1[c]$ is a cyclic group of order c. Let $\overline{J}$ be the left annihilator in $\mathrm{End}(\overline{E}_1[c]) \approx M_2(\mathbb{Z}/c\mathbb{Z})$ of D. For each prime $p \mid c$, we have $\mathrm{End}(\overline{E}_1[p]) \approx M_2(\mathbb{F}_p)$, and the factor of D in $\overline{E}_1[p]$ is of order p. The left annihilator in $M_2(\mathbb{F}_p)$ of a 1-dimensional subspace of $(\mathbb{F}_p)^2$ has $\mathbb{F}_p$-dimension 2, since it is the 2-dimensional $\mathbb{F}_p$-vector space of matrices whose rows are both a multiple of v, where v has dot product 0 with a basis for our 1-dimensional subspace. Putting these factors for each p together, we see that $\overline{J}$ is free of rank 2 over $\mathbb{Z}/c\mathbb{Z}$.

Since c kills $\ker(\overline{\hat{\psi}}_\mathfrak{b})$, we see that $cR \subset J_\mathfrak{b}$. We thus have an isomorphism of abelian groups

$$R/J_\mathfrak{b} \to M_2(\mathbb{Z}/c\mathbb{Z})/\overline{J}.$$

It is surjective because of Lemma 6.8. It is injective because $J_\mathfrak{b}$ is defined to be those endomorphisms that kill the subgroup D of $\overline{E}_1[c]$, which is a condition we can check in $\mathrm{End}(\overline{E}_1[c])$. The lemma thus follows. □

Next we use the left R-ideal $J_\mathfrak{b}$ to define a right R-ideal:

$$I'_\mathfrak{b} = \{\varphi \in R \ : \ J_\mathfrak{b}\varphi \subset cR\}.$$

Proposition 6.10. *We have*

$$I_{\mathfrak{b}} = I'_{\mathfrak{b}}$$

Proof. The strategy of the proof is to show that $I_{\mathfrak{b}} \subset I'_{\mathfrak{b}}$, then observe that both $I_{\mathfrak{b}}$ and $I'_{\mathfrak{b}}$ have the same index in R, so they must be equal.

To see that the inclusion $I_{\mathfrak{b}} \subset I'_{\mathfrak{b}}$ hold is a straightforward calculation using the definitions, as follows. An element $\varphi \in I_{\mathfrak{b}}$ is by definition of the form $\varphi = \overline{\psi}_{\mathfrak{b}} \circ \vartheta$, where $\vartheta : \overline{\mathbf{E}}_1 \to \overline{\mathbf{E}}_{\mathfrak{b}}$ and $\overline{\psi}_{\mathfrak{b}} : \overline{\mathbf{E}}_{\mathfrak{b}} \to \overline{\mathbf{E}}_1$, as above. Suppose $\delta \in J_{\mathfrak{b}}$, so $\delta \in \mathrm{End}(\overline{\mathbf{E}}_1)$ and $\delta(\ker(\overline{\hat{\psi}}_{\mathfrak{b}})) = 0$, hence $\delta = \delta' \circ \overline{\hat{\psi}}_{\mathfrak{b}}$ for some $\delta' : \overline{\mathbf{E}}_{\mathfrak{b}} \to \overline{\mathbf{E}}_1$. Thus

$$\delta \circ \varphi = (\delta' \circ \overline{\hat{\psi}}_{\mathfrak{b}}) \circ (\overline{\psi}_{\mathfrak{b}} \circ \vartheta) = \delta' \circ [c] \circ \vartheta \in cR,$$

which proves that $I_{\mathfrak{b}} \subset I'_{\mathfrak{b}}$.

We next prove that $[R : I'_{\mathfrak{b}}] = c^2$, as an application of Lemma 6.9. We have $c \in I'_{\mathfrak{b}}$, so $cR \subset I'_{\mathfrak{b}} \subset R$, hence $I'_{\mathfrak{b}}$ is completely determined by an ideal $\overline{I}'_{\mathfrak{b}} \subset \overline{R} = R \otimes (\mathbb{Z}/c\mathbb{Z}) \approx M_2(\mathbb{Z}/c\mathbb{Z})$. The ideal $\overline{I}'_{\mathfrak{b}}$ is the right annihilator of the left ideal $\overline{J}_{\mathfrak{b}} \subset \overline{R}$. For each prime $p \mid c$, Lemma 6.9 implies that the right annihilator mod p of $J_{\mathfrak{b}}$, i.e., the image of $I'_{\mathfrak{b}}$ in $R \otimes \mathbb{F}_p \cong M_2(\mathbb{F}_p)$, is proper and nontrivial. We conclude that $[R : I'_{\mathfrak{b}}] = c^2$.

Finally we observe that $[R : I_b] = c^2$. In light of Equation (6.5), the ideal $I_{\mathfrak{b}}$ is one of the ideals that appears in the sum in the definition of the Hecke operator T_c, so $[R : I_{\mathfrak{b}}] = c^2$. Since $[R : I'_{\mathfrak{b}}] = c^2$ and $I_{\mathfrak{b}} \subset I'_{\mathfrak{b}}$, it follows that $I_{\mathfrak{b}} = I'_{\mathfrak{b}}$, which proves the proposition. □

Suppose $[\alpha] \in (\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times$ with $\alpha \in \mathcal{O}_K$, and let $\mathfrak{a} \subset \mathcal{O}_K$ be the corresponding fractional $\mathcal{O}_c$-ideal (as in Section 6.1.4). Let $J_\alpha = J_{\mathfrak{a}}$. Proposition 6.12 below asserts that the natural right action of $(\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times$ on the left ideals in $\overline{R}$ is compatible with the natural right action of $(\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times$ on sublattices $\mathfrak{a} \subset \mathcal{O}_K$ of index c. Note the inverse that appears, which makes a left action into a right action (the group acting is abelian, so we are being slightly pedantic in emphasizing this). First we prove a lemma about an action on certain kernels.

Lemma 6.11. *Suppose* $[\alpha], [\beta] \in (\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times$ *with* $\alpha, \beta \in \mathcal{O}_K$. *Then*

$$\ker(\hat{\psi}_{\alpha\beta}) = \alpha \ker(\hat{\psi}_\beta).$$

Proof. As above, let $\mathfrak{a} \subset \mathcal{O}_K$ be the lattice of index c corresponding to $[\alpha]$. Also, recall from page 15 that the map $\hat{\psi}_\alpha : E_1 \to E_{\mathfrak{a}}$ is given over the complex numbers by the map $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathfrak{a}$ induced by multiplication by the integer c on $\mathbb{C}$. We have

$$E_1[c] = \left(\frac{1}{c}\mathcal{O}_K\right)/\mathcal{O}_K \cong \mathcal{O}_K/c\mathcal{O}_K \tag{6.8}$$

and the lattice $\mathfrak{a}$ defines a rank 1 subspace of $\mathcal{O}_K/c\mathcal{O}_K$. The isomorphism (6.8) identifies $\ker(\hat{\psi}_\alpha) \subset E_1[c]$ with the image of $\mathfrak{a}$ in $\mathcal{O}_K/c\mathcal{O}_K$. If $\mathfrak{b}$ corresponds to $[\beta]$, then $\alpha\mathfrak{b} = [\alpha\beta]$, so in terms of this presentation of $E_1[c]$, the claimed equality of the lemma follows. □

Note that since $[\alpha] \in (\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times$, the image $\overline{\alpha} \in \overline{R} = R \otimes (\mathbb{Z}/c\mathbb{Z})$ of α is invertible.

Proposition 6.12. *Let* α, β *be as above, let* J *be a left* R*-ideal, and let* $\overline{J}$ *denote its image in* $\overline{R}$. *Then*

$$\overline{J}_{\alpha\beta} = \overline{J}_\beta \cdot \overline{\alpha}^{-1},$$

where $\overline{\alpha}$ *is the image of* α *in* $\overline{R}$.

Proof. The reduction modulo λ map $E_1[c]$ to $\overline{E}_1[c]$ is an isomorphism since $\ell \nmid cN$ (see Remark 6.4), so reducing both sides of Lemma 6.11 modulo λ, we see that $\ker(\overline{\hat{\psi}}_{\alpha\beta}) = \alpha \ker(\overline{\hat{\psi}}_\beta)$. Thus

$$\begin{aligned} J_{\alpha\beta} =& \{\varphi \in R : \varphi(\ker(\overline{\hat{\psi}}_{\alpha\beta})) = 0\} \\ =& \{\varphi \in R : \varphi(\alpha(\ker(\overline{\hat{\psi}}_\beta))) = 0\} \\ =& \{\varphi \in R : (\varphi\alpha)(\ker(\overline{\hat{\psi}}_\beta)) = 0\} \\ =& \{\varphi \in R : \varphi\alpha \in J_\beta\} = R \cap (J_\beta \cdot \alpha^{-1}) \subset J_\beta \cdot \alpha^{-1}. \end{aligned}$$

We thus have an inclusion of (equivalent) fractional left R-ideals

$$J_{\alpha\beta} \subset J_\beta \cdot \alpha^{-1}.$$

Taking the image of both ideals in $\overline{R}$ gives an inclusion

$$\overline{J}_{\alpha\beta} \subset \overline{J}_\beta \cdot \overline{\alpha}^{-1} \subset \overline{R}.$$

Right multiplication by an invertible element in $\overline{R}$ is a bijection, so $[\overline{R} : \overline{J}_\beta \cdot \overline{\alpha}^{-1}] = [\overline{R} : \overline{J}_\beta] = c^2$, by Lemma 6.9. Since $[\overline{R} : \overline{J}_{\alpha\beta}] = c^2$, again by Lemma 6.9, it follows that $\overline{J}_{\alpha\beta} = \overline{J}_\beta \cdot \overline{\alpha}^{-1}$, as claimed.

