EXPLICIT REALIZATION OF ELEMENTS OF THE TATE-SHAFAREVICH GROUP CONSTRUCTED FROM KOLYVAGIN CLASSES

LAZAR RADIČEVIĆ

Abstract. We consider the Kolyvagin cohomology classes associated to an elliptic curve E over $\mathbb{Q}$ from a computational point of view. We explain how to go from a model of a class as an element of $(E(L)/pE(L))^{\mathrm{Gal}(L/\mathbb{Q})}$, where p is prime and L is a dihedral extension of $\mathbb{Q}$ of degree $2p$, to a geometric model as a genus one curve embedded in $\mathbb{P}^{p-1}$. We adapt the existing methods to compute Heegner points to our situation, and explicitly compute them as elements of $E(L)$. Finally, we compute explicit equations for several genus one curves that represent non-trivial elements of $Ш(E/\mathbb{Q})[p]$, for $p \leq 11$, and hence are counterexamples to the Hasse principle.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, with a fixed modular parametrization $\phi : X_0(N) \to E$. Let K be an imaginary quadratic field satisfying the Heegner hypothesis, that is, all prime factors of N split in K. Let H be the Hilbert class field of K. Using the theory of complex multiplication and the modular parametrization ϕ, one defines certain points in $E(H)$, known as the Heegner points.

Let us fix an odd prime p. Kolyvagin ([Kol89]) has used Heegner points to construct certain cohomology classes in the p-Selmer group $\mathrm{Sel}^p(E/\mathbb{Q})$. The images of these classes in the Tate-Shafarevich group $Ш(E/\mathbb{Q})[p]$ under the natural map $\mathrm{Sel}^p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p]$ are known as the Kolyvagin classes. Elements of $Ш(E/\mathbb{Q})[p]$ can be represented by genus one curves embedded in $\mathbb{P}^{p-1}$.

The main result of this paper is an algorithm (divided into Algorithm 5.1 and Algorithm 3.2) to compute such representations for the Kolyvagin classes in $Ш(E/\mathbb{Q})[p]$, and thus obtain explicit counter examples to the Hasse principle. In Section 6 we then use these algorithms to compute explicit equations for smooth genus curves embedded in $\mathbb{P}^{p-1}$, that have points over every completion of $\mathbb{Q}$, but no points defined over $\mathbb{Q}$ for primes $p \leq 11$.

These calculations are especially interesting if $p > 5$, and the curve E does not admit a p-isogeny. The standard method to compute such counter examples to the Hasse principle is to use the method of complete p-descent to compute the entire p-Selmer group $\mathrm{Sel}^{(p)}(E/\mathbb{Q})$. However, when $p > 5$, this is not feasible in practice, as one runs into difficulties with computing class groups of very large number fields. Our method does not run into this problem, and in particular,

Date: 16th November, 2021.

in Section 6, Example 6.3, we compute the first known explicit realization of a non-trivial element of $Ш(E/\mathbb{Q})[7]$ for an elliptic curve E that does not have a 7-isogeny.

These classes have already been studied from a computational point of view by Jetchev, Leuter and Stein in [JLS09]. They are able to compute representations of these classes as elements of $E(L)/pE(L)$, where L is a certain abelian extension of K. However, their aim is only to test whether these classes are non-zero, for which this representation is sufficient, whereas we compute explicit equations defining the corresponding homogeneous space.

The problem of computing these equations breaks up into two problems. First, given a suitable elliptic curve E, a discriminant D and a prime p, we compute a Heegner point x_K, defined over a certain dihedral extension of $\mathbb{Q}$. Our method for doing this is Algorithm 3.2. To this point we associate a Kolyvagin class $c \in \mathrm{Sel}^{(p)}(E/\mathbb{Q})$. Algorithm 5.1 then represents this class by a genus one curve $C \subset \mathbb{P}^{p-1}$. The main difficulty in our computations is caused by the fact that typically the Heegner points x_K have very large height, making them hard to compute and work with. We note that despite this, the output of Algorithm 5.1 is a model for the curve C with small integral coefficients, i.e. a *minimized* and *reduced* model, in the sense of [CFS10].

Acknowledgements. I am deeply grateful to my PhD advisor Tom Fisher, for suggesting the problem to me and for his patient guidance along the way. I would also like to thank Jack Thorne and Vladimir Dokchitser for their helpful comments. Finally, I thank Trinity College and Max Planck Institute for Mathematics for their financial support.

2. Background on Kolyvagin classes and statement of results

In this section we review basic material from the theory of Heegner points. The main references are the articles of Gross, [Gro91] and [Gro84], as well as [Wes15], [Wat05] and Chapter 8 of [Coh08].

2.1. **Heegner points on modular curves.** For $N \geq 1$ an integer, let $Y_0(N)$ be the open modular curve, defined over $\mathbb{Q}$. The $\mathbb{C}$-points of $Y_0(N)$ classify isomorphism classes of cyclic N-isogenies $E \to E'$, defined over $\mathbb{C}$. Fix an imaginary quadratic field K satisfying the Heegner hypothesis: every prime dividing N splits completely in K. It follows that there exists an ideal $\mathcal{N}$ of the ring of integers $\mathcal{O}_K$ with $\mathcal{N}\bar{\mathcal{N}} = N\mathcal{O}_K$, and hence $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$.

Given such an ideal $\mathcal{N}$, an ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_K)$ determines an a map of complex torii $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$. Since we have $\mathfrak{a}\mathcal{N}^{-1}/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}$, this map is a cyclic N-isogeny, and determines a point in $Y_0(N)(\mathbb{C})$. We say this is the Heegner point associated to the triple $(\mathcal{O}_K, [\mathfrak{a}], \mathcal{N})$.

2.2. **Rationality of Heegner points.** A key property of Heegner points, implied by the theory of complex multiplication, is that they are defined over abelian extensions of the field K. More precisely, let $(\mathcal{O}_K, [\mathfrak{a}], \mathcal{N})$ be a Heegner point on $Y_0(N)$. This point is defined over the Hilbert class field H of K. See §5 of [Gro84]. The key point is that both $\mathbb{C}/\mathfrak{a}$ and $\mathbb{C}/\mathfrak{a}\mathcal{N}^{-1}$ have complex

multiplication by $\mathcal{O}_K$. This is a consequence of the Shimura reciprocity law, as explained in Chapter 6.8 of [Shi71], or Chapter II of [Sil94].

The field H is an abelian extension of K, and the Artin map provides a canonical isomorphism $F : \mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Gal}(H/K)$. Explicitly, by Shimura reciprocity, for an ideal class $[\mathfrak{b}]$ we have

$$(\mathcal{O}_K, [\mathfrak{a}], \mathcal{N})^{F([\mathfrak{b}])} = (\mathcal{O}_K, [\mathfrak{a}\mathfrak{b}^{-1}], \mathcal{N}).$$

Suppose that $\tau \in \mathrm{Gal}(H/\mathbb{Q})$ is a lift of complex conjugation. The action of τ is given by

$$(\mathcal{O}_K, [\mathfrak{a}], \mathcal{N})^{\tau} = (\mathcal{O}_K, [\tau(\mathfrak{a})], \tau(\mathcal{N})).$$

2.3. **Heegner points on elliptic curves and Kolyvagin classes.** Now let E be an elliptic curve defined over $\mathbb{Q}$, of conductor N. Let $X_0(N)$ be the compactified modular curve of level N. By the modularity theorem (see [BCDT01]), there exists a modular parametrization map $\phi : X_0(N) \to E$. For every discriminant D that satisfies the Heegner condition, we fix an ideal $\mathcal{N}$ with $N\mathcal{O}_K = \mathcal{N}\bar{\mathcal{N}}$, and define the Heegner point $x_K \in E(H)$ by setting $x_K = \phi(\mathcal{O}, [\mathfrak{a}], \mathcal{N})$. We also define the basic Heegner point $y_K \in E(K)$ by setting $y_K = \mathrm{Tr}_{H/K} x_K$.

Let $p > 2$ be a prime such that $E(H)[p]$ is trivial, $y_K \in pE(K)$ and p divides $|\mathrm{Cl}(\mathcal{O}_K)| = |H : K|$ exactly once. These assumptions are fairly mild, as we will see later. Then there exists a unique degree p subfield of H, which we denote by L. Let $z_D = \mathrm{Tr}_{H/L} x_D$, and let σ be a generator of $G = \mathrm{Gal}(L/K)$. Now define the operators D_σ and Tr in $\mathbb{Z}[G]$ by

$$D_\sigma = \sum_{i=1}^{p-1} i\sigma^i, \quad \mathrm{Tr} = \sum_{i=0}^{p-1} \sigma^i.$$

The operator D_σ is known as the *Kolyvagin derivative* and Tr is just the trace operator. They satisfy the identity

$$(\sigma - 1)D_\sigma = p - \mathrm{Tr},$$

We now define the *derived* Heegner point P as $P = D_\sigma \cdot z_K$. The class $[P] \in E(L)/pE(L)$ is invariant under the action of G, since we have

$$(\sigma - 1)(D_\sigma \cdot z_K) = pz_K - \mathrm{Tr}(z_K) = pz_K - \mathrm{Tr}_{H/K}(x_K) = pz_K - y_K,$$

and by assumption $y_K \in pE(K)$. The Kummer map $\delta : E(L)/p(L) \to H^1(L, E[p])$ is Galois equivariant, and so we can define a cohomology class $c_L \in H^1(L, E[p])^{\mathrm{Gal}(L/K)}$ by $c_L = \delta([P])$. We have the inflation-restriction exact sequence

$$H^1(L/K, E[p](L)) \xrightarrow{\inf} H^1(K, E[p]) \xrightarrow{\mathrm{res}} H^1(L, E[p])^{\mathrm{Gal}(L/K)} \to H^2(L/K, E[p](L)).$$

As $E[p](L)$ is trivial, the two outermost groups are trivial, and the restriction map defines an isomorphism $\mathrm{res} : H^1(K, E[p]) \to H^1(L, E[p])^{\mathrm{Gal}(L/K)}$. We define $c \in H^1(K, E[p])$ to be the preimage of c_L under the restriction map. The class c is in fact an element of the p-Selmer group

$\mathrm{Sel}^{(p)}(E/K)$, see Prop. 6.2 of [Gro91]. Finally, let d be the image of c in $H^1(K, E)$. Then d is an element of $Ш(E/K)[p]$.

2.4. **Descent from K to $\mathbb{Q}$.** Let ϵ be the sign of the functional equation of $E/\mathbb{Q}$. The proof of Proposition 5.4 in [Gro91] shows that the class c lies in the ϵ-eigenspace for the action of complex conjugation on $H^1(K, E[p])$. Thus, if E is a curve of rank 0, c is fixed by complex conjugation, and by the same inflation-restriction argument we naturally obtain an element of $H^1(\mathbb{Q}, E[p])$, which we will also call c.

As E has no non-trivial p-torsion and rank 0, the group $E(\mathbb{Q})/pE(\mathbb{Q})$ is trivial, and hence if c is non-zero, its image d in $H^1(K, E[p])$ will be a non-trivial element of $Ш(E/\mathbb{Q})[p]$. Tracing through the isomorphisms used to define c, we see that the class c is non-zero if and only if the point P is not divisible by p in $E(L)$.