□

Proof of Theorem 6.6. We have $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ two lattices of index c and corresponding classes

$$[\alpha], [\beta] \in (\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times.$$

Let $\sigma \in \mathrm{Gal}(K_c/K_1)$ be the automorphism corresponding to $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_c)$. Let $\mathfrak{g} \subset \mathcal{O}_K$ be the lattice of index c corresponding to the class $[\alpha^{-1}\beta] = [\alpha]^{-1}[\beta] \in (\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times$, so $I_{\alpha^{-1}\beta} = I_{\mathfrak{g}}$. Then, under reduction modulo λ, we have

$$(\mathcal{O}_c, \mathfrak{n}_c, \mathfrak{b})^\sigma = (\mathcal{O}_c, \mathfrak{n}_c, \mathfrak{a}^{-1}\mathfrak{b}) \longmapsto [I_{\alpha^{-1}\beta}].$$

For any left or right ideal I of R, let $\overline{I}$ be the image of I in $\overline{R} = R \otimes (\mathbb{Z}/c\mathbb{Z})$. By Proposition 6.10 the right ideal $\overline{I}_{\mathfrak{b}}$ is the right annihilator of the left ideal $\overline{J}_{\mathfrak{b}}$, and this is true for any $\mathfrak{b}$. By Proposition 6.12, we have that $\overline{I}_{\alpha^{-1}\beta}$ is the right annihilator of the left ideal $\overline{J}_{\alpha^{-1}\beta} = \overline{J}_\beta \cdot \overline{\alpha}$. We thus have

$$\begin{aligned} \overline{\alpha}^{-1} \cdot \overline{I}_\beta &= \overline{\alpha}^{-1} \cdot \{\varphi \in \overline{R} \ : \ \overline{J}_\beta \cdot \varphi = 0\} \\ &= \{\overline{\alpha}^{-1} \cdot \varphi \in \overline{R} \ : \ \overline{J}_\beta \cdot \varphi = 0\} \\ &= \{\varphi \in \overline{R} \ : \ \overline{J}_\beta \cdot \overline{\alpha}\varphi = 0\} \\ &= \{\varphi \in \overline{R} \ : \ \overline{J}_{\alpha^{-1}\beta} \cdot \varphi = 0\} = \overline{I}_{\alpha^{-1}\beta}, \end{aligned}$$

where in the third equality we replace φ by $\overline{\alpha}\varphi$, using that multiplication by $\overline{\alpha}$ defines a bijection $\overline{R} \to \overline{R}$. The displayed equality proves the theorem.

□

7 Reduction of Derived Classes

Let E be an elliptic curve over $\mathbb{Q}$, and let $P_{c,\sigma}$ be as in Equation (5.4) of Section 5. In this section, we apply the general results of Section 6 to give an algorithm to compute the reduction $z_{c,\sigma,\ell} \in E(\mathbb{F}_{\ell^2}) \otimes (\mathbb{Z}/p\mathbb{Z})$ (see Equation 5.6) when p is an odd prime and $E[p]$ is absolutely irreducible. We will apply this algorithm in Section 8 to verify that $[P_{c,\sigma}] \neq 0$, in specific examples. It is of interest to verify that $[P_{c,\sigma}] \neq 0$ in specific examples since, as was mentioned in Section 1, this was until now not known in even a single case for a curve E of rank ≥ 2.

We continue to assume that E and K satisfy the Heegner hypothesis. The goal of this section is to give an algorithm that we can use (in some specific examples) to verify that $[P_{c,\sigma}] \neq 0$ for some c. To do this, we consider the reduction map

$$r_\ell : E(K_c) \otimes (\mathbb{Z}/p^n\mathbb{Z}) \to E(\mathbb{F}_{\ell^2}) \otimes (\mathbb{Z}/p^n\mathbb{Z}), \tag{7.1}$$

given by reducing points modulo a fixed choice of prime λ over ℓ, where $\ell \nmid c$ is a prime that is inert in K, just as at the end of Section 5. If we find one prime ℓ such that $z_{c,\sigma,\ell} = r_\ell([P_{c,\sigma}]) \neq 0$, we conclude that $[P_{c,\sigma}] \neq 0$, as desired. We will thus be concerned primarily with computing whether or not $z_{c,\sigma,\ell}$ is 0 in the case when $n = 1$.

Remark 7.1. Assume that $Ш(E/\mathbb{Q})[p] = 0$, that $r_{\mathrm{an}}(E/\mathbb{Q}) = \mathrm{rank}(E(\mathbb{Q})) = 2$, and that we have shown that $[P_{c,\sigma}] \neq 0$ for some prime c. Then there is an alternative approach to compute the line spanned by $P_{c',\sigma'}$ for *any* inert prime c'. Jared Weinstein and the author learned about this idea from Karl Rubin after we implemented and ran the main algorithm of this paper, and wanted to better understand the data we obtained. The algorithm builds on [How04] and the Mazur-Rubin theory of Kolyvagin systems [MR04]. This is the subject of the forthcoming paper [SW10], and we have also used this algorithm as a double check on the calculations in Section 8. Quick summary: an easy calculation shows that the line has to be in the kernel of r_c; moreover, and this is deeper, r_c fails to have maximal rank if and only if $[P_c] = 0$.

In Section 7.1 we explain how to compute the reduction map from Heegner points in characteristic 0 to supersingular points in characteristic ℓ as an application of Deuring's lifting theorem and explicit computation with ternary quadratic forms. Section 7.2 contains the promised reinterpretation of Kolyvagin's derived classes construction directly on the divisor group of supersingular points, and Section 7.3 explicitly links this construction with reduction of derived classes from characteristic 0. Section 7.4 refines a crucial surjectivity result that Cornut used in proving Mazur's conjecture, which is also extremely important to our algorithm. Finally, Section 7.5 proves a multiplicity one theorem, which ensures that we have a general algorithm, rather than just a procedure that happens to work in every case we try.

7.1 Explicit computation of the reduction map using quaternion algebras

Let ℓ be a prime that is inert in K, as above. Following [Ste09, Piz80], let $B = B_{\ell,\infty}$ be the unique (up to isomorphism) quaternion algebra ramified at ℓ and ∞, and fix an Eichler order R of level N in B.

The group of Atkin-Lehner operators of level N has order 2^ν, where ν is the number of prime divisors of N. As discussed in Remark 4.1 above, the Heegner point x_1 is only well defined up to the choice of an ideal $\mathfrak{n}$ of $\mathcal{O}_K$ with $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$, and there are 2^ν

choices for $\mathfrak{n}$. We temporarily write $x_{1,\mathfrak{n}}$ for the choice of Heegner point x_1 associated to the ideal $\mathfrak{n}$.

The prime ℓ is inert in K, so by Lemma 6.5, each of the points $x_{1,\mathfrak{n}}$ defines a point on $X_0(N)(K_1)$ that reduces to a supersingular point in $X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}}$. Moreover, we have the bijection of Equation 6.3 between $X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}}$ and a certain set of right R-ideal classes. In terms of this bijection, we compute some $\overline{x}_1 \in X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}}$ corresponding to a choice of $\mathfrak{n}$ as follows. First, we enumerate all right ideal classes $[I]$ using standard algorithms, e.g., if N is odd by applying the Hecke operator T_2 repeatedly, starting with the unit ideal, and using theta series to check equivalence (see, e.g., [Piz80, Prop. 1.18]). Then we apply Theorem 7.2 below to find an I such that $\mathcal{O}_K$ embeds in R_I.

Let I be a fractional right R-ideal, and consider the left order

$$R_I = \{x \in B : xI \subset I\}$$

associated to I. We use the Deuring lifting theorem to give an algorithm to compute $\overline{x}_1$.

Theorem 7.2 (Deuring)**.** *The bijection of Equation* (6.3) *induces a bijection*

$$\{\overline{x}_{1,\mathfrak{n}} \in X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}} : \quad \textit{ideals } \mathfrak{n} \textit{ with } \mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}\} \xrightarrow{\cong} \{[I] : \mathcal{O}_K \textit{ embeds in } R_I\}.$$

Proof. See [GZ85, Prop. 2.7] (see also [JK10, §2] for a generalization in which $\mathcal{O}_K$ is replaced by $\mathcal{O}_c$). □

To compute a choice of $\overline{x}_1$ thus reduces to giving an algorithm to decide whether or not $\mathcal{O}_K$ embeds in R_I. As in [Gro87, pg. 172], let $G_I \approx \mathbb{Z}^3$ be the trace zero elements in $2R_I + \mathbb{Z}$, and let $q_I : G_I \to \mathbb{Q}$ be the normalized *ternary* quadratic form got by restricting the reduced norm on B to G_I.

Lemma 7.3. *There is an embedding of $\mathcal{O}_K$ into R_I if and only if the quadratic form q_I represents the absolute value $|D_K|$ of the discriminant of $\mathcal{O}_K$.*

Proof. This follows from [Gro87, Prop. 12.9] (see also [JK10, Lem. 4.1]). □

To compute $\overline{x}_1$ we compute the quadratic form q_I for a representative I for each right ideal class in turn, and decide whether or not it represents $|D_K|$. When we find one that does, we declare that our representative element is $\overline{x}_1 = \overline{x}_{1,\mathfrak{n}}$, which is well defined up to the choice of ideal $\mathfrak{n}$. In general (e.g., when the class number of K is bigger than 1), our current formula unfortunately requires computing all $x_{1,\mathfrak{n}}$ for all $\mathfrak{n}$ (see Theorem 7.8).

7.2 Kolyvagin's derived classes construction in terms of quaternion algebras

Let I be a right ideal in our fixed choice of Eichler order R of level N such that I corresponds to $\overline{x}_{1,\mathfrak{n}}$, computed as above.

Lemma 7.4. *By replacing I by an equivalent ideal, we can arrange that $I \otimes (\mathbb{Z}/c\mathbb{Z}) = R \otimes (\mathbb{Z}/c\mathbb{Z})$.*

Proof. For any prime $r \nmid N\ell$, the graph of the Hecke operator T_r is connected (see [Mes86, §2.4, pg. 223] or [Rib90a, Lem. 3.17]). If we choose r also coprime to c, then enumerate the right ideals of R by computing the action of T_r, starting with the unit

ideal, we will cover all the right ideal classes of R; in particular, there is an ideal I' equivalent to I obtained via this procedure. From the formula of Equation (6.4) for the action of Hecke operators, we see that $[R : I']$ is a power of r. Thus $I' \otimes (\mathbb{Z}/c\mathbb{Z}) = R \otimes (\mathbb{Z}/c\mathbb{Z})$, as claimed. □

Next we compute a choice of homomorphism

$$s : R \twoheadrightarrow M_2(\mathbb{Z}/c\mathbb{Z}). \tag{7.2}$$

This can be done individually for each prime divisor of c, and the maps assembled together to give s. For example, for each prime divisor $q \mid c$, one could consider the algebra $R \otimes (\mathbb{Z}/q\mathbb{Z})$ and apply [Voi, §4] to find an explicit isomorphism $R \otimes (\mathbb{Z}/q\mathbb{Z}) \to M_2(\mathbb{Z}/q\mathbb{Z})$.

Let q be any prime that is inert in K. Suppose the image of $\alpha \in \mathcal{O}_K$ generates the cyclic group

$$(\mathcal{O}_K/q\mathcal{O}_K)^\times/(\mathbb{Z}/q\mathbb{Z})^\times$$

of order $q+1$. Using a fixed choice of embedding of $\mathcal{O}_K$ into the left order of I from above (which exists by Theorem 7.2), we view α as an element of B. Let $\overline{\alpha}$ be the canonical image of α in $M_2(\mathbb{Z}/q\mathbb{Z}) = \overline{R}/q\overline{R}$ using the splitting s of (7.2).

For each $i = 0, \ldots, q$, let

$$\overline{J}_i = \{B \in M_2(\mathbb{Z}/q\mathbb{Z}) : (1,0)\overline{\alpha}^i B = 0\} \subset \overline{R}/q\overline{R}.$$

Suppose $[M]$ is a right ideal class of R, and (as in Lemma 7.4) choose a representative right ideal $M \subset R$ such that $q \nmid [R : M]$, so s defines a map $M \twoheadrightarrow \overline{R}$. For each i, let J_i be the inverse image of $\overline{J}_i$ in M. Define

$$D_{q,\alpha}([M]) = \sum_{i=1}^{q} i[J_i].$$

Extending linearly, we define an endomorphism

$$D_{q,\alpha} \in \mathrm{End}(\mathrm{Div}(X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}})).$$

Remark 7.5. We make two remarks about the above operator:

1. The map $D_{q,\alpha}$ is explicitly computable; it is closely related to computing the Hecke operator T_q, since $T_q([M]) = \sum_{i=0}^{q}[J_i]$ is almost the same as $D_{q,\alpha}([M])$, except without the coefficient in the enumeration of the J_i's.

2. The maps $D_{q,\alpha}$ typically do not commute with the Hecke operators or with each other.

Next write $c = p_1 \cdots p_t$, let $\sigma = (\sigma_1, \ldots, \sigma_t)$ with $\sigma_i \in \mathrm{Gal}(K_c/K_{c/p_i})$ be choices of generators, and let $\alpha = (\alpha_1, \ldots, \alpha_t)$ with $\alpha_i \in \mathcal{O}_K$ be the corresponding elements via the map of Equation 4.1 above. Define

$$D_{c,\alpha} = \prod_{i=1}^{t} D_{p_i,\alpha_i} \in \mathrm{End}(\mathrm{Div}(X_0(N)(\mathbb{F}_{\ell^2})^{\mathrm{ss}})).$$

7.3 Reduction of Kolyvagin's derived points

Let $f \in S_2(\Gamma_0(N))$ be a newform, let $I_f \subset \mathbb{T}$ be the annihilator of f in the Hecke algebra associated to $J_0(N)$, let $A_f = J_0(N)/I_f J_0(N)$ be the corresponding modular abelian variety with modular parametrization $\pi_f : J_0(N) \to A_f$ and let

$$\psi_f : \mathrm{Div}(X_0(N)^{\mathrm{ss}}_{\mathbb{F}_{\ell^2}}) \to A_f(\mathbb{F}_{\ell^2})$$

be the homomorphism that sends each supersingular point x to $\overline{\pi}_f(x - \infty)$, where $\overline{\pi}_f$ is the reduction modulo λ of π_f. By [BCDT01], our elliptic curve E is isogeneous to some A_f for a newform $f \in S_2(\Gamma_0(N))$ where N is the conductor of E.

Theorem 7.6. *We have the following in $A_f(\mathbb{F}_{\ell^2}) \otimes (\mathbb{Z}/p^n\mathbb{Z})$:*

$$[\overline{\pi}_f(D_{c,\sigma}(y_c))] = [\psi_f\left(D_{c,\alpha}([I])\right)].$$

Proof. This follows from Theorem 6.6. □

Let

$$\mathcal{I} = \{[I] : \mathcal{O}_K \hookrightarrow R_I\}$$

be the set of all right ideal classes of R whose left order admits an embedding of $\mathcal{O}_K$. For each such $[I]$, let n_I be half the number of primitive representatives of $|D_K|$ by the ternary quadratic form q_I. Let $\mathcal{H}$ be the $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$-orbit of the set of all Heegner points $x_{1,\mathfrak{n}} \in X_0(N)(K_1)$ for all ideals $\mathfrak{n} \subset \mathcal{O}_K$ with $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$.

Lemma 7.7. *For each $[I] \in \mathcal{I}$, the number of elements of $\mathcal{H}$ reducing to the point of $X_0(N)(\mathbb{F}_{\ell^2})$ corresponding to $[I]$ is equal to n_I.*

Proof. By [JK10, §2] there is a one-to-one correspondence between the Heegner points $x_{1,\mathfrak{n}}$ reducing to $[I]$ and $R_I^\times$ conjugacy classes of embeddings $O_K \hookrightarrow R_I$. By [JK10, Prop. 4.2] there is a $(\#R_I^\times/2)$-to-1 correspondence between embeddings $\mathcal{O}_K \hookrightarrow R_I$ and primitive representations of $|D|$ by q_I. Thus every pair of primitive representations of $|D|$ by q_I corresponds to $\#R_I^\times$ embeddings, so half the number of primitive representatives is the number of $R_I^\times$ conjugacy classes of embeddings. □

Theorem 7.8. *Let ν be the number of distinct prime divisors of N. We have the following in $A_f(\mathbb{F}_{\ell^2}) \otimes (\mathbb{Z}/p^n\mathbb{Z})$:*

$$\overline{\pi}_f([P_{c,\sigma}]) = 2^{-\nu} \cdot \sum_{[I]\in\mathcal{I}} n_I \cdot [\psi_f\left(D_{c,\alpha}([I])\right)] \tag{7.3}$$

Proof. This follows by combining Lemma 7.7 and Theorem 7.6, and noting that $\mathcal{H}$ is a disjoint union of $[K_1 : K]$ Atkin-Lehner orbits, each of size 2^ν. Thus in computing the sum on the right of (7.3) we are computing $\mathrm{Tr}_{K_1/K}(D_{c,\sigma}(y_c))$ separately 2^ν times, hence we divide out this extra factor of 2^ν, which is harmless since p is odd. □

We still have not explained how to explicitly compute the map ψ_f, so Theorem 7.8 does not yet yield an algorithm. In Section 7.4 we will establish that ψ_f is surjective after tensoring with $\mathbb{Z}/p\mathbb{Z}$, and in Section 7.5 we give conditions under which ψ_f is uniquely determined up to scalars by being Hecke equivariant ("multiplicity one"), which means we can compute ψ_f up to a scalar. Alternatively, as mentioned in Remark 2.3, we can sometimes instead avoid computing ψ_f at all if we know ψ_f is surjective by instead verifying that the $\mathbb{T}$-span of $\sum n_I D_{c,\alpha}([I])$ is all of $X \otimes \mathbb{F}_p$.