2.5. **Galois cohomology and n-diagrams.** Let F be a number field, E/F an elliptic curve and $n \geq 1$ an integer. We briefly recall a few standard facts about the Galois cohomology groups $H^1(F, E)$ and $H^1(F, E[n])$, see for example [CFO+08].

A torsor under E is a smooth projective curve C/F, together with a regular simply transitive action of E on T. An isomorphism of torsors C_1 and C_2 is an isomorphism of curves C_1 and C_2 that respects the action of E. The left action of E on itself by translations makes E a torsor, which we call the trivial torsor. There is a natural identification of the group $H^1(F, E)$ with the set of isomorphism classes of torsors defined over F, and the trivial torsor E corresponds to the identity element.

We will also need the following interpretation of the group $H^1(F, E[n])$. We define a diagram $[C \to S]$ to be a morphism from a torsor C to a variety S. An isomorphism of diagrams $[C_1 \to S_1] \sim [C_2 \to S_2]$ is an isomorphism of torsors $\phi : C_1 \cong C_2$ together with an isomorphism of varieties $\psi : S_1 \cong S_2$ making the diagram

$$\begin{array}{ccc} C_1 & \longrightarrow & S_1 \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ C_2 & \longrightarrow & S_2 \end{array}$$

commute. We define the trivial n-diagram to be the diagram $[E \to \mathbb{P}^{n-1}]$ where the morphism is induced by the complete linear system of the divisor $n \cdot 0_E$, and in general, we say a diagram $[C \to S]$ is an n-diagram if it is defined over F, but isomorphic to the trivial diagram over the algebraic closure $\bar{F}$, i.e. a twist of the trivial diagram. The set of isomorphism classes is also naturally identified with $H^1(F, E[n])$.

The group law on E induces a map $\sum : \mathrm{Div}E \to E$, given by $\sum n_p \cdot (P) \mapsto \sum n_p P$. The Kummer map $\delta : E(F)/nE(F) \to H^1(F, E[n])$ sends a class $[P] \in E(F)/nE(F)$ to the isomorphism class

of the n-diagram $[E \to \mathbb{P}^{n-1}]$, where the map is induced by the complete linear system of any degree degree n divisor D with $\mathrm{sum}(D) = P$.

In this article we consider only n-diagrams of the form $[C \to \mathbb{P}^{n-1}]$. When $n \geq 3$, such an n-diagram is a closed embedding, and its image is a smooth projectively normal curve C of genus one and degree n. If $n = 3$, C is a plane cubic. For $n \geq 4$, the ideal defining C is generated by $n(n-3)/2$ quadrics. Finally, as a consequence of class field theory, under the above identification, the elements of the n-Selmer group of E can be represented by n-diagrams of the form $[C \to \mathbb{P}^{n-1}]$.

2.6. **Summary of the setup and the statement of results.** Our starting data is an elliptic curve $E/\mathbb{Q}$ of rank 0 and an odd prime p for which the Birch and Swinnerton-Dyer conjecture predicts that the group $Ш(E/\mathbb{Q})[p]$ is non-trivial. To construct a Kolyvagin class, we also need to find a discriminant D of an imaginary quadratic field K with Hilbert class field H that satisfies the following: D satisfies the Heegner hypothesis, $E(H)[p]$ is trivial, p divides $|\mathrm{Cl}(\mathcal{O}_\mathcal{K})| = |H : K|$ exactly once, the rank of E/K is 0, and the basic Heegner point y_K is divisible by p in $E(K)$.

Remark 2.1. For given E and p, it is usually easy to find a discriminant D that satisfies these conditions by a naive search. In practice, a naive search will usually find plenty of discriminants that are easily seen to satisfy all conditions but the last one, and a famous theorem of Kolyvagin (Theorem 1.3 of [Gro91]) then often guarantees that we must have $p|y_K$.

Starting from the data of E, p and D, we compute a p-diagram representing the Kolyvagin class $c \in \mathrm{Sel}^{(p)}(E/\mathbb{Q})$ defined above. There are two main steps. Algorithm 3.2 computes the Heegner point x_K as an element of $E(H)$, and using this data Algorithm 5.1 then computes the equations defining a genus one normal curve $C \subset \mathbb{P}^{n-1}$, and the inclusion $C \subset \mathbb{P}^{p-1}$ is the p-diagram representing the class c. If this class is non-trival, the curve C is a counter-example to the Hasse principle. We were able to succesfully use these algorithms for various elliptic curves with $p = 3, 5$ and 7, and we give examples in Section 6. Note that the examples with $p = 3$ and $p = 5$ can also be obtained by the method of p-descent, but Example 6.3 with $p = 7$ is out of reach of p-descent at the moment, and is the first such example to our knowledge.

Remark 2.2. If the curve E has rank 1 over $\mathbb{Q}$, then the class d is in the (-1)-eigenspace of complex conjugation, and hence is obtained as the restriction of an element of $Ш(E_D/\mathbb{Q})[p]$, where E_D is the quadratic twist of E by D. If this quadratic twist has rank 0, then by the same argument, the class d is non-zero if and only if the class c is.

Our method applies in this case as well, and in fact we are able to compute an example (Example 6.4) with $p = 11$, i.e. a genus one normal curve $C \subset \mathbb{P}^{10}$ that is a counter-example to the Hasse principle. We suspect that p could be increased even further - in this case, computing the Heegner point appears to be much easier. Note that in this case, as the Kolyvagin class is naturally an element of $Ш(E_D/\mathbb{Q})$ for the quadratic twist E_D of the curve E we begin with, it seems difficult to use this version of our method as a tool to compute $Ш(E/\mathbb{Q})[p]$ of a given curve E.

3. Computing the Heegner point

In this section we describe the algorithm we will use to compute the Heegner points needed to define the Kolyvagin class.

3.1. **Computing the modular parametrization.** We briefly recall how to compute a modular parametrization of an elliptic curve, following [Coh08] and [JLS09]. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, p an odd prime, and let K be an imaginary quadratic field. We assume that the maximal order $\mathcal{O}_K$ of K is of discriminant $-D \neq 3, 4$ and that K satisfies the Heegner hypothesis: all prime factors of N split completely in $\mathcal{O}_K$. We fix an ideal $\mathcal{N}$ with $N\mathcal{O}_K = \mathcal{N}\bar{\mathcal{N}}$. Let H be the Hilbert class field of K, and fix a modular parametrization $\phi : X_0(N) \to E$ that maps the cusp ∞ to the origin of E. We assume that H has unique subfield of degree p over K, denoted L. The Heegner point x_K is defined to be the image $x_K = \phi(\mathcal{O}_K, [\mathcal{O}_K], \mathcal{N}) \in E(H)$, and we set $z_K = \mathrm{Tr}_{H/L} x_K$.

Following [JLS09], we give an explicit description of the map ϕ. Let Λ be the period lattice associated to E, and let $f \in S_2(\Gamma_0(N))$ be the newform associated to E. Let $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ be the extended upper half plane, and identify the modular curve $X_0(N)$ with the quotient $\mathcal{H}^*/\Gamma_0(N)$. The modular parametrization map $\phi : X_0(N) \to \mathbb{C}/\Lambda$ is given by integrating the holomorphic differential $f(z)dz$ on $X_0(N)$. We can compute it using the power series

$$\phi(\tau) = \int_\tau^\infty f(z)dz = \sum_{n \geq 1} \frac{a_n}{n} e^{2\pi i n \tau}, \tag{1}$$

where $f = \sum_{n \geq 1} a_n q^n$ is the Fourier expansion of f. To obtain a parametrization $X_0(N) \to E$, we compose with the uniformization $\psi = \mathbb{C}/\Lambda \to E(\mathbb{C})$. The map ψ is defined using the Weierstrass $\wp$-function, and is is easy to compute numerically to high precision.

The Artin map provides us with an isomorphism between the class group $\mathrm{Cl}(\mathcal{O}_K)$ and the Galois group $\mathrm{Gal}(L/K)$. We first compute a set of representatives $\mathfrak{a}_1, ..., \mathfrak{a}_m$ for Cl_K. Let σ_i be the image of $\mathfrak{a}_i$ under the Artin map. As explained in Section 2, the Galois conjugates of the point x corresponding to the isogeny $[\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}^{-1}]$ are given by

$$\sigma_i(x) = [\mathbb{C}/\mathfrak{a}_i^{-1} \to \mathbb{C}/\mathfrak{a}_i^{-1}\mathcal{N}^{-1}]. \tag{2}$$

For every conjugate we then compute a corresponding point τ in the upper half plane. Now fix an embedding i of L into $\mathbb{C}$. As the morphism ϕ is defined over $\mathbb{Q}$, we can use the above description of the Galois action to compute the coordinates of the Galois conjugates $\sigma_i(x_K)$, to whatever precision we like, and then do the same for the point $z_K = \mathrm{Tr}_{H/L} x_K$.

3.2. **Recognizing the Heegner point using lattice reduction.** We now discuss how to use the LLL algorithm to recover the point z_K from the data computed in the previous section. Recognizing an algebraic number from floating point approximations is a well-studied problem, and in the setting of Heegner points has been considered in [JLS09]. An algorithm similar to

the one they propose has been implemented in MAGMA by Steve Donnelly. For our purposes however, their method is too slow to handle the case when $p \geq 5$, so in this section we propose a variant to this method that seems to work quite well in this setting.

Let L be a number field of degree n, with n complex embeddings $\sigma_1, \ldots, \sigma_n$, and let $\alpha_1, ..., \alpha_n$ be a $\mathbb{Z}$-basis of the ring integers $\mathcal{O}_L$.

Definition 3.1. Let $\epsilon > 0$, $C = 10^B$ for an integer $B > 0$, L and let $z_1, ..., z_n \in \mathbb{C}$ be such that $|\sigma_i(z) - z_i| < \epsilon$. Let $\alpha_{ij} \in \mathbb{C}$ be such that $|\sigma_j(\alpha_i) - \alpha_{ij}| < \epsilon$. To this data we associate the $2n \times 3n$ integer matrix $A_{z,\epsilon,C}$:

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & 0 & \lfloor C\alpha_{1,1} \rfloor & \ldots & \lfloor C\alpha_{1,2p} \rfloor \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ldots & \vdots \\ \vdots & \vdots & \ldots & \vdots & \vdots & \lfloor C\alpha_{1,1}z_1 \rfloor & \ldots & \lfloor C\alpha_{1,2p}z_{2p} \rfloor \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 1 & \lfloor C\alpha_{2p,1}z_1 \rfloor & \ldots & \lfloor C\alpha_{2p,2p}z_{2p} \rfloor \end{pmatrix}$$

i.e. the left $2n \times 2n$-block is the $2n \times 2n$ identity matrix, and the right $2n \times n$-second block splits into the upper $n \times n$ block $(\lfloor C\alpha_{ij} \rfloor)_{ij}$ and the lower $n \times n$ block $(\lfloor C\alpha_{ij}z_j \rfloor)_{ij}$. We define $L_{z,\epsilon,C}$ to be the lattice in $\mathbb{R}^{3n}$ spanned by the rows of $A_{z,\epsilon,C}$.