7.4 Map from the supersingular module to an optimal abelian variety quotient

Let ℓ be an inert prime that does not divide the level N, and let $k = \mathbb{F}_{\ell^2} \approx \mathcal{O}_K/\ell\mathcal{O}_K$, which is a finite field of order ℓ^2. The Hecke algebra $\mathbb{T}$ acts via correspondences on many objects attached to the modular curves $X_0(N)$ and $X_1(N)$, e.g., via endomorphisms on the Jacobian $J_0(N)$ and also on

$$X = \mathrm{Div}(X_0(N)(k)^{\mathrm{ss}}) \qquad \text{and} \qquad X^0 = \mathrm{Div}^0(X_0(N)(k)^{\mathrm{ss}}). \tag{7.4}$$

Also, $\mathbb{T}$ acts on the *Shimura subgroup* $\Sigma = \ker(J_0(N) \to J_1(N))$. We say that a $\mathbb{T}$-module M is *Eisenstein* (in the sense of [Maz77]) if for any prime $p \nmid N$, the operator $T_p - (1+p)$ annihilates M. For example, [Rib88, Thm. 1] asserts that Σ is Eisenstein.

Let $J = J_0(N)_k$, and consider the natural $\mathbb{T}$-module homomorphism

$$X \to J(k) \tag{7.5}$$

that sends a divisor $D \in X$ to the equivalence class of the degree zero divisor $D - \deg(D)\infty$ in the Jacobian.

Proposition 7.9 (Ribet)**.** *The cokernel S of the induced map*

$$X^0 \to J(k) \tag{7.6}$$

is the Cartier dual $\Sigma^\vee$ of Σ, and the $\mathbb{T}$-module $\Sigma^\vee$ is Eisenstein.

Proof. The following argument is due to Ribet (see [Rib10]). Let F be the ℓth power Frobenius endomorphism of J and let V be its dual. We have $J(k) = J[1-F^2]$. This kernel is Cartier dual to $J[1-V^2]$, since it is obtained by dualizing the following exact sequence (see [Mum70, §15, pg. 143] and [Mil86, §11]):

$$0 \to J[1-F^2] \to J \xrightarrow{1-F^2} J \to 0.$$

Ribet proved in 1983 (see [Pra95, Prop. 3.6]) that the subgroup $J[1-V^2]$ contains the reduction modulo ℓ of the Shimura subgroup Σ of J, and S is the annihilator of Σ in the natural perfect pairing between $J[1-F^2]$ and $J[1-V^2]$. The content of [Pra95, Prop. 3.6] is that the supersingular group is "as large as possible" in the sense that it is the full annihilator.

In the pairing between $J[1-F^2]$ and $J[1-V^2]$, there is the standard formula $\langle Tx, y\rangle = \langle x, T^\dagger y\rangle$, where the dagger refers to the Rosati involution of $\mathrm{End}(J)$ and T is a Hecke operator. The Hecke operators T_n with n coprime to N are self dual with respect to the Rosati involution.

To see that the group $J[1-F^2]/S$ is Eisenstein in the sense that $T_p = 1+p$ on this quotient for p prime to N, let η be the difference $T_p - (1+p)$, which is self dual with respect to the Rosati involution, since T_p is self dual and multiplication by the integer $(1+p)$ is also self dual. For $x \in J[1-F^2]$, we want to show that $\eta(x)$ is in the supersingular divisor class group; by [Pra95, Prop. 3.6], as mentioned above, this is the same as showing that $\langle \eta(x), y\rangle = 0$ for all $y \in \Sigma$. However, η annihilates Σ (see [Rib88, Thm. 1]), so

$$\langle \eta(x), y\rangle = \langle x, \eta(y)\rangle = 0.$$

□

The following proposition is a refinement of [Cor02, Prop. 4.4]. An *optimal quotient* A of $J_0(N)$ is any quotient of $J_0(N)$ by an abelian subvarieties (see [CS01, §3] for the basic properties of optimal quotients). For example, the abelian varieties A_f of Section 7.3 above are, up to isogeny, the simple optimal quotients of $J_0(N)$ that satisfy the hypothesis of Proposition 7.10 below.

Proposition 7.10. *Let A be any abelian variety optimal quotient of $J_0(N)$ such that $\ker(J_0(N) \to A)$ is Hecke stable, let $\mathfrak{m}$ be a non-Eisenstein maximal ideal of $\mathbb{T}$, and let X^0 be as in Equation* (7.6)*. Then the natural map*

$$X^0 \to A(k) \otimes_{\mathbb{T}} (\mathbb{T}/\mathfrak{m}) \tag{7.7}$$

is surjective. In particular, if $A[\mathfrak{m}]$ is irreducible, then (7.7) *is surjective.*

Proof. As above, let S be the image of X^0 in $J(k)$, and let S_A be the image of S in $A(k)$. Also, let $Q = A(k)/S_A$. In light of Proposition 7.9, we have a commutative diagram of $\mathbb{T}$-modules with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S & \longrightarrow & J(k) & \longrightarrow & \Sigma^\vee & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & S_A & \longrightarrow & A(k) & \longrightarrow & Q & \longrightarrow & 0. \end{array}$$

Since A is an optimal quotient of $J_0(N)$, there is an abelian variety B such that we have an exact sequence $0 \to B \to J_0(N) \to A \to 0$ of abelian varieties over $\mathbb{Q}$ with good reduction at ℓ (since $\ell \nmid N$). This sequences reduces to an exact sequence $0 \to B_k \to J \to A_k \to 0$ over k by [BLR90, §7.5, Thm. 4] (we have "$e < p-1$", since $p = \ell$ is odd and $e = 1$). Lang's theorem (see [Lan56] or [Ser88, §VI.4]) implies that $\mathrm{H}^1(k, B_k) = 0$, so $J(k) \to A(k)$ is surjective. The snake lemma then implies that the vertical map $\Sigma^\vee \to Q$ is surjective.

If $\Sigma^\vee \otimes_{\mathbb{T}} (\mathbb{T}/\mathfrak{m}) \cong \Sigma^\vee/\mathfrak{m}\Sigma^\vee$ is nonzero then $I = \mathrm{Ann}_{\mathbb{T}}(\Sigma^\vee/\mathfrak{m}\Sigma^\vee)$ equals $\mathfrak{m}$ since $\mathfrak{m}$ is maximal. Every $\eta_q = T_q - (q+1)$ for $q \nmid N$ is in I, since $\Sigma^\vee$ is Eisenstein by Proposition 7.9. But some $\eta_q \notin \mathfrak{m}$, since $\mathfrak{m}$ is non-Eisenstein, a contradiction. Thus $\Sigma^\vee \otimes_{\mathbb{T}} (\mathbb{T}/\mathfrak{m}) = 0$, so upon tensoring the rightmost vertical surjection of the above diagram with $\mathbb{T}/\mathfrak{m}$, we conclude that $Q \otimes_{\mathbb{T}} (\mathbb{T}/\mathfrak{m}) = 0$. Tensoring the bottom row over $\mathbb{T}$ with $\mathbb{T}/I$ and using that tensor product is right exact again then implies that (7.7) is surjective.

Since $\mathfrak{m}$ is a maximal ideal such that $A[\mathfrak{m}]$ is irreducible (which implies by definition that $A[\mathfrak{m}] \neq 0$), there is a prime $q \nmid N$ such that $\eta_q = T_q - (1+q)$ does not act as 0 on $A[\mathfrak{m}]$, since otherwise $A[\mathfrak{m}]$ would have semisimplification the reducible representation $1 \oplus \chi$, where χ is the cyclotomic character. Thus $\mathfrak{m}$ is non-Eisenstein, and the first part of the proposition proves the second claim. □

7.5 Multiplicity one theorem

The results of this section may be viewed as a partial generalization of [Rib99, Theorem. 2.3] and [Eme02, Thm. 4.2, Thm. 4.6] to more general levels. In particular, we prove under mild hypothesis that the multiplicity of a certain submodule of the $\mathbb{T}$-module $\mathrm{Div}(X_0(N)^{\mathrm{ss}}_{\mathbb{F}_{\ell^2}}) \otimes \mathbb{F}_p$ is 1. Our proof proceeds by finding a natural injective map from this submodule into $J_0(N\ell)[p]$, and observing that the image lies in a 1-dimensional subspace, as a consequence of a general multiplicity one result for $J_1(N\ell)$. For any positive integer N, let $\mathbb{T}(N)$ denote the ring of Hecke operators acting on $S_2(\Gamma_0(N))$.

Let N be a positive integer and ℓ a prime that does divide N, and let $X = \mathrm{Div}(X_0(N)^{\mathrm{ss}}_{\mathbb{F}_{\ell^2}})$, as in Equation (7.4). Let $f = \sum a_n q^n \in S_2(\Gamma_0(N))$ be a newform of level N and let $\mathfrak{m}_0$ be a maximal ideal of $\mathbb{T}(N)$ such that the following three conditions simultaneously hold:

1. $\mathfrak{m}_0$ has odd residue characteristic p,
2. $a_\ell, \ell + 1 \in \mathfrak{m}_0$, and
3. the 2-dimensional mod p Galois representation ρ attached to $\mathfrak{m}_0$ is absolutely irreducible.

By Ribet's level raising theorem (see [Rib90b]), for each choice of ± 1, there is a maximal ideal $\mathfrak{m}$ in the Hecke algebra $\mathbb{T} = \mathbb{T}(N\ell)$ such that $\rho_{\mathfrak{m}} \approx \rho$ and $T_\ell \pm 1 \in \mathfrak{m}$. Letting $J = J_0(N\ell)$, as explained in [RS01, §3.3], we have

$$J[\mathfrak{m}] \cong \bigoplus_{i=1}^{t} \rho, \tag{7.8}$$

for some integer $t \geq 1$ called the *multiplicity of* $\mathfrak{m}$. That $t \geq 1$ follows from an argument of Mazur, as explained in [RS01, §3.3].

Proposition 7.11. *We have* $\dim_{\mathbb{T}/\mathfrak{m}} \mathrm{Hom}(X, \mu_p)[\mathfrak{m}] \leq t$.

Proof. The proof is inspired by [Rib94, Prop. 7.7], though that argument takes place in the midst of a proof by contradiction.

Let $G_\ell \approx \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ be the decomposition subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ associated to our fixed choice of prime λ of $\overline{\mathbb{Z}}$ over ℓ, and let $I_\ell \subset G_\ell$ be the inertia subgroup. Let $k = \mathbb{F}_\ell$, and let J_k be the special fiber of the Néron model of J at k. By [ST68, Lem. 2], we have $J_k[\mathfrak{m}] \cong J[\mathfrak{m}]^{I_\ell}$, and because ρ is unramified at ℓ, we have $J[\mathfrak{m}]^{I_\ell} = J[\mathfrak{m}]$, so $J_k[\mathfrak{m}] \cong J[\mathfrak{m}]$.

Let Φ be the component group of J_k. As explained in [CS01, §4], we have a diagram with an exact row and exact column, where T is the toric part of J_k^0 and B is an abelian variety:

$$\begin{array}{ccccccccc} & & & & 0 & & & & \\ & & & & \downarrow & & & & \\ & & & & T & & & & \\ & & & & \downarrow & & & & \\ 0 & \longrightarrow & J_k^0 & \longrightarrow & J_k & \longrightarrow & \Phi & \longrightarrow & 0 \\ & & & & \downarrow & & & & \\ & & & & B & & & & \\ & & & & \downarrow & & & & \\ & & & & 0 & & & & \end{array}$$

Moreover, $X^0 \cong \mathrm{Hom}(T, \mathbb{G}_m)$, so $T \cong \mathrm{Hom}(X^0, \mathbb{G}_m)$ and $T[p] = \mathrm{Hom}(X^0, \mu_p)$. Hence

$$\mathrm{Hom}(X^0, \mu_p)[\mathfrak{m}] = T[\mathfrak{m}] \hookrightarrow J_k^0[\mathfrak{m}] \subset J_k[\mathfrak{m}] \cong J[\mathfrak{m}]. \tag{7.9}$$

The representation ρ arises from level N, so is unramified at ℓ. The characteristic polynomial of $\rho(\mathrm{Frob}_\ell)$ is $x^2 - a_\ell x + \ell$. Our hypothesis 2 on a_ℓ and $\ell + 1$ imply that

$$x^2 - a_\ell x + \ell = x^2 - 1 \in \mathbb{F}_p[x].$$

Since $x^2 - 1 = (x-1)(x+1)$ and p is odd, we have a decomposition of $\mathbb{T}[D]$-modules $J[\mathfrak{m}] \cong J[\mathfrak{m}]^+ \oplus J[\mathfrak{m}]^-$ and (7.8) implies that the two summands have dimension t. Here we are using that $J[\mathfrak{m}] = \oplus\rho$; if V is the space underlying ρ, then V has dimension 2 and the characteristic polynomial of Frob_ℓ on V is $(x-1)(x+1)$, so V^+ and V^- each have dimension 1.

By [Rib90a, Prop. 3.7–3.8], the action of Frob_ℓ on X^0 is via $-T_\ell$. Since $T_\ell \pm 1 \in \mathfrak{m}$ (for some choice of sign), the action of Frob_ℓ on the $\mathbb{T}[D]$-module $\mathrm{Hom}(X^0, \mu_p)[\mathfrak{m}]$ is by $\pm\ell$ (because Frob_ℓ acts on μ_p by ℓth powering). Since $\ell + 1 \in \mathfrak{m}_0$, we have $\ell \equiv \pm 1 \pmod{p}$, so we conclude that Frob_ℓ acts on $\mathrm{Hom}(X^0, \mu_p)[\mathfrak{m}]$ as either $+1$ or -1. Thus the sequence of inclusions of Equation (7.9) sends $\mathrm{Hom}(X^0, \mu_p)[\mathfrak{m}]$ to a submodule of $J[\mathfrak{m}]^\pm$ for one choice of sign, from which we conclude that

$$\dim_{\mathbb{T}/\mathfrak{m}} \mathrm{Hom}(X^0, \mu_p)[\mathfrak{m}] \leq \dim_{\mathbb{T}/\mathfrak{m}} J[\mathfrak{m}]^\pm = t.$$

□

Lemma 7.12. *We have $X/\mathfrak{m}X \cong X^0/\mathfrak{m}X^0$. (In fact, this lemma is true for any non-Eisenstein maximal ideal $\mathfrak{m}$.)*

Proof. It follows from the explicit description of Hecke operators (see Section 6.1.3) that we have an exact sequence $0 \to X^0 \to X \xrightarrow{\deg} \mathbb{Z} \to 0$, where $\mathbb{T}$ acts on $\mathbb{Z}$ by $T_r = r + 1$ for r a prime coprime to $N\ell$. Tensoring this exact sequence over $\mathbb{T}$ with $\mathbb{T}/\mathfrak{m}$ yields an exact sequence

$$\mathrm{Tor}_1^{\mathbb{T}}(\mathbb{Z}, \mathbb{T}/\mathfrak{m}) \to X/\mathfrak{m}X \to X^0/\mathfrak{m}X^0 \to \mathbb{Z} \otimes_{\mathbb{T}} (\mathbb{T}/\mathfrak{m}) \to 0.$$

Since $\mathfrak{m}$ is non-Eisenstein, $\mathbb{Z} \otimes_{\mathbb{T}} (\mathbb{T}/\mathfrak{m}) = 0$ and

$$\mathrm{Tor}_1^{\mathbb{T}}(\mathbb{Z}, \mathbb{T}/\mathfrak{m}) = \mathrm{Tor}_1^{\mathbb{T}}(\mathbb{T}/\mathfrak{m}, \mathbb{Z}) = \mathbb{Z}[\mathfrak{m}] = 0.$$

□

Recall that $\mathfrak{m}$ is any maximal ideal of level $N\ell$ arising from level raising, as explained above (7.8) at the beginning of this section.

Proposition 7.13. *We have* $\dim_{\mathbb{T}/\mathfrak{m}} \mathrm{Hom}(X, \mu_p)[\mathfrak{m}] \geq 1$.