To recover z from $A_{z,\epsilon,C}$, our strategy will be to use the LLL lattice reduction algorithm to find short vectors in the lattice $L_{z,\epsilon,C}$. We will take $C = 10^B$ to be a large constant and ϵ as small as possible. Let the rows of $A_{z,\epsilon,C}$ be $r_1, r_2, ..., r_{4p}$. The lattice reduction algorithm gives us integers $u_1, u_2, ..., u_{4p}$ such that the row vector $\sum_{i=1}^{4p} u_i r_i$ is "small", and if ϵ is small enough, we hope that we will have

$$0 = u_1\alpha_1 + u_2\alpha_2 + ... + u_2p\alpha_{2p} + u_{2p+1}\alpha_2 z + u_{2p+2}\alpha_2 z + ... + u_{4p}\alpha_{2p}z,$$

i.e.

$$z = -\frac{\sum_{i=1}^{2p} u_i\alpha_i}{\sum_{i=1}^{2p} u_{2p+i}\alpha_i}.$$

and hence recover z from the matrix $A_{z,\epsilon,C}$. We summarise the discussion of this section in the following algorithm.

Algorithm 3.2.

- INPUT: An elliptic curve E, a Heegner discriminant D, and a prime p that divides $|\mathrm{Cl}(\mathcal{O}_K)|$ exactly once.
- OUTPUT: Coordinates (x, y) of a point $P \in E(L)$ that is (conjecturally) the point $z_K = \mathrm{Tr}_{H/L} x_K$.

(i) Find a set of representatives $\mathfrak{a}_1, \mathfrak{a}_2, ...\mathfrak{a}_n$ for the class group $\mathrm{Cl}(K)$, and for each point $[\mathbb{C}/\mathfrak{a}_i^{-1} \to \mathbb{C}/\mathfrak{a}_i^{-1}\mathcal{N}^{-1}]$, compute a corresponding τ_i in the upper half plane.

(ii) Compute an integral basis of the maximal order $\mathcal{O}_L$.

(iii) Pick an $\epsilon > 0$, and compute $\phi(\tau_i) \in \mathbb{C}$ to precision $\epsilon/2$, using the formula (1), by computing enough of the Fourier coefficients a_n.

(iv) Compute the period lattice Λ and hence the uniformisation map $\psi : \mathbb{C}/\Lambda \to E$ to the required precision, and hence find $\psi(\phi(\tau_i))$. Then use the description of the Galois action on Heegner points 2, to take the trace from H to L, and hence obtain $z_1, ..., z_{2p}$ with $|\sigma_i(x) - z_i| < \epsilon$.

(v) Using $z_1, z_2, ..., z_{2p}$ and choosing a large C, form the matrix $A_{z,\epsilon,C}$ as in Definition 3.1. Use the LLL algorithm to find a $U \in \mathrm{SL}_{4p}(\mathbb{Z})$ such that the rows of $UA_{z,\epsilon,C}$ form an LLL-reduced basis of $L_{z,\epsilon,C}$. Then let $x = -\frac{\sum_{i=1}^{2p} u_{1,i}\alpha_i}{\sum_{i=1}^{2p} u_{1,2p+i}\alpha_i}$ and test if x is the x-coordinate of a point in $E(L)$. If it is, solve for the y-coordinate and return (x, y). Otherwise, replace ϵ by $\epsilon/2$, and return to Step 3.

Steps (i), (ii) and (iii) of the algorithm have been studied extensively in the literature, see for example Section 8.6 of [Coh08] or [Wat05], so we do not provide details on how to implement them. We have used the existing MAGMA implementations of these steps in our calculations. The algorithm has not proven that the point (x, y) is indeed the point x_K, although we believe it is highly improbable that it isn't, nor have we proven that it always terminates. However, in practice we have been able to use it to compute points on various for $p \leq 11$.

The main bottleneck is Step 3. If the height of the Heegner point is very large, then we may need to take ϵ very small for the algorithm to return a point in $E(L)$, and this might require computing a very large number of the Fourier coefficients a_n.

Remark 3.3. The output of our algorithm, if it terminates, will be a point $u = (x', y') \in E(H)$, and as noted in [JLS09], verifying that this point coincides with the Heegner point $z_K = (x, y)$ is a nontrivial matter. We know that the point we obtain is a good Archimedean approximation of the Heegner point, in the sense that by increasing the precision in Algorithm 3.2 we can make the absolute values $|\sigma(x) - \sigma(x')|$, where σ is any embedding $L \hookrightarrow \mathbb{C}$, as small as we like. However, without a bound on the height of z_K, we can't actually prove that $u = z_K$.

Since our main goal is to construct examples of non-trivial elements of the Tate-Shafarevich group of E, it suffices to verify that the point u satisfies the same properties as the Heegner point z_K for the purpose of constructing a Kolyvagin class, as formalized in Lemma 4.2. This also serves as a consistency check on our calculations, and in all of the examples we have computed, we believe it is very unlikely that the resulting point is not the Heegner point. Note that the appendix of [JLS09] provides a method one could use to compute a bound on the height of x_K and hence make the calculations provably correct, but we did not implement this algorithm.

Remark 3.4. The idea to use the LLL-algorithm method to recover z from the matrix $A_{z,\epsilon,C}$ is very well known. Our approach differs from a standard method, as explained in, for example Chapter 7

of [Han09], and also used in [JLS09]. Briefly, the standard method to recover an algebraic number z from a set of complex numbers $\{z_g : g \in G\}$ that approximate Galois conjugates of z is to approximate the minimal polynomial f of z by $\prod_{g\in G}(x - z_g)$, and try to recognize the coefficients of f as rationals, using continued fractions, or better yet the LLL algorithm. However, for us this method is not efficient enough, since z is of very large height in examples we consider, and the coefficients of polynomial f are symmetric polynomials in z_g, and hence are of even larger height.

We instead take advantage of the fact that we know that x is defined over the Hilbert class field H, which one can compute very quickly using standard methods of computational class field theory.

Moreover, to use lattice reduction, one needs to represent elements of L by tuples of rational numbers, and heuristically, we expect that LLL will work better if these numbers are of small height, so that the corresponding lattice is less complicated. In the standard method, one uses the coefficients of the minimal polynomial, and another natural method would be to identify $L \cong \mathbb{Q}^{2p}$ by choosing a basis of L. The coefficients of z in both of these representations can be obtained from an expression $z = \frac{\sum u_i\alpha_i}{\sum v_i\alpha_i}$ by clearing the denominator, and so will usually be much larger.

Remark 3.5. A further improvement along the same lines is to use the fact that we can also compute numerically the y-coordinate, and look for linear relations of the form $A + Bx + Cy = 0$. Recall that we have assumed that L is of class number 1, so that $x = r/t^2$ and $y = s/t^3$, for some $r, s, t \in \mathcal{O}_L$. Thus if $A + Bx + Cy = 0$, we see that $t|A$, and that hence $A^2x \in \mathcal{O}_L$. It is then simple to recover A^2x from its floating point approximation, and hence compute the point (x, y). Based on experimental data we have computed, this seems to be an improvement. A heuristic explanation might be that the minimal A, B, C that can appear in a relation $A + Bx + Cy = 0$ can be a lot smaller than the minimal u, v appearing in a relation $u + vx = 0$, and so it is easier to guess a short vector in the corresponding lattice.

4. Geometric realization of the Kolyvagin class

4.1. **The p-diagram associated to the Kolyvagin class.** In this section we explain how to compute, given a Heegner point, equations for the p-diagram representing the Kolyvagin class. We first formalize the input we need from Heegner points.

Throughout this section, we fix the following data. Let $E/\mathbb{Q}$ be an elliptic curve of rank 0, let p be an odd prime and $K/\mathbb{Q}$ be a quadratic field. In addition, let $L/\mathbb{Q}$ be a dihedral extension, of degree $2p$, that contains K, such that $E(L)[p]$ is trivial.

Proposition 4.1. *Let $P \in E(L)$ be a point such that the class $[P] \in E(L)/pE(L)$ is invariant under the action of $G = \mathrm{Gal}(L/\mathbb{Q})$. Let $\delta : E(L)/pE(L) \to H^1(L, E[p])$ be the Kummer map, and let $\mathrm{res} : H^1(\mathbb{Q}, E[p]) \to H^1(L, E[p])$ be the restriction map.*

Then there exists a unique class $c \in H^1(\mathbb{Q}, E[p])$ such that $\mathrm{res}(c) = \delta([P])$.

Proof. This is the inflation-restriction argument from Section 2. □

The aim of this section is to give method to compute equations for the p-diagram representing the class c. This is accomplished by Galois descent, and involves explicit cocycle calculations. Let $\sigma \in G$ be an element of order p, and let $\tau \in G$ be an involution.

Lemma 4.2. *Let $P \in E(L)$ be a point with $[P] \in (E(L)/pE(L))^G$, and suppose that we also have $\tau(P) = P$. We then have the following.*

(i) For each $g \in G$, there exists a unique $R_g \in E(L)$ with $pR_g = g(P) - P$. The map $g \mapsto R_g$ defines a cocycle in $H^1(G, E(L))$, meaning that for any $g, h \in G$ we have

$$R_{gh} = g(R_h) + R_g,$$

(ii) For $0 \leq k \leq p-1$, we have $R_{\sigma^k} = \sum_{i=1}^{k} \sigma^{i-1}(R_\sigma)$, and $R_{\sigma^k \tau} = R_{\sigma^k}$.

(iii) We have $\sum_{k=1}^{p} \sigma^k(R_\sigma) = 0_E$ and $\tau(R_{\sigma^k}) = R_{\sigma^{p-k}}$.

(iv) We have $[P] = [D_\sigma R_\sigma] = [\sum_{i=1}^{p-1} i\sigma^i(R_\sigma)] = [\sum_{i=1}^{p-1} R_{\sigma^i}] \in E(L)/pE(L)$.

Proof. Since $[g(P)] = [P] \in E(L)/pE(L)$ for every $g \in G$, there exists $R_g \in E(L)$ with $pR_g = g(P) - P$. Since $E(L)$ is trivial, R_g is unique, and the cocycle condition follows from

$$pR_{gh} = gh(P) - P = g(h(P) - P) + g(P) - P = pg(R_h) + pR_g = p(g(R_h) + R_g),$$

proving (i). Parts (ii) and (iii) then follow from (i) and the identity $\sigma^{p-k}\tau = \tau\sigma^k$. For (iv), using (ii) we see that

$$\sum_{i=1}^{p-1} R_{\sigma^i} = \sum_{i=1}^{p-1} \sum_{j=1}^{i} \sigma^{j-1}(R_\sigma) = \sum_{i=1}^{p-1} i\sigma^i(R_\sigma) = D_\sigma R_\sigma.$$

The identity $(\sigma - 1) \cdot D_\sigma = p - \sum_{i=1}^{p} \sigma^i$ and (iii), we have $\sigma(D_\sigma R_\sigma) - D_\sigma R_\sigma = pR_\sigma - \sum_{i=1}^{p} \sigma^i(R_\sigma) = pR_\sigma$. Using (iii), $\tau(D_\sigma R_\sigma) = \tau(\sum_{i=1}^{p} R_{\sigma^i}) = \sum_{i=1}^{p} R_{\sigma^{p-i}} = D_\sigma R_\sigma$. Let $Q = P - D_\sigma R_\sigma$. We have $\sigma(Q) = \tau(Q) = Q$, and hence $Q \in E(\mathbb{Q})$. But we have assumed that $E(\mathbb{Q})$ is finite, so Q is a torsion point. As $E(L)[p]$ is trivial, the image of Q in $E(L)/pE(L)$ is zero, and hence $[P] = [D_\sigma R_\sigma]$, as desired. □