Proof. Let $A = A_f$ be the optimal quotient of $J_0(N)$ attached to f, let $k = \mathbb{F}_{\ell^2}$, and let $\mathbb{T} = \mathbb{T}(N)$. Consider the $\mathbb{T}[\mathrm{Frob}_\ell]$-module $M = A(k) \otimes \mathbb{T}/\mathfrak{m}_0$. Proposition 7.10 implies that the $\mathbb{T}$-module homomorphism

$$X^0 \to M \cong M^+ \oplus M^-$$

is surjective. Projection onto a one-dimensional $\mathbb{T}/\mathfrak{m}_0$-subspace of each of M^+ and M^- defines a nonzero element of $\mathrm{Hom}(X^0, \mu_p)[\mathfrak{m}]$ for each of the two possible choices of $\mathfrak{m}$. Note that $\mathrm{Frob}_\ell^2 = 1$ on $A[\mathfrak{m}]$ by hypothesis, so $A[\mathfrak{m}](\overline{k}) = A[\mathfrak{m}](k)$. Here we also use that $\dim_{\mathbb{T}/\mathfrak{m}} A[\mathfrak{m}] \geq 1$ (see [RS01, §3.3]).

It is elementary that every element of $\mathrm{Hom}(X, \mu_p)[\mathfrak{m}]$ factors through $X/\mathfrak{m}X$ and likewise for X^0, so by Lemma 7.12 we have

$$\mathrm{Hom}(X, \mu_p)[\mathfrak{m}] \cong \mathrm{Hom}(X/\mathfrak{m}X, \mu_p)[\mathfrak{m}] \cong \mathrm{Hom}(X^0/\mathfrak{m}X^0, \mu_p)[\mathfrak{m}] \cong \mathrm{Hom}(X^0, \mu_p)[\mathfrak{m}].$$

□

Theorem 7.14. *If $p \nmid N$, then* $\dim_{\mathbb{T}/\mathfrak{m}} \mathrm{Hom}(X, \mu_p)[\mathfrak{m}] = 1$.

Proof. In light of the above two propositions, it suffices to show that $t = 1$, where t is the multiplicity in Equation (7.8). Let f be a cuspidal eigenform in $S_2(\Gamma_0(N\ell))$ such that $\mathrm{Ann}_{\mathbb{T}}(f) \subset \mathfrak{m}$, and view f as an element of $S_2(\Gamma_1(N\ell))$. Let $\mathfrak{m}_1$ be the inverse image of $\mathfrak{m}$ in $\mathbb{T}_1 = \mathbb{T}_1(N\ell)$ under the natural map $\mathbb{T}_1 \to \mathbb{T}$. Since $p > 2$ and $p \nmid N\ell$, [Edi92, Th. 9.2, part 1] implies that $\dim_{\mathbb{T}_1/\mathfrak{m}_1} J_1(N\ell)[\mathfrak{m}_1] = 2$. The inclusion $J_0(N\ell) \to J_1(N\ell)$ has kernel the Shimura subgroup, which is Eisenstein (by [Rib88, Thm. 1]), so $J_0(N\ell)[\mathfrak{m}] \hookrightarrow J_1(N\ell)[\mathfrak{m}_1]$. Since $t \geq 1$, this inclusion implies that $t = 1$. □

8 Implementation and Data

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 8.1. Let r_ℓ be the reduction map from Equation (7.1). We choose 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, has $\mathrm{ord}_{s=1} L(E^D, s) \leq 1$, and for which ℓ is inert. The restriction to class number 1 is not essential.

8.1 Tables

Table 8.1: Rank 2 curves, discriminants, and primes for which we computed $z_{c,\sigma,\ell}$.

E	D	p	ℓ	E	D	p	ℓ	E	D	p	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

[1] All computations in this section can be done in Version 4.6.1 using the free open source software Sage [S+11]. Our implementation was peer reviewed by John Cremona for inclusion in Sage. Some relevant output files from running the computation can be found at `http://wstein.org/home/wstein/db/kolyconj/`. All computations were done under Linux (Ubuntu and Redhat) on several NSF-funded Sun Fire X4450 servers with 24 2.6Ghz cores and 128GB RAM each, at University of Washington and University of Georgia, and the computations took a few weeks CPU time.

We refer to elliptic curves using Cremona's notation (see [Crea]). Table 8.1 has columns E, D, p, 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 $p \mid \gcd(\ell+1, a_\ell(E))$. We selected these examples because the $\mathbb{Z}$-rank of $\mathrm{Div}(X_0(N)^{\mathrm{ss}}_{\mathbb{F}_{\ell^2}})$ is relatively small (the dimensions are in Table 8.2).

The Tamagawa numbers of all of our curves are 1 or 2, and in all cases $\rho_{E,p}$ is surjective (see Proposition 8.1).

Table 8.2 contains data about the points $z_{c,\sigma,\ell}$. The columns labeled E, D, p, and ℓ correspond exactly to the entries in Table 8.2. The column labeled dim gives the dimension of $\mathrm{Div}(X_0(N)^{\mathrm{ss}}_{\mathbb{F}_{\ell^2}})$; this dimension directly impacts the runtime of our implementation. The column labeled $\max c$ contains the largest c such that we managed to compute $z_{c,\sigma,\ell}$. The columns labeled "$= 0$" 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 generator σ (see below for how we chose 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.

A consistency check on Table 8.2 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 8.2 we find at least one c such that $z_{c,\ell} \neq 0$, so Conjecture 1.1 is true in these cases.

One initially surprising numerical observation we made is that the classes $\tau_{c,p}$ appear to *not* be equidistributed in the most naive possible sense. For example, in our computations with $p = 3$, the 0 subspace occurs about twice as much as any other subspace. Once we know that one class is nonzero, the exact asymptotic distribution of *all* classes can then be determined as an application of work of Mazur-Rubin, B. Howard [How04], and the Chebotarev density theorem. See the forthcoming paper [SW10]. As mentioned in Remark 7.1 above, this also leads to an alternate way to compute $\tau_{c,p}$ up to scaling. This provided an convincing double check on the correctness of our tables.

Tables 8.3–8.4 provide further details about the distribution of elements of

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

coming from this construction. The first 5 columns labeled E, D, p, ℓ_1 and ℓ_2 specify an elliptic curve, fundamental discriminant D, a prime p and two primes ℓ_1 and ℓ_2, chosen from the data summarized in Table 8.2. As mentioned above, the primes ℓ_1 and ℓ_2 are chosen so that the intersection of the two reduction maps to $E(\mathbb{F}_{\ell_i}) \otimes (\mathbb{Z}/p\mathbb{Z})$ is 0. Since the Selmer group has dimension 2 and in our implementation we chose the generator $\sigma \in \mathrm{Gal}(K_c/K_1) \cong (\mathcal{O}_K/c\mathcal{O}_K)^\times/(\mathbb{Z}/c\mathbb{Z})^\times$ to be $\sqrt{D} + n$ with $n \geq 1$ minimal, where $D = \mathrm{disc}(K)$. This allows us to deduce the subspace spanned by $\tau_{c,p}$ in $\mathrm{Sel}^{(p)}(E/\mathbb{Q})$ with respect to some unknown basis for $\mathrm{Sel}^{(p)}(E/\mathbb{Q})$. The column labeled $\tau_{c,p}$ gives the normalized generator for this subspace. The next column, labeled # gives the number of c such that $\tau_{c,p}$ spans the given subspace, and the last column gives the first few such primes c.

Table 8.2: Data about $z_{c,\sigma,\ell}$.

E	D	q	ℓ	dim	$\max c$	$=0$	$\neq 0$	c with $z_{c,\ell}=0$	c with $z_{c,\ell}\neq 0$
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 8.3: Data about normalized elements $\tau_{c,p} \in \mathrm{Sel}^{(q)}(E/\mathbb{Q})$ (part 1 of 2)

E	D	q	ℓ_1	ℓ_2	$\tau_{c,p}$	#	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 8.4: Data about normalized elements $\tau_{c,p} \in \mathrm{Sel}^{(q)}(E/\mathbb{Q})$ (part 2 of 2)

E	D	q	ℓ_1	ℓ_2	$\tau_{c,p}$	#	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 8.5: Data about **non-scaled** elements $\tau_{c,p} \in \mathrm{Sel}^{(q)}(E/\mathbb{Q})$ (part 1 of 2)

E	D	q	ℓ_1	ℓ_2	$\tau_{c,p}$	#	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 8.6: Data about **non-scaled** elements $\tau_{c,p} \in \mathrm{Sel}^{(q)}(E/\mathbb{Q})$ (part 2 of 2)

E	D	q	ℓ_1	ℓ_2	$\tau_{c,p}$	#	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

8.2 Appendix: remarks about surjectivity of Galois representations

In order to pass from $[P_{c,\sigma}]$ to $\tau_{c,p^n} \in \mathrm{H}^1(K, E[p^n])$ in Section 5.2, we assumed that p is an odd prime such that

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

is surjective. If we assume that E does not have CM (as will be the case for our examples), the p-adic representation $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ is surjective for all but finitely many p. Moreover, we can compute all primes p such that $\rho_{E,p}$ is not surjective, as explained in [GJP+09, §2.1] and implemented in Sage (see also forthcoming work of A. Sutherland [Sut09]). For example, we have the following proposition:

Proposition 8.1. *If E is a rank 2 elliptic curve with conductor < 1058, then $\rho_{E,p}$ is surjective for all odd primes p.*

Proof. Using the algorithm of [GJP+09, §2.1] as implemented in [S+11] shows that the mod-p representations $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ are surjective for all rank 2 curves E of conductor < 1058 and all primes p. As explained in [GJP+09, §2.1], this implies that the p-adic representation $\rho_{E,p}$ is surjective for $p \geq 5$.