We now describe the p-diagram corresponding to c_L and the action of the Galois group on this diagram. For a point $Q \in E(L)$, we denote the translation by Q map on E by ϕ_Q

Proposition 4.3. *(i) Consider the degree p divisor D on E, defined by $D = \sum_{i=1}^{p} R_{\sigma^i}$. Let $l_1, ..., l_p$ be a basis of the Riemann-Roch space $\mathcal{L}(D)$ and let $E \xrightarrow{l} \mathbb{P}^{p-1}$ be the embedding induced by this choice of basis. Then $[E \xrightarrow{l} \mathbb{P}^{p-1}]$ is the p-diagram representing $c_L \in H^1(L, E[p])$.*

(ii) The action of the Galois group G on the divisor D is given by

$$g\left(\sum_{i=0}^{p-1} R_{\sigma^i}\right) = \phi^*_{-R_g}\left(\sum_{i=0}^{p-1} R_{\sigma^i}\right),$$

(iii) For each $g \in G$, the translation map ϕ_{R_g} induces an isomorphism of p-diagrams $g \cdot [E \xrightarrow{l} \mathbb{P}^{p-1}]$ and $[E \xrightarrow{l} \mathbb{P}^{p-1}]$, represented by the commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{g\cdot l} & \mathbb{P}^{p-1} \\ {\scriptstyle \phi_{R_g}}\downarrow & & \downarrow{\scriptstyle M_g} \\ E & \xrightarrow{l} & \mathbb{P}^{p-1} \end{array} \tag{3}$$

where $M_g \in \mathrm{PGL}_p(L)$. The map $g \mapsto M_g$ determines a cocycle class in $H^1(G, \mathrm{PGL}_p(L))$.

Proof. By Lemma 4.2(iv), we have $[\mathrm{sum}(D)] = [D_\sigma R_\sigma] = [P] \in E(L)/pE(L)$. Then part (i) follows from the description of the Kummer map given in Section 2. For part (ii), by Lemma 4.2(ii) and (iii) we have

$$\sigma\left(\sum_{i=0}^{p-1} R_{\sigma^k}\right) = \phi^*_{-R_\sigma}\left(\sum_{i=0}^{p-1} R_{\sigma^i}\right), \quad \tau\left(\sum_{i=0}^{p-1} R_{\sigma^k}\right) = \sum_{i=0}^{p-1} R_{\sigma^k}.$$

The cocycle condition for $g \mapsto R_g$ implies the result for all $g \in G$.

To see the isomorphism of p-diagrams in (iii), note that by (ii) we have $\phi^*_{-R_g}(D) = g(D)$, and that $g(l_1), ..., g(l_p)$ and $\phi^*_{-R_g}(l_1), ...\phi^*_{-R_g}(l_p)$ are two bases of $\mathcal{L}(g(D))$. We can then take M_g to be the matrix taking one base to the other. Finally, to see that $g \mapsto M_g$ is a cocycle, let C_L be the image of E in $\mathbb{P}^{p-1}$. C_L is a genus one normal curve of degree p, so in particular it spans $\mathbb{P}^{p-1}$, and M_g restricted to C_L is equal to ϕ_{R_g}. As $g \mapsto \phi_{R_g}$ is a cocycle, we deduce that $M_{gh} = g(M_h)M_g$ holds on C_L, and as C_L spans $\mathbb{P}^{p-1}$ and M_g is an automorphism of $\mathbb{P}^{p-1}$, it must hold on the entire $\mathbb{P}^{p-1}$. □

The Galois group G acts in a natural way on the field $\mathcal{L}(E)$ of rational functions on E. Explicitly, for $g \in G$ and $f = u/v \in \mathcal{L}(E)$, with $u, v \in L[x, y]$, we have $g(f) = g(u)/g(v)$, where g acts on u and v by acting on their coefficients. Using this action, we define a twisted action of G on $\mathcal{L}(E)$ by setting $g \star f = \phi^*_{-R_g}(g(f))$. That this is a group action follows immediately from the cocycle condition for $g \mapsto R_g$. By Proposition 4.3(ii), it restricts to an action on the space $\mathcal{L}(D)$.

The action $\star$ is semilinear, meaning that we have $g(v + w) = g(v) + g(w)$ and $g(\alpha v) = g(\alpha)g(v)$ for all $v, w \in V$, $\alpha \in L$ and $g \in \mathrm{Gal}(L/\mathbb{Q})$. We need the following standard result, which is equivalent to (generalized) Hilbert's theorem 90.

Lemma 4.4. *Let V be an n-dimensional L-vector space with a semilinear action of $\mathrm{Gal}(L/\mathbb{Q})$. The set of invariant elements $V(D)^G$ invariant is a p-dimensional $\mathbb{Q}$-vector subspace of V. We have $V \cong V^G \otimes_{\mathbb{Q}} L$, i.e. V has a basis of G-invariant vectors.*

Proof. Follows immediately from Lemma 5.8.1 in Chapter II of [Sil09]. □

Remark 4.5. For V as in the above lemma, the trace map $V \to V^G$ is surjective. In other words, if $\alpha_1, \alpha_2, ..., \alpha_{2p}$ is a basis of L over $\mathbb{Q}$, then V^G is spanned by the elements $\sum_{g\in G} g(\alpha_i v)$ for $1 \le i \le 2p$, $v \in V$. This provides a simple method to compute a basis of V^G.

Let $l_1, \ldots, l_p$ be a basis of $\mathcal{L}(D)$, and for each $g \in G$, define $N_g \in \mathrm{GL}_p(L)$ be the matrix representing the action of g on $\mathcal{L}(D)$ with respect to this basis. Then the matrix N_g^{-1} represents the automorphism $M_g \in \mathrm{PGL}_p(L)$ defined in Proposition 4.3(iii), and slightly abusing notation, we write $M_g = N_g^{-1}$.

Remark 4.6. The semilinearity of the action $\star$ immediately implies that $g \mapsto M_g$ is a cocycle taking values in $\mathrm{GL}_p(L)$, i.e. we lifted the cocycle $g \mapsto M_g$ to an element of $Z^1(G, \mathrm{GL}_(L)$. This can also be interpreted as showing that the obstruction of the class $c \in H^1(\mathbb{Q}, E[p])$ in the Brauer group vanishes.

Proposition 4.7. *Let $f_1, f_2, ..., f_p$ be a basis of $\mathcal{L}(D)$ invariant under the action $\star$. Then the image $C_{\mathbb{Q}}$ of E under the embedding $X \to [f_1(X) : f_2(X) : ... : f_p(X)]$ can be defined over $\mathbb{Q}$, i.e. the ideal defining $C_{\mathbb{Q}}$ as a projective curve has a basis consisting of polynomials with rational coefficients. The p-diagram $C_{\mathbb{Q}} \to \mathbb{P}^{p-1}$ represents the Kolyvagin class c.*

Proof. Since f_i are invariant under the action $\star$, for each g the matrix N_g that represents this action is the identity matrix. For each $g \in G$, let $g(C_{\mathbb{Q}})$ be the image of $C_{\mathbb{Q}}$ under the standard action of G on $\mathbb{P}^{p-1}$, i.e. $g \cdot (u_1 : \ldots : u_p) = (g(u_1) : \ldots : g(u_p))$. By Proposition 4.3(iii), we have $g(C_{\mathbb{Q}}) = C_{\mathbb{Q}}$ for all $g \in G$.

Let I be the ideal defining $C_{\mathbb{Q}}$. I is generated by quadric forms if $p \geq 5$, and if $p = 3$, I is generated by a ternary cubic form. For $p \geq 5$, the L-vector space of quadrics vanishing on $C_{\mathbb{Q}}$ is stable under the natural semilinear action of G, and hence, by Lemma 4.4, has a basis consisting of G-invariant elements, i.e. quadrics with rational coefficients. Similarly, if $p = 3$, there exists a rational ternary cubic defining $C_{\mathbb{Q}}$. Thus $[C_{\mathbb{Q}} \subset \mathbb{P}^{p-1}]$ is a 3-diagram defined over $\mathbb{Q}$, which represents a class in $H^1(\mathbb{Q}, E[p])$ that restricts to the class $c_L \in H^1(L, E[p])$, and hence is a 3-diagram that represents the Kolyvagin class. □

The above proposition thus reduces our problem to computing a basis of $\mathcal{L}(D)^G$. which, by Lemma 4.4, is reduced to linear algebra if we can compute the cocycle M_g representing the action $\star$ relative to a basis of $\mathcal{L}(D)$. We now explain how to do this.

4.2. **Computing the matrices M_g.** Note that it suffices to compute M_σ and M_τ, as σ and τ generate G.

We start by fixing a basis of $\mathcal{L}(D)$. We assume that the points R_{σ^i} are pairwise distinct - it is easy to see that this assumption holds if the class $[P] \in E(L)/pE(L)$ is non-trivial. To make the formulas simpler, we will assume E is in short Weierstrass form, defined by $y^2 = x^3 + Ax + B$. Let $R_g = (x_g, y_g)$ for each $g \in G$ different from identity. Define $l_k = \frac{y + y_{\sigma^k}}{x - x_{\sigma^k}}$ for $1 \leq k \leq p-1$, and set $l_p = 1$.

For $k < p$, it is clear that l_k has a simple pole at 0_E. We note that it has a simple pole at R_σ, and no other poles. Indeed, $x - x_{\sigma^k}$ is of degree two and vanishes at R_{σ^k} and $-R_{\sigma^k}$, and $y + y_{R\sigma}$

vanishes at $-R_{\sigma^k}$. Now it follows easily that $l_k \in \mathcal{L}(D)$, and furthermore that $l_1, l_2, ..., l_{p-1}, l_p$ are linearly independent, and so they span the p-dimensional space $\mathcal{L}(D)$.

Proposition 4.8. *The matrices M_σ and M_τ, relative to the basis $l_1, \ldots, l_p$, are given by*

$$M_\sigma = \begin{pmatrix} 0 & 0 & \ldots & 0 & -1 & 0 \\ 1 & 0 & \ldots & 0 & -1 & c_2 \\ 0 & 1 & \ldots & 0 & -1 & c_3 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -1 & c_{p-1} \\ 0 & 0 & \ldots & 0 & 0 & 1 \end{pmatrix}, \quad M_\tau = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 1 & 0 \\ 0 & 0 & 0 & \ldots & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 & 1 \end{pmatrix}$$

where $c_k = \frac{y_\sigma + y_{\sigma^k}}{x_\sigma - x_{\sigma^k}}$ for $2 \leq k \leq p-1$.

We need the following lemma.

Lemma 4.9. *Let E be an elliptic curve over a field k. For any $P = (x_P, y_P) \in E(k)$ different from 0_E, let $l_P = \frac{y+y_P}{x-x_P} \in k(E)$. Let $P_1, P_2 \in E(k)$ be points such that $P_1 \neq -P_2$.*

(i) Define $f_{P_1,P_2} = \frac{\phi^*_{P_2}(l_{P_1+P_2})}{l_{P_1}} \in k(E)$. Then f_{P_1,P_2} is regular at P_1 and we have $f_{P_1,P_2}(P_1) = 1$.

(ii) For any $R \in E(k)$, we have $\frac{\phi^*_R(l_R)}{l_{-R}} = -1$.

(iii) For disctinct $R_1, R_2 \in E(k)$, we have $(l_{R_1} - l_{R_2})(0_E) = 0$

Proof. (i) It is clear that $f_{P_1,P}$ is regular at P_1. We define a rational function $g \in k(E)$ by $P \mapsto f_{P_1,P}(P_1)$. As $\frac{y+y_{P_1+P_2}}{x-x_{P_1+P_2}}$ has a simple pole at $P_1 + P_2$, $\phi^*_{-P_2}(\frac{y+y_{P_1+P_2}}{x-x_{P_1+P_2}})$ has a simple pole at P_1, and therefore g is regular with no zeros on the open set $E \setminus \{-P_1\}$. But the only such rational function is the constant one, and since $g(0_E) = 1$, we deduce that $g = 1$, and hence $f_{P_1,P_2}(P_1) = 1$.

(ii) Note that both $\phi^*_R(l_R)$ and l_{-R} have simple poles at $-R$ and 0_E. The Riemann-Roch space $\mathcal{L}((0_E) + (-R))$ is 2-dimensional, and therefore there exists a $c_R \in k$ such that $\phi^*_R(l_R) + c_R \cdot l_{-R}$ is a constant function, i.e. the function on $E \times E$

$$\frac{y_{P+R} + y_R}{x_{P+R} - x_R} + c_R \frac{y_P - y_R}{x_P - x_R},$$

depends only on R, and so can be viewed as a rational function on E. It is clearly regular on $E \setminus \{0_E\}$, and therefore it must be constant. Since it does not have a pole at 0_E, we have $c_R = 1$.

(iii) We compute

$$l_{R_1} - l_{R_2} = \frac{y + y_{R_1}}{x - x_{R_1}} - \frac{y + y_{R_2}}{x - x_{R_2}} = \frac{(y_{R_1} + y_{R_2})x - (x_{R_1} + x_{R_2})y - (y_{R_1}x_{R_2} + x_{R_1}y_{R_2})}{(x - x_{R_1})(x - x_{R_2})}.$$

The numerator has a pole of order 3 at 0_E, the denominator has pole of order 4, and hence $l_{R_1} - l_{R_2}$ vanishes at 0_E,

□

Proof of Proposition 4.8. We first compute the matrix M_σ. By Lemma 4.2, we have $R_{\sigma^{p-2}} = \sum_{i=0}^{p-2} \sigma^i(R_\sigma) = -\sigma^{p-1}(R_\sigma)$ and $\sigma(R_{\sigma^k}) = R_{\sigma^{k+1}} - R_\sigma$. Also note that as $l_p = 1$, we have $\sigma(l_p) = \phi^*_{-R_\sigma}(l_p) = 1$, giving the last row of M_σ. The proposition amounts to proving that for $1 \leq k \leq p-2$ we have

$$\phi^*_{R_\sigma}(l_{k+1}) = \sigma(l_k) - \sigma(l_{p-1}) + c_k l_p,$$

as well as

$$\phi^*_{R_\sigma}(l_1) = \sigma(l_{p-1}).$$

Suppose first that $k < p-1$. Recall that we have assumed that the points R_g are distinct, and note that $\phi^*_{R_\sigma}(l_{k+1})$ has simple poles at $R_{\sigma^{k+1}} - R_\sigma = \sigma(R_{\sigma^k})$ and $-R_\sigma$, $\sigma(l_k)$ has simple poles at $\sigma(R_{\sigma^k})$ and 0_E, and $\sigma(l_{p-1})$ has simple poles at $\sigma(R_{\sigma^{p-1}}) = -R_\sigma$ and 0_E.

Hence the function $\frac{\phi^*_{R_\sigma}(l_{k+1})}{\sigma(l_k)}$ is regular at the point $\sigma(R_{\sigma^k})$. By Lemma 4.9, taking $P_1 = \sigma(R_{\sigma^k}) = R_{\sigma^{k+1}} - R_\sigma$ and $P_2 = -R_\sigma$, we see that $\frac{\phi^*_{R_\sigma}(l_{k+1})}{\sigma(l_k)}(\sigma(R_{\sigma^k})) = 1.$. As a consequence we see that the function $\phi^*_{R_\sigma}(l_{k+1}) - \sigma(l_k)$ is regular at $\sigma(R_{\sigma^k})$. By Lemma 4.9(iii), $\sigma(l_k) - \sigma(l_{p-1})$ is regular at 0_E with $\sigma(l_k - l_{p-1})(0_E) = 0$. Hence the rational function $\phi^*_{R_\sigma}(l_{k+1}) - \sigma(l_k) + \sigma(l_{p-1})$ has no poles except perhaps a simple one at $-R_\sigma$, and therefore must be the constant $-c_k$. By evaluating at 0_E, we find that

$$c_k = -(\phi^*_{R_\sigma}(l_{k+1}) - \sigma(l_k) + \sigma(l_{p-1})) = -(\phi^*_{R_\sigma}(l_{k+1}))(0_E) = -l_{k+1}(R_\sigma) = -\frac{y_{\sigma^{k+1}} + y_\sigma}{x_\sigma - x_{\sigma^{k+1}}}.$$

as desired. To prove that $\sigma(l_{p-1}) = -\phi^*_{R_\sigma}(l_1)$, note that in the notation of Lemma 4.9, $\sigma(l_{p-1}) = l_{-R_\sigma}$, and $l_1 = l_{R_\sigma}$, and so we are done by the final assertion of Lemma 4.9.

The computation of M_τ is simpler. Note that $R_\tau = 0_E$, and so the last row of M_τ is the assertion that $\tau(l_p) = l_p = 1$. For the other rows, we need to show that $\tau(l_k) = l_{p-k}$. This follows from the identity $\tau(R_{\sigma^k}) = R_{\sigma^{p-k}}$, which is the content of Lemma 4.2(iii). □

The cocycle condition determines the other M_g as follows: $M_{\sigma^k} = M_\sigma \sigma(M_\sigma) \cdots \sigma^{k-1}(M_\sigma)$, and $M_{\sigma^k \tau} = M_{\sigma^k} M_\tau$.

5. Minimization and reduction

Proposition 4.7 reduces the problem of computing a p-diagram representing the Kolyvagin class to linear algebra over $\mathbb{Q}$, since we now only need to compute a basis for the p-dimensional $\mathbb{Q}$-vector space $\mathcal{L}(D)^G$. However, if we do not do this linear algebra carefully, the resulting diagram $C \subset \mathbb{P}^{p-1}$ will be defined by equations with enormous coefficients. Moreover, even just doing this linear algebra can be computationally very expensive.

The reason for this is that the Heegner point we start with is typically of very large height. From the theory of *minimization* and *reduction* of genus one models, as developed in [CFS10], [Fis13] and [Rad21], we know that every element of the n-Selmer group of E can be represented

by a minimal model, which is an n-diagram given by equations with 'nice' equations. To make this more precise, Theorem 1.2 of [Fis12] shows that the coefficients of these equations are integers bounded by a power of the naive height of E, for $2 \leq n \leq 4$. Another result that is similar in spirit, that holds all odd n, is Theorem 1.0.1 of [Rad21].

We are free to modify a p-diagram $[C \to \mathbb{P}^{p-1}]$ by making a linear change of coordinates on $\mathbb{P}^{p-1}$. In this section we explain how to choose such a coordinate change so that the Kolyvagin class c is represented by a diagram defined by equations with small integer coefficents. This breaks up into two steps known as minimization and reduction. The minimization step finds a $\mathrm{GL}_p(\mathbb{Q})$-transformation so that the diagram $[C \to \mathbb{P}^{p-1}]$ can be represented by an integral model which has nice reduction properties modulo each prime. The reduction step then finds a $\mathrm{GL}_p(\mathbb{Z})$-transformation to make the coefficients of such a model as small as possible.

5.1. **Minimization.**

5.1.1. *Toy example.* We give first an informal overview of what goes wrong with the naive approach and how it can be fixed. Consider the following simpler problem. Let $E/\mathbb{Q}$ be an elliptic curve, let $n \geq 5$ be an odd integer, let $[P] \in E(\mathbb{Q})/nE(\mathbb{Q})$, and suppose we want to compute an n-diagram representing the class $\delta([P]) \in H^1(\mathbb{Q}, E[n])$. Let $y^2 = x^3 + ax + b$ be a Weierstrass equation W for E, with $a, b \in \mathbb{Z}$.

As explained in Section 2, we need to choose a degree n divisor D with $\mathrm{sum}(D) = P$ and compute a basis for the Riemann-Roch space $\mathcal{L}(D)$. A natural choice would be to take $D = (n-1) \cdot (0_E) + (P)$, and for the basis $l_1, \ldots, l_{n-1}$ of $\mathcal{L}(D)$ we can take $1, x, y, x^2, xy, \ldots, x^{\frac{n-1}{2}}$ together with $\frac{y+y_P}{x-x_P}$, if $P = (x_P, y_P) \in E(\mathbb{Q})$, and $\delta([P])$ is represented by $C \subset \mathbb{P}^{n-1}$, where C is the image of E under the map $Q \mapsto (l_1(Q) : \ldots : l_n(Q))$. An integral model for C is then determined by $n(n-3)/2$ quadrics that form the basis for the $\mathbb{Z}$-module of quadrics in integral coefficients that vanish on C.

The problem that arises is that, if q is a prime of good reduction of E, for which the point P maps to zero under the reduction map $E \to \tilde{E}$, i.e. q divides the denominators of x_P and y_P, then the above basis does not reduce to a basis of $\mathcal{L}(\tilde{(D)})$, and it is not difficult to show that this implies that the integral model for C reduces to a singular curve modulo q. If the point P is of large height, then the primes q can be very large, and in practice this forces the coefficients of C to be large, since the discriminant invariant of the integral model of C, as defined in [CFS10], [Fis13], is non-zero integer divisible by q, and so at least q.

In this case, the issue can be resolved as follows. We first replace $(n-1)0_E + P$ by the linearly equivalent divisor $n \cdot (0_E) - (-P)$. Then $\mathcal{L}(D) \subset \mathcal{L}(n \cdot 0_E)$. It follows from the Riemann-Roch theorem that $1, x, y, x^2, xy, x^{\frac{n-1}{2}}, x^{\frac{n-3}{2}}y$ is a basis of $\mathcal{L}(n \cdot 0_E)$. This is a nice basis, in the sense that if q is a prime that does not divide the discriminant of W, then $1, \tilde{x}, \tilde{y}, \tilde{x}^2, \tilde{x}\tilde{y}, x^{\frac{n-1}{2}}, \tilde{x}^{\frac{n-3}{2}}\tilde{y}$ is a basis of $\mathcal{L}(n \cdot 0_{\tilde{E}})$. For the basis of $\mathcal{L}(D)$ we take $l_1, \ldots, l_n$ to be a $\mathbb{Z}$-basis of the module of spanned by those $\mathbb{Z}$-linear combinations of $1, x, y, x^2, xy, x^{\frac{n-1}{2}}, x^{\frac{n-3}{2}}y$ that vanish at $-P$. Then

$l_1, \dots, l_n$ reduces to a basis a of $\mathcal{L}(\tilde{D})$ on the reduction $\tilde{E}$. The curve $C \subset \mathbb{P}^{p-1}$ defined by this embedding has an integral model that reduces to a non-singular curve modulo any prime q with $q \nmid \mathrm{Disc}(E)$, see [Rad21, Lemma 7.4.5]. In fact, if the Weierstrass equation W is minimal, one can also show that this model is a minimal genus one model, in the sense of Theorem 1 of [CFS10].