It remains to deal with $p = 3$. For $p = 3$ we use the method of [Elk06], namely that it is enough to check that $j(E) - f(x)$ has no rational zero, where $f(x)$ is the function

$$f(x) = \frac{3^7 \cdot (x^2-1)^3 \cdot (x^6+3x^5+6x^4+x^3-3x^2+12x+16)^3 \cdot (2x^3+3x^2-3x-5)}{(x^3-3x-1)^9}$$

of degree 27 from [Elk06, pg. 5]. Elkies remarks (see [Elk10]) that there is a minus sign in the formula in [Elk06, pg. 5] that does not belong, as we verify by trying the integral specializations tabulated on [Elk06, pg. 7], and also by factoring $f - 1728$. Doing this computation for our curves yields the claimed result.

□

Remark 8.2. Andrew Sutherland used the techniques of [Sut09] to show [Sut10] that "the rank 2 elliptic curves with conductor less than 1058 all have surjective Galois images in $\mathrm{GL}_2(\mathbb{Z}/16\mathbb{Z})$." We thus also expect that $\rho_{E,2}$ is surjective for all rank 2 curves with conductor less than 1058.

Remark 8.3. The rank 2 curve 1058c1 has a rational 3 isogeny.

9 Related Projects

There are several future projects that are suggested by this paper, and we briefly sketch some of the most promising ones here.

We can do the same computations as we do here, but for modular abelian varieties A_f attached to newforms with $\mathrm{ord}_{s=1} L(f,s) \geq 2$. There is a table of such abelian varieties in [AS05]. For example, we carried out this computation for the modular abelian variety **1061b** of dimension 2 and indeed verified the natural higher dimensional analogue of Kolyvagin's conjecture for this abelian variety (for $p = 3$). Note that Kolyvagin appears to have never explicitly made such a conjecture, though of course

he considers modular abelian varieties in [KL89]. We could also use our method to show that $Ш(A_f/\mathbb{Q})[p] = 0$ for a particular A_f, even when $\operatorname{ord} L(f,s) \leq 1$. This may require extending Kolyvagin's structure theorem to abelian varieties, or otherwise making results of [KL89] more explicit.

We could verify Conjecture 1.1 for the rank 3 elliptic curve of conductor 5077, and possibly some other rank 3 curves. Indeed, Jennifer Balakrishnan and the author have verified Conjecture 1.1 at least for **5077a** for $p = 3$.

It would be of interest to generalize Algorithm 2.1 to treat the case p^n with $n > 1$ or the case when $\rho_{E,p}$ is reducible. We could also consider an example such as the rank 2 curve **916c1** and $p = 3$ in which p divides a Tamagawa number.

Since we are doing explicit computation, it would also be interesting to closely investigate the case $p = 2$; this is particularly exciting when $r_{\text{an}}(E/\mathbb{Q}) = 2$, since, after a harmless trace (as in Remark 5.7), we find that the points y_c, for c prime, are defined over **real quadratic** extensions of $\mathbb{Q}$, and define explicit elements of $\text{Sel}^{(2)}(E/\mathbb{Q})$ that define globally trivial [2]-coverings $X \to E$. For example, if we take E to be **389a**, $K = \mathbb{Q}(\sqrt{-7})$ and $c = 3$, then y_3 is defined over a cyclic degree 4 extension K_3 of K; the trace z_3 of y_3 to the quadratic subfield of K_3 is defined over the real quadratic field $\mathbb{Q}(\sqrt{21})$; it is the point

$$z_3 = \left(-\frac{131}{84}, \frac{1091}{3528}\sqrt{21} - \frac{1}{2}\right).$$

Also, we find that $0 \neq \tau_{3,2} = \delta((0,0)) \in \text{Sel}^{(2)}(E/\mathbb{Q})$. Is there any connection between these Heegner points over real quadratic fields and Stark-Heegner points?

Much of the work of Kolyvagin and Gross-Zagier has been generalized to totally real fields by Zhang and his students. Likewise, it would be of interest to see to what extent the results of this paper generalize to totally real fields.

It would also be of interest to investigate rank 2 curves E for which E^D exhibits some unusual behavior, e.g., nontrivial odd Ш or rank ≥ 3. For example, for E the curve **389a** of rank 2, and $K = \mathbb{Q}(\sqrt{-264})$, which has class number 8, the twist E^D has rank 3, so Kolyvagin's structure theorem implies that $[P_{c,\sigma}] = 0$ for all prime c, and it would be interesting to (a) computationally observe this, and (b) find a c that is a product of primes for which $[P_{c,\sigma}] \neq 0$. Similarly, if we take $K = \mathbb{Q}(\sqrt{-667})$, then K has class number 4 and $5 \mid \#Ш(E^D/\mathbb{Q})$; thus we expect that $[P_{c,5}] = 0$ for all prime c. Again it would beinteresting to observe this computationally, and find a prime c such that $[P_{c,5^2}] \neq 0$.

As a challenge, we could attempt to verify Conjecture 1.1 for the rank 4 elliptic curve of conductor 234446 given by the equation $y^2 + xy = x^3 - x^2 - 79x + 289$. This computation is at the edge of feasible, so it will require very sophisticated linear algebra or some other new idea.

References

[AS05] Agashe Agashe and William 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, `http://wstein.org/papers/shacomp/`. MR 2085902

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* **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

[BFH90] Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), no. 3, 543–618, http://wstein.org/papers/bib/bump-friedberg-hoffstein-nonvanishing.pdf. MR 1074487 (92a:11058)

[Bir65] B. J. Birch, *Conjectures concerning elliptic curves*, Proceedings of Symposia in Pure Mathematics, VIII, Amer. Math. Soc., Providence, R.I., 1965, http://wstein.org/papers/bib/Birch-Conjectures_Concerning_Elliptic_Curves.pdf, pp. 106–112. MR 30 #4759

[Bir71] B. J. Birch, *Elliptic curves over* $\mathbf{Q}$*: A progress report*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, R.I., 1971, http://wstein.org/papers/bib/Birch-Elliptic_curves_over_Q-A_Progress_Report.pdf, pp. 396–400.

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

[Bra10] Robert Bradshaw, *Provable Computation of Motivic L-functions*, University of Washington Ph.D. Thesis under William Stein (2010), http://www.sagemath.org/files/thesis/bradshaw-thesis-2010.pdf.

[BS10] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Preprint (2010), http://arxiv.org/abs/1006.1002.

[BS11] R. Bradshaw and W. A. Stein, *Heegner Points and the Arithmetic of Elliptic Curves over Ring Class Extensions*, Submitted (2011), http://wstein.org/papers/bs-heegner/.

[BY09] Jan Hendrik Bruinier and Tonghai Yang, *Faltings heights of CM cycles and derivatives of L-functions*, Invent. Math. **177** (2009), no. 3, 631–681, http://arxiv.org/abs/0807.0502. MR 2534103

[CFO+08] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves. I. Algebra*, J. Reine Angew. Math. **615** (2008), 121–155. MR 2384334 (2009g:11067)

[CLS09] J. Coates, Z. Liang, and R. Sujatha, *The Tate-Shafarevich group for elliptic curves with complex multiplication*, J. Algebra **322** (2009), no. 3, 657–674. MR 2531216 (2010e:11052)

[CLS10] ———, *The Tate-Shafarevich group for elliptic curves with complex multiplication II*, Preprint (2010), http://arxiv.org/abs/1005.4206.

[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)

[Cor02] Christophe Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), no. 3, 495–523, http://www.math.jussieu.fr/~cornut/papers/mcinv_published.pdf.

[Crea] J. E. Cremona, *Elliptic Curves Data*, `http://www.warwick.ac.uk/~masgaj/ftp/data/`.

[Creb] ———, `mwrank` *(computer software)*, `http://www.warwick.ac.uk/~masgaj/mwrank/`.

[Cre97] ———, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997, `http://www.warwick.ac.uk/~masgaj/book/fulltext/`.

[CS01] B. Conrad and W. A. Stein, *Component groups of purely toric quotients*, Math. Res. Lett. **8** (2001), no. 5-6, 745–766, `http://wstein.org/papers/compgrp/`. MR 2003f:11087

[ÇW08] Mirela Çiperiani and Andrew Wiles, *Solvable points on genus one curves*, Duke Math. J. **142** (2008), no. 3, 381–464, `http://www.ma.utexas.edu/users/mirela/solvable.pdf`. MR 2412044 (2009m:11092)

[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)

[Edi92] B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594, `http://www.math.leidenuniv.nl/~edix/public_html_rennes/publications/weight.html`.

[Elk06] Noam Elkies, *Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9*, Preprint (2006), `http://arxiv.org/abs/math/0612734`.

[Elk10] ———, *Email: surjective p-adic repn for some rank 2 curves*, Personal Communication (2010), `http://wstein.org/papers/bib/2010-elkies-3.txt`.

[Eme02] Matthew Emerton, *Supersingular elliptic curves, theta series and weight two modular forms*, J. Amer. Math. Soc. **15** (2002), no. 3, 671–714 (electronic), `http://www.math.northwestern.edu/~emerton/pdffiles/two.pdf`. MR 1896237 (2003b:11038)

[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)

[Gro87] ———, *Heights and the special values of L-series*, Number theory (Montreal, Que., 1985), CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, `http://wstein.org/papers/bib/Gross-Heights_and_the_Special_Values_of_L-series.pdf`, pp. 115–187. MR 894322 (89c:11082)

[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.

[GZ85] Benedict H. Gross and Don B. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220, http://wstein.org/papers/bib/gross-zagier-on_singular_moduli.pdf. MR 772491 (86j:11041)

[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

[How04] Benjamin Howard, *The Heegner point Kolyvagin system*, Compos. Math. **140** (2004), no. 6, 1439–1472, https://www2.bc.edu/~howardbe/Research/heegner.pdf. MR 2098397 (2006a:11070)

[JK10] Dimitar Jetchev and Ben Kane, *Equidistribution of Heegner Points and Ternary Quadratic Forms*, Preprint (2010), http://arxiv.org/abs/0908.3905.

[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)

[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, http://wstein.org/papers/bib/kolyvagin-logachev-finiteness_of_the_shafarevich-tate_group_and_the_group_of_rational_points_for_some_modular_abelian_varieties.pdf.

[Koh97] D. R. Kohel, *Computing modular curves via quaternions*, Fourth CANT Conference (1997), http://wstein.org/papers/bib/kohel-sydney.pdf.

[Koh01] David R. Kohel, *Hecke module structure of quaternions*, Class field theory—its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, http://wstein.org/papers/bib/kohel-hecke.pdf, pp. 177–195. MR 1846458 (2002i:11059)

[Kol88a] V. A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and $Ш(E, \mathbf{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671, http://wstein.org/papers/bib/kolyvagin-finitess_of_EQ_and_sha_for_a_subclass.pdf. MR 89m:11056

[Kol88b] ———, *The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 6, 1154–1180, 1327, http://wstein.org/papers/bib/kolyvagin-on_the_mw_and_sha_groups.pdf. MR 90f:11035

[Kol91] ———, *On the structure of Selmer groups*, Math. Ann. **291** (1991), no. 2, 253–259, http://wstein.org/papers/stein-ggz/references/kolyvagin-structure_of_selmer_groups/. MR 93e:11073

[Lan56] S. Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563, http://wstein.org/papers/bib/Lang-Algebraic_Groups_Over_Finite_Fields.pdf. MR 19,174a

[Lan87] ———, *Elliptic functions*, second ed., Graduate Texts in Mathematics, vol. 112, Springer-Verlag, New York, 1987, With an appendix by J. Tate. MR 890960 (88c:11028)

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

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978), http://archive.numdam.org/article/PMIHES_1977__47__33_0.pdf.

[McC91] W. G. McCallum, *Kolyvagin's work on Shafarevich-Tate groups*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, http://wstein.org/papers/bib/mccallum-kolyvagin.pdf, pp. 295–316. MR 92m:11062

[Mes86] J.-F. Mestre, *La méthode des graphes. Exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata) (1986), 217–242, See http://wstein.org/papers/rank4/mestre-fr.pdf and http://wstein.org/papers/rank4/mestre-en.pdf (English translation).

[Mil72] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190, http://wstein.org/papers/bib/Milne-On_the_Arithmetic_of_Abelian_Varieties.pdf. MR 48 #8512

[Mil86] ———, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

[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.

[MR04] Barry Mazur and Karl Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96. MR 2031496 (2005b:11179)

[Mum70] D. Mumford, *Abelian varieties*, Published for the Tata Institute of Fundamental Research, Bombay, 1970, Tata Institute of Fundamental Research Studies in Mathematics, No. 5.

[Piz80] A. Pizer, *An algorithm for computing modular forms on* $\Gamma_0(N)$, J. Algebra **64** (1980), no. 2, 340–390, http://wstein.org/papers/bib/pizer-algorithm_for_computing_modular_forms_on_gamma0.pdf.

[Pra95] Dipendra Prasad, *Ribet's theorem: Shimura-Taniyama-Weil implies Fermat*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), CMS Conf. Proc., vol. 17, Amer. Math. Soc., Providence, RI, 1995, http://wstein.org/papers/bib/prasad-ribets_theorem-shimura_taniyama_weil_implies_fermat.pdf, pp. 155–177. MR 1357211 (96j:11072)

[Rib88] Kenneth A. Ribet, *On the component groups and the Shimura subgroup of* $J_0(N)$, Séminaire de Théorie des Nombres, 1987–1988 (Talence, 1987–1988), Univ. Bordeaux I, Talence, 1988, `http://math.berkeley.edu/~ribet/Articles/bx_87.pdf`, pp. Exp. No. 6, 10. MR 993107 (91b:11070)

[Rib90a] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476, `http://math.berkeley.edu/~ribet/Articles/invent_100.pdf`.

[Rib90b] ———, *Raising the levels of modular representations*, Séminaire de Théorie des Nombres, Paris 1987–88, Birkhäuser Boston, Boston, MA, 1990, `http://math.berkeley.edu/~ribet/Articles/dpp.pdf`, pp. 259–271.

[Rib94] ———, *Report on mod* ℓ *representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Motives (Seattle, WA, 1991), Amer. Math. Soc., Providence, RI, 1994, `http://math.berkeley.edu/~ribet/Articles/motives.pdf`, pp. 639–676.

[Rib99] ———, *Torsion points on* $J_0(N)$ *and Galois representations*, Arithmetic theory of elliptic curves (Cetraro, 1997), Springer, Berlin, 1999, `http://math.berkeley.edu/~ribet/Articles/cime.pdf`, pp. 145–166. MR 2001b:11054

[Rib10] Kenneth A. Ribet, *Email: supersingular points on elliptic curves modulo* ℓ, Personal Communication (2010), `http://wstein.org/papers/bib/2010-ribet-eis.txt`.

[RS01] K. A. Ribet and W. A. Stein, *Lectures on Serre's conjectures*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, `http://wstein.org/papers/serre/`, pp. 143–232. MR 2002h:11047

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

[Ser88] J-P. Serre, *Algebraic groups and class fields*, Springer-Verlag, New York, 1988, Translated from the French.

[Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.

[ST68] J-P. Serre and J. T. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517, `http://wstein.org/papers/bib/Serre-Tate-Good_Reduction_of_Abelian_Varieties.pdf`.

[Ste09] William Stein, *Computational Number Theory Course Notes*, Unpublished (2009), `http://wiki.wstein.org/09/583e`.

[Ste10] William Stein, *Toward a Generalization of the Gross-Zagier Conjecture*, Internat. Math. Res. Notices (2010), `http://wstein.org/papers/stein-ggz/`.

[Sut09] Andrew Sutherland, *Computing the image of Galois representations attached to an elliptic curve*, Talk Slides (2009), `http://math.mit.edu/~drew/ImageOfGalois.pdf`.

[Sut10] ———, *Email: surjective p-adic repn for some rank* 2 *curves*, Personal Communication (2010), http://wstein.org/papers/bib/2010-sutherland-16.txt.

[SW02] William Stein and Mark Watkins, *A database of elliptic curves—first report*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, http://wstein.org/ecdb, pp. 267–275. MR 2041090 (2005h:11113)

[SW10] William Stein and Jared Weinstein, *Kolyvagin classes on elliptic curves: structure, distribution, and algorithms*, In preparation (2010).

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

[Tat66] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1965/66, http://wstein.org/papers/bib/tate-bsd.pdf, pp. Exp. No. 306, 415–440.

[Vat02] V. Vatsal, *Uniform distribution of Heegner points*, Invent. Math. **148** (2002), no. 1, 1–46, http://www.math.ubc.ca/~vatsal/research/uniform3.pdf. MR 1892842 (2003j:11070)

[Voi] John Voight, *Identifying the matrix ring: algorithms for quaternion algebras and quadratic forms*, Submitted, http://arxiv.org/abs/1004.0994 or http://www.cems.uvm.edu/~voight/articles/quatalgs-040110.pdf.

[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.

[YZZ11] X. Yuan, S. Zhang, and W. Zhang, *Triple product L-series and Gross-Schoen cycles I: split case*, Preprint (2011), http://www.math.columbia.edu/~yxy/preprints/triple.pdf.

[Zha01] 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)

[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