5.1.2. *Minimizing the Kolyvagin class.* Let us recall the setup of Section 4.1, We assume that we have the data specified in Lemma 4.2: an elliptic curve $E/\mathbb{Q}$, an odd prime p, an imaginary quadratic field $K/\mathbb{Q}$, a cyclic extension L/K of degree p, and a point $P \in E(L)$ such that $[P] \in (E(L)/pE(L))^G$, where $G = \mathrm{Gal}(L/\mathbb{Q})$. We also assume, for simplicity, that L has class number one. This assumption holds in most of the examples we were able to compute in practice. From this data one can compute the points $R_g \in E(L)$ giving rise to the cocycle $g \mapsto R_g$ defined in Lemma 4.2.

Fix a short Weierstrass equation W of E, and let $R_g = (x_g, y_g)$ for $g \in G$. Recall that we have defined two divisors on E

$$D = 0_E + (R_\sigma) + ... + (R_{\sigma^{p-1}}),$$
$$D' = (2p-1) \cdot 0_E - (-R_\sigma) - ... - (-R_{\sigma^{p-1}}).$$

Let D' be the divisor $(2p-1) \cdot 0_E - (-R_\sigma) - ... - (-R_{\sigma^{p-1}})$. As $\mathrm{sum}(D') = \mathrm{sum}(D)$ and both D' and D have degree p, divisors $[D]$ and $[D']$ are linearly equivalent, and the Kolyvagin class $c_L \in H^1(L, E[p])$ is represented by the p-diagram $[E \to \mathbb{P}^{p-1}]$ where the map is induced by the linear system $|D'|$. A choice of a rational function f with $\mathrm{div}(f) = D - D'$ determines an isomorphism between the vector spaces $\mathcal{L}(D)$ and $\mathcal{L}(D')$, and we transport the action of G to $\mathcal{O}_E(D')$ via such an isomorphism. The subset $\mathcal{L}(D')^G$ of G-invariant elements is a p-dimensional $\mathbb{Q}$-vector space. We can naturally view $\mathcal{L}(D')$ as a subspace of $\mathcal{O}_E((2p-1) \cdot 0_E)$ that consists of functions that vanish at $R_\sigma, R_{\sigma^2}, ..., R_{\sigma^{p-1}}$.

Note that $1, x, y, x^2, xy, ..., x^{p-1}, x^{p-2}y$ is a basis of $\mathcal{L}((2p-1) \cdot 0_E)$. Let $S \subset \mathcal{L}((2p-1) \cdot 0_E)$ be the free $\mathcal{O}_L$-module spanned by $1, x, y, x^2, xy, ..., x^{p-1}, x^{p-2}y$ and let $T = S \cap \mathcal{L}(D')$. Then the subset of T^G of invariant elements of T is a $\mathbb{Z}$-module, and since we have $T^G \otimes \mathbb{Q} = \mathcal{L}(D')^G$, T^G is a free Z-module of rank p.

Finally, let $l_1, \dots, l_p$ be a basis of T^G as a $\mathbb{Z}$-module. Then $l_1, \dots, l_p$ is also a basis of $\mathcal{L}(D')^G$ as a $\mathbb{Q}$-vector space, and hence, by Proposition 4.7, determines an embedding $C \to \mathbb{P}^{p-1}$ that represents the Kolyvagin class c. This representation of c is sufficiently nice for us. In fact, in [Rad21, Section 7.4], we show that the reduction of this curve mod q is non-singular for any prime q that does not divide the discriminant of E or the discriminant of L, and in fact we conjecture that the resulting genus one model is minimal.

5.1.3. *Practical computation of a minimal model.* We now explain how to compute equations for the p-diagram defined in above. This essentially amounts to doing linear algebra of Proposition

4.7 over $\mathbb{Z}$. We need to take some care with solving the resulting linear equations, since they have very large coefficients.

Matrix representation of a basis of $\mathcal{L}(D')$. We have an inclusion $\mathcal{L}(D') \subset \mathcal{L}((2p-1)\cdot 0_E)$. Let $e_1 = 1, e_2 = x, e_3 = y, ..., e_{2p-2} = x^{p-1}, e_{2p-1} = x^{p-3}y$ be the usual basis of $\mathcal{L}(D')$. For a basis $f_1, ..., f_p$ of $\mathcal{L}(D')$, we can then write $f_i = \sum_{j=1}^{2p-1} A_{ij}e_j$ for some $A_{ij} \in L$, and from now on we identify the vector space $\mathcal{L}(D')$ with the span of rows of A.

Recall that we have defined a free $\mathcal{O}_L$-module T as the subset of elements of $\mathcal{L}(D')$ that can be expressed as $\mathcal{O}_L$-integral linear combinations of $e_1, ..., e_{2p-1}$. Under the above identification, elements of T correspond to linear combination of rows with integral entries.

Making the action of $\mathrm{Gal}(L/\mathbb{Q})$ explicit. In Section 2 we have defined a basis of $\mathcal{L}(D)$ by setting $l_1 = \frac{y+y_\sigma}{x-x_\sigma}, ..., l_{p-1} = \frac{y+y_{\sigma^{p-1}}}{x-x_{\sigma^{p-1}}}, l_p = 1$. Set $l_i' = \prod_{i=1}^{p-1}(x - x_\sigma)\cdot l_i$, so that l_i' are a basis of $\mathcal{L}(D')$. Let $\alpha_1, ..., \alpha_{2p}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_L$, and consider $\mathcal{L}(D')$ as a $\mathbb{Q}$-vector space with the basis $\alpha_i f_j$, $1 \le i \le 2p$, $1 \le j \le p$. Recall the matrices M_g computed in Proposition 4.8. Let $N_g = M_g^{-1}$. By Proposition 4.3, we have

$$\begin{pmatrix} g(l_1') \\ g(l_2') \\ \vdots \\ g(l_p') \end{pmatrix} = N_g \cdot \begin{pmatrix} l_1' \\ l_2' \\ \vdots \\ l_p' \end{pmatrix}.$$

As the action of G is semilinear, by multiplying the left and right sides by $g(\alpha_j)$ we obtain

$$\begin{pmatrix} g(\alpha_j l_1') \\ g(\alpha_j l_2') \\ \vdots \\ g(\alpha_j l_p') \end{pmatrix} = \frac{g(\alpha_j)}{\alpha_j} N_g \cdot \begin{pmatrix} \alpha_j l_1' \\ \alpha_j l_2' \\ \vdots \\ \alpha_j l_p' \end{pmatrix}.$$

For a general basis $f_1, ..., f_p$ of $\mathcal{L}(D)$ we have a similar formula, with N_g represented by $g(T)N_gT^{-1}$, where $T \in \mathrm{GL}_p(L)$ is the matrix relating the bases l_i' and f_i.

Computing an integral basis of T^G. Using the above formulas we can compute the row vector representation of $g(\alpha_i f_j)$ for each i and j. Let $A_1 \in \mathrm{Mat}_{2p^2, 2p-1}(L)$ be the matrix formed by the rows corresponding to the elements $\sum_{g\in G} g(\alpha_i f_j)$ for $1 \le i \le 2p$, $1 \le j \le p$. By Proposition 4.3, the space $\mathcal{L}(D')^G$ is spanned by the rows of A_1. Note that $T^G = \mathcal{L}(D')^G \cap T$.

Next, the choice of basis $\alpha_1, ...\alpha_{2p}$ determines an isomorphism $L \cong \mathbb{Q}^{2p}$, and hence an isomorphism $\mathrm{Mat}_{k,l}(L) \cong \mathrm{Mat}_{k,2pl}(\mathbb{Q})$ for any pair k, l. To be explicit, for each entry z of A_1, write $z = c_1\alpha_1 + ... + c_{2p}\alpha_{2p}$ for $c_i \in \mathbb{Q}$, and let $A_2 \in \mathrm{Mat}_{2p^2, 2p(2p-1)}(\mathbb{Q})$ be the matrix obtained from A_1 by replacing each entry of A by the associated $2p$-tuple $c_1, ..., c_{2p}$. We say A_2 is obtained from A_1 by the restriction of scalars from L to $\mathbb{Q}$.

The space T^G then corresponds to the $\mathbb{Z}$-sublatice of row vectors with integral entries in the $\mathbb{Q}$-span of rows of A_2, and finding a basis is a standard problem. For example one can scale A_2 by an integer $d \in \mathbb{Z}$ so that $dA_2 \in \mathrm{Mat}_{2p^2,2p(2p-1)}(\mathbb{Z})$, then finding such a basis is dual to the problem of solving a system of integral linear equations, which can be done efficiently using Hermite normal form.

We summarise the above discussion in the following algorithm:

Algorithm 5.1.

- INPUT: E, D, $p \geq 5$ and a point $P \in E(L)$ that satisfies the conditions of Lemma 4.2.
- OUTPUT: An integral model $\mathcal{C}$ of the class $c_{\mathbb{Q}}$.

(i) Compute the points R_g, and then the matrices M_g using the Proposition 4.8.

(ii) Choose a basis $f_1, ..., f_p$ of $\mathcal{L}(D')$, and represent it by a matrix $A \in \mathrm{Mat}_{p,2p-1}(L)$. Use the formulas defining the Galois action to compute the matrix $A_1 \in \mathrm{Mat}_{2p^2,2p-1}(L)$ representing a set of generators of $\mathcal{L}(D')^G$, and its restriction-of-scalars representation $A_2 \in \mathrm{Mat}_{2p^2,2p(2p-1)}(\mathbb{Q})$, as described above. Let V be the $\mathbb{Q}$-span of rows of A_2, and set $T' = \mathbb{Z}^{2p(2p-1)} \cap V$.

(iii) Compute a basis of T' as a matrix $B' \in \mathrm{Mat}_{p,2p(2p-1)}(\mathbb{Z})$, and then compute the matrix $B \in \mathrm{Mat}_{p,2p-1}(\mathcal{O}_L)$ such that B' is the restriction of scalars of B. We recover a basis of T by setting $f_i^G = \sum_{j=1}^{2p-1} B_{ij} e_j$ for $1 \leq i \leq p$.

(iv) Compute a basis $q_1, ..., q_{p(p-3)/2}$ for the $\mathbb{Z}$-module of quadrics with $\mathbb{Z}$-coefficients vanishing on the image of E in $\mathbb{P}^{p-1}$ under the map e induced by $f_1^G, ..., f_p^G$, and return as the model $\mathcal{C}$ the subscheme of $\mathbb{P}^{n-1}_{\mathbb{Z}}$ defined by the q_i.

.

Two steps of the algorithm need further explanation. We need to explain how to compute the quadrics in Step 4, which is straightforward and we will do now, and we need explain how to choose the basis in Step 2, which is a subtler problem.

Step 4 of the algorithm. Let $C_{\mathbb{Q}}$ be the image of E in $\mathbb{P}^{p-1}$ under the embedding e and let C_L be the base change of C_Q to L. As C_L is a genus one normal curve, so in particular projectively normal, the monomials $f_i^G f_j^G$, $1 \leq i, j \leq p$, span the $2p$-dimensional L-vector space $\mathcal{L}(2D')$.

Let $x_1, ..., x_p$ be the coordinates on $\mathbb{P}^{p-1}$, and let $V_{\mathbb{Q}}$ be the $\mathbb{Q}$-space of all rational quadratic forms, spanned by the monomials $x_i x_j$, $1 \leq i, j \leq p$. We then define a $\mathbb{Q}$-linear map $j : V \to \mathcal{L}(2D')$ by the rule $x_i x_j \mapsto f_i^G f_j^G$.

The kernel of this map consists of all of the quadrics that vanish on $C_{\mathbb{Q}}$. We compute a matrix representing the map j, and then use linear algebra over $\mathbb{Z}$ to compute a set of generating quadrics $q_1, ..., q_{p(p-3)/2}$ of $I(C_{\mathbb{Q}})$, with the property that they generate the $\mathbb{Z}$-submodule of integral quadrics that vanish at $C_{\mathbb{Q}}$.

When $p = 3$, $C_{\mathbb{Q}}$ is defined by a single ternary cubic, and it is simple to adapt the above method to work in this case as well.

Picking a basis in Step 2. A natural choice of basis of $\mathcal{L}(D')$, given the computation of Proposition 4.8, would be $l'_1, ..., l'_p$. This, however, does not lead to a practical algorithm. With this choice, computing the basis of T' in Step 3 can be very time consuming, as the dimension of matrix A_2 grows quickly with p and the entries of A_2 tend to be rational numbers of large height, as they were obtained from the coordinates of the Heegner point. We now describe a more careful way to choose a basis.

We start by rescaling the basis l'_i. For legibility write $x_i = x_{\sigma^i}$ and $y_{\sigma^i} = y_i$. As $\mathcal{O}_L$ is a PID, it is a standard fact that we can write $x_i = \frac{r_i}{t_i^2}$ and $y_i = \frac{s_i}{t_i^3}$ for some r_i, s_i, t_i, with r_i, t_i and s_i, t_i being pairs of coprime algebraic integers. For $1 \leq i \leq p-1$, we put

$$f'_i = t_i \cdot t_1^2 \cdots t_{p-1}^2 \cdot l'_i = (t_1^2 x - r_1) \cdots (t_{i-1}^2 + r_{i-1})(t_i^3 y + s_i)(t_{i+1}^2 x + r_{i+1}) \cdots (t_{p-1}^2 x - r_{p-1})$$

Having chosen this scaling, we see that $f'_i \in T$, i.e. the matrix A' whose rows represent f'_i have integral entries, and so do the corresponding matrices A'_1 and A'_2.

We now make a heuristic observation to motivate our next step. Note that, for $l < k < p$, we have $R_{\sigma^k} - R_{\sigma^l} = \sum_{i=1}^{k} \sigma^{i-1}(R_\sigma) - \sum_{i=1}^{l} \sigma^{i-1}(R_\sigma) = \sigma^l(R_{\sigma^{k-l}})$. If for a prime $\mathfrak{p}$ of $\mathcal{O}_L$ the point $\sigma^l(R_{\sigma^{k-l}})$ reduces to $0_{\widetilde{E}}$, then $\widetilde{R_{\sigma^k}} = \widetilde{R_{\sigma^l}}$, and hence $\widetilde{f_k} = \widetilde{f_l}$. Hence $\mathfrak{p}$ will divide all entries of the difference $r_{k,l}$ of rows of A' corresponding to f_k and f_l. As the primes for which $\sigma^l(R_{\sigma^{k-l}})$ reduces to zero are exactly those that divide $\sigma^l(t_{k-l})$, we expect that the entries of $r_{k,l}$ and $\sigma^{k-l}(t_l)$ will have a large common divisor.

To cancel out these divisors for all pairs of rows we use the following procedure, reminiscent of Gaussian elimination. Let $r_1, ..., r_p$ be the rows of A'. For $1 \leq k \leq p-1$, consider the $2 \times (2p-1)$ submatrix A^k of A' formed by r_k and r_{p-1}, and let d_k be the generator of the ideal of $\mathcal{O}_L$ generated by the 2×2 minors of A^k. We then compute $c_k \in \mathcal{O}_L$ such that the entries of $r_{p-1} - c_k r_k$ are divisible by d_k - this amounts to putting A^k in Hermite normal form (over $\mathcal{O}_L$), which is possible since we assumed $\mathcal{O}_L$ is a PID, and can be done efficiently.

Next, compute a generator D_k of the ideal $(d_k, d_1 \cdots d_{k-1} d_{k+1} \cdots d_{p-2})$, and find $i_k \in \mathcal{O}_L \frac{d_k}{D_k}$ and $j_k \in \mathcal{O}_L \cdot \frac{d_k, d_1 \cdots d_{k-1} d_{k+1} \cdots d_{p-2}}{D_k}$, with $i_k + j_k = 1$ - this is also a standard problem, see [Coh13]. We then replace r_{p-1} with $r'_{p-1} = r_{p-1} - j_1 c_1 \cdot r_1 - ... - j_{p-2} c_{p-2} \cdot r_{p-2}$, and then divide r'_{p-1} by the GCD of its entries. In practice, D_k will often be a unit or at worst divisible by a few small primes, and so this GCD will be the product $d_{1,p-1} \cdots d_{p-2,p-1}$, up to a small factor. We then repeat this process for rows $r_1, ..., r_{p-2}$, with r_{p-2} taking the role of r_{p-1}, and so on.

At the end of this process we obtain a new matrix $A'' \in \mathrm{Mat}_{p,2p-1}(\mathcal{O}_L)$ and $U \in \mathrm{GL}_p(L)$ with $A'' = UA'$. We then take $f_1, ..., f_p$ to be the basis of $\mathcal{L}(D')$ that corresponds to the rows of A''. To

account for the change of basis, we replace M_g by $UM_g g(U^{-1})$ for each $g \in G$, and then compute a basis $f_1^G, ...f_p^G$ of T^G using the approach described for A.

5.2. **Reduction.** The final step is to find a $\mathrm{GL}_p(\mathbb{Z})$-change of coordinates making the coefficients of the equations defining $C \subset \mathbb{P}^{p-1}$ as small as possible. For this, we use the method of reduction, developed in Section 6 of [CFS10]. This method extends with minimal changes to our setting, so we give a very brief summary.

To compute a reduced p-diagram equivalent to the diagram $[C \subset \mathbb{P}^{p-1}]$ representing the Kolyvagin class, we first compute the reduction covariant $\phi(C)$, according to the recipe given in Section 6 of [CFS10]. The reduction covariant is a certain symmetric positive definite matrix, well-defined up to a scalar in $\mathbb{R}^\times$ one associates to a p-diagram $[C \subset \mathbb{P}^{p-1}]$ defined over $\mathbb{R}$, which transforms in a natural way under linear changes of coordinates on $\mathbb{P}^{p-1}$. Computing it amounts to computing the set of flex points of C, i.e. points $P \in C(\mathbb{C})$ with the property that the tangent hyperplane at P meets C only at P. In our case this is is easy, since we have a description of C as an embedding of E via the complete linear system $|D'|$. We then use the LLL algorithm to compute a $g \in SL_n\mathbb{Z}$ such that $g^{-t}\phi(C)g^{-1}$ is LLL-reduced, and replace C with $g(C)$. For more details on our implementation, see Section 7.4.3 of [Rad21].

6. Examples

In this section we apply the theory we developed to concrete examples, and construct elements of p-torsion subgroups of Tate-Shafarevich groups, for $p \leq 11$ an odd prime.

As mentioned in the introduction, these computations are of the most interest when the prime p is at least 7, since for $p \leq 5$ the usual method of p-descent works quite well for computing these examples. As a warmup, we compute an element of $Ш(E/\mathbb{Q})[3]$ for the curve E labelled $681b3$ in Cremona's tables. We then follow with our main result, explicit equations representing an element of $Ш(E/\mathbb{Q})[p]$ for $p = 7$, where E is the curve $3364c1$.

Note that we can't apply the theory we developed in Section 2 to the Kolyvagin class c_Q directly. We defined this class as the image of the class $[D_\sigma z_K] \in E(L)/pE(L)$, and the point $D_\sigma z_K$ needs not satisfy the conditions of Proposition 4.2, since it is not necessarily fixed by complex conjugation τ. However, since c_Q is in the $\pm$-eigenspace of $H^1(\mathbb{Q}, E[p])$, where $\pm$ is the sign of the functional equation of E, we have $2 \cdot [D_\sigma z_K] = [D_\sigma z_K \pm \tau D_\sigma z_K] = [P] \in (E(L)/pE(L))^G$. We can then recover the $\mathbb{F}_p$-line spanned by c in $H^1(\mathbb{Q}, E[p])$, since we can use Algorithm 5.1 to compute a p-diagram representing the class $[mP]$ for any $m \in \mathbb{Z}$.

Recall that by Proposition 4.2(ii), we have $[P] = [D_\sigma R_\sigma]$, with $R_\sigma = \frac{\sigma(P)-P}{p}$. In practice, the point R_σ is of much smaller height than z_K, and it is simple to adapt Algorithm 3.2 to compute this point directly. However, a drawback is that there are p^2 possible p-division points of the point $\sigma(P) - P$ in $E(\mathbb{C})$, and only one of them is the point R_σ. Thuse we use Algorithm 3.2 on each division point successively, until the algorithm returns a point. If the height of the Heegner point

is very large, like in our $p = 7$ example, this is worth doing, however if p is large and the height of the point is small, like in our $p = 11$ example, it will slow down our code.

For all of our computations we used the computer algebra system MAGMA ([BCP97]). The source code, along with further examples we computed, is available as a GitHub repository at `https://github.com/lazaradicevic/kolyvagin.classes`.

Example 6.1. Consider the elliptic curve E labeled 681b3 in Cremona's tables. E has no rational 3-isogeny and $Ш(E)[3] = (\mathbb{Z}/3\mathbb{Z})^2$. There are no elliptic curves of smaller conductor with this property, so E is a natural first candidate for us. E is defined by the minimal Weierstrass equation

$$y^2 + xy = x^3 + x^2 - 1154x - 15345$$

For our Heegner discriminant, we choose $D = -107$. The conductor of E is $N = 3 \cdot 227$, and one verifies that 3 and 227 split completely in $K = \mathbb{Q}(\sqrt{-107})$, so D satisfies the Heegner hypothesis.

For our field L, we take the Hilbert class field of K. As K has class number 3, by class field theory $L/\mathbb{Q}$ is a dihedral extension of degree 6. We use the machinery implented in MAGMA to find that $L = \mathbb{Q}[\alpha]$, where the minimal polynomial of α is $x^6 - 2x^5 - 2x^3 + 30x^2 - 52x + 29$, and that L has class number 1. We fix an ideal $\mathcal{N}$ with $\mathcal{N}\bar{\mathcal{N}} = N\mathcal{O}_K = 681\mathcal{O}_K$. Let $z_K \in E(H)$ be the Heegner point that is the image of the point $(\mathcal{O}_K, [\mathcal{O}_K], \mathcal{N})$. There are 4 possible choices for $\mathcal{N}$, corresponding to the factorization $N = 3 \cdot 227$. Which one we choose is not important for the purpose of constructing non-trivial Kolyvagin classes, since changing the choice of $\mathcal{N}$ replaces z_K by $\pm z_K + T$, where $T \in E_{tors}(\mathbb{Q})$. See Proposition 5.3 of [Gro91].

Using Algorithm 3.2, slightly modifed as explained above, we compute the point $R_\sigma \in E(L)$. Its x-coordinate is

$$\begin{aligned}
&1/17416824132637709581434 50(48340302691531197918278708 1\alpha^5 + \\
&3545382560549856607374381 0\alpha^4 - 1374984585681049490117664 87\alpha^3 - \\
&2452468960182058461987679215\alpha^2 + 9038525365115044024894770546\alpha - \\
&3473956084362757366189406163).
\end{aligned}$$

Next, we run the Algorithm 5.1 up to Step 3, computing rational functions l_1, l_2 and l_3 that form an invariant basis of $\mathcal{L}(5 \cdot 0_E - R_\sigma - R_{\sigma^2})$. Let C be the image of E in $\mathbb{P}^2$ under the map $(x, y) \mapsto (l_1(x, y) : l_2(x, y) : l_3(x, y))$. Step 4 of Algorithm 5.1 does not apply in this case, since C is defined by a ternary cubic rather than by quadrics. However it is easy to compute a cubic G defining C, using the standard algorithms implemented in MAGMA:

$$\begin{aligned}
G = {} & 2372x^3 + 4174x^2y - 3043x^2z + 2340xy^2 - 3457xyz + 1271xz^2 + \\
& 419y^3 - 940y^2z + 700yz^2 - 173z^3
\end{aligned}$$

Next step is to reduce G. We find that making a change of variables associated to the unimodular matrix

$$\begin{pmatrix} -1 & -5 & -9 \\ 0 & 3 & 4 \\ 0 & 1 & 1 \end{pmatrix},$$

takes G to the cubic

$$F = x^3 + 2x^2y - 3x^2z - xy^2 + 9xyz - 8xz^2 + y^3 - 11y^2z - 5yz^2 + 6z^3$$

The cubic F is minimal, in the sense of Definition 3.1 of [CFS10], and is essentially as nice as of an equation as we can hope. Let $C \subset \mathbb{P}^2$ be the curve defined by F. The diagram $[C \to \mathbb{P}^2]$ is the representation of the class $c_{\mathbb{Q}} \in H^1(\mathbb{Q}, E[3])$ that we set out to obtain.

Note that as Algorithm 3.2 does not prove that the point we computed is the Heegner point, we still need to prove that the this class is in the 3-Selmer group $\mathrm{Sel}^{(3)}(E/\mathbb{Q})$, i.e. that the curve C is everywhere locally soluble. Since we have represented c by the ternary cubic F, we can use the standard algorithms for genus one models implemented in MAGMA to do so.

Finally, to check that the image of $c_{\mathbb{Q}}$ is a non-trivial element of $Ш(E/\mathbb{Q})$, note that E has rank 0 and $E(\mathbb{Q})[3]$ is trivial. Hence $E(\mathbb{Q})/3E(\mathbb{Q})$ is trivial, and we only need to show that $c_{\mathbb{Q}}$ is non-zero. Thus it suffices to check that the class $[D_\sigma R]$ is non-zero in $E(L)/3E(L)$, i.e. that $D_\sigma \cdot R_\sigma$ is not divisible by 3, and it is easy to check that this is indeed the case. Hence $C(\mathbb{Q})$ is empty, and C is a counterexample to the Hasse principle.

Remark 6.2. One can easily find an equation for $c_{\mathbb{Q}}$ using the method of 3-descent. However, our method gives us an additional piece of information - we know that the class $c_{\mathbb{Q}}$ capitulates over the field L, i.e. the curve C admits an L-rational point. By construction of our model for $[C \to \mathbb{P}^{n-1}]$, we know that the images of the points R_{σ^i}, where $0 \leq i \leq p-1$, under the embedding $E \xrightarrow{l} \mathbb{P}^{p-1}$, lie on the intersection of the curve C and a hyperplane H defined over $\mathbb{Q}$. We can compute an equation for H using linear algebra, since p points uniquely determine a hyperplane in $\mathbb{P}^{p-1}$. In our case, we find

$$H = 771x - 2818y + 4751z.$$

Hence, the binary cubic obtained by substituting $z = -771/4751x + 2818/4751y$ in F splits as a product of three distinct linear forms over L.

Example 6.3. Let E be the curve labeled 3364c1 in Cremona's tables, defined by a minimal Weierstrass equation $y^2 = x^3 - 4062871x - 3152083138$. Similarly to the previous examples, we chose E because it is the smallest rank 0 curve with no rational 7-isogeny and $Ш(E/\mathbb{Q})[7] \cong (\mathbb{Z}/7\mathbb{Z})^2$.

For the Heegner discriminant, we take $D = -71$, which has class number 7. The Hilbert class field L of $K = \mathbb{Q}(\sqrt{-71})$ is a degree 14 dihedral extension of $\mathbb{Q}$, defined by

$$f = x^{14} + 7x^{13} + 25x^{12} + 59x^{11} + 103x^{10} + 141x^9 + 159x^8 + 153x^7 + \\ 129x^6 + 95x^5 + 58x^4 + 27x^3 + 10x^2 + 3x + 1;$$

The class group of the Hilbert class field L of K is trivial, so $\mathcal{O}_L$ is a PID. We compute $R = z_K - Q$ directly, using 250 digits of precision in the computation of modular parametrization, and finding a point of height 194.99. This calculation took less than a minute with our MAGMA implementation. Unfortunately the results of the computation are too large to print here, so we refer the reader to our GitHub repository.

As before, we use the algorithm of Section 5.1.3 compute the rational functions $l_1, l_2, \ldots, l_7$ that define an embedding $E \to \mathbb{P}^6$ over L. The image of the embedding is a curve C, that admits a minimal model defined over $\mathbb{Q}$. We then compute a basis for the 14-dimensional space of quadrics that cut out the curve C. Strikingly, the coefficients of all of the equations are remarkably small. We give two of the equations below:

$$f_1 = 2x_1x_2 - 2x_1x_3 + 2x_1x_5 - x_1x_6 + x_2^2 - x_2x_3 - x_2x_4 + 2x_2x_5 - 4x_2x_6 + 2x_2x_7 - 3x_3^2 - 3x_3x_5$$

$$\vdots$$

$$f_{14} = 2x_1^2 + 3x_1x_2 - x_1x_3 + 3x_1x_7 - 2x_2^2 - 2x_2x_3 - x_2x_4 + x_2x_5 + 4x_2x_6 + 3x_2x_7 - 2x_3^2 \\ + 4x_3x_4 - 4x_3x_5 + 2x_3x_6 + 4x_4^2 + x_4x_5 + 2x_4x_7 - 4x_5^2 - 5x_5x_6 - 4x_5x_7 - 7x_6^2 + x_6x_7.$$

We need to check that the curve C is everywhere locally soluble, and so represents an element of the 7-Selmer group. Testing a genus one curve for local solubility is a well-studied problem, and we use the standard method do this. We use MAGMA to check that for for any prime q except 2 and 29, the reduction of above quadrics modulo q defines defines a non-singular curve of genus one $\tilde{C}$ in $\mathbb{P}^{p-1}_{\mathbb{F}_q}$. By Lang's theorem there exists a point $\tilde{Q} \in \tilde{C}(\mathbb{F}_q)$, and Hensel's lemma (as stated in Proposition 5, Section 2.3 of [BLR12]) provides a lift to a point $Q \in C(\mathbb{Q}_p)$. For $q = 2$ and $q = 29$, we find a smooth point $C(\mathbb{F}_q)$ by a naive search, and again use Hensel's lemma to show the existence of a lift to $C(\mathbb{Q}_p)$.

Note that 2 and 29 are exactly the primes of bad reduction for E, and that checking that they were the only primes of bad reduction for C is very easy, from a computational point of view, only because we the model of C we have computed is minimized. Had we not done so, and just naively computed a G-invariant basis by, for example, averaging the basis $l_1, \ldots, l_p$ of Section 4.2 using the trace operator, working out primes of bad reduction would have required factoring a very large number, and would not have been computationally feasible.

Finally, to show that $C(\mathbb{Q})$ is empty, we only need to check that $c_{\mathbb{Q}}$ is non-trivial, since E is of rank zero and $E[7](\mathbb{Q})$ is trivial. It suffices to show that $c_L = [D_\sigma R_\sigma] \in E(L)/7E(L)$ is non-trivial, i.e. that $D_\sigma R_\sigma$ is not divisible by 7, and to show this, it suffices to find a prime $\mathfrak{p}$ of L such that the reduction $\tilde{D_\sigma R_\sigma}$ is not divisible by 7 in $\tilde{E}(\mathbb{F}_\mathfrak{p})$. A naive search quickly shows that this is true if $\mathfrak{p}$ is a prime lying above 47.

We have also computed the equation of the hyperplane H passing through the (images of) points R_{σ^i} on C - the coefficients are large, but still much smaller than the coordinates of R_σ.

Example 6.4. Finally, another interesting example we have computed is a non-trivial element of $Ш(E_D/\mathbb{Q})[11]$, where E_D is the quadratic twist of the curve $37a1$ by $D = -2731$. The curve E has rank 1, and this is the smallest value of D for which the BSD conjecture predicts that $Ш(E_D/\mathbb{Q})[11] \cong (\mathbb{Z}/11\mathbb{Z})^2$, the Heegner condition is satisfied, the curve E_D is of rank 0, and the class number of $\mathbb{Q}(\sqrt{D})$ is equal to 11. The 11-diagram that represents this class is a curve in $\mathbb{P}^{10}$ defined by 44 quadrics, and so is impractical to print here. In this rank one case, the Heegner point has much smaller height, and so the precision to which we need to compute the modular parametrization of the curve is much smaller. The class c_L is given as $[D_\sigma R] \in E(L)/11E(L)$, where R is a point of height approximately 3.812. In contrast, for the curve 8350c1, which is the smallest curve in Cremona's tables with $Ш(E/\mathbb{Q})[11]$ non-trivial, no 11-isogeny and rank zero, we have not succeeded in computing a Heegner point for any of the first few Heegner discriminants D for which $p|\mathrm{Cl}(D)$.

References

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over q: wild 3-adic exercises*, Journal of the American Mathematical Society (2001), 843–939.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system I: The user language*, Journal of Symbolic Computation **24** (1997), no. 3-4, 235–265.

[BLR12] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, vol. 21, Springer Science & Business Media, 2012.

[CFO+08] John E Cremona, Tom A Fisher, Cathy O'Neil, Denis Simon, and Michael Stoll, *Explicit n-descent on elliptic curves, i. algebra*, Journal für die reine und angewandte Mathematik **2008** (2008), no. 615, 121–155.

[CFS10] John E Cremona, Tom A Fisher, and Michael Stoll, *Minimisation and reduction of 2-, 3-and 4-coverings of elliptic curves*, Algebra & Number Theory **4** (2010), no. 6, 763–820.

[Coh08] Henri Cohen, *Number theory: Volume i: Tools and diophantine equations*, vol. 239, Springer Science & Business Media, 2008.

[Coh13] ———, *A course in computational algebraic number theory*, vol. 138, Springer Science & Business Media, 2013.

[Fis12] T Fisher, *Some bounds on the coefficients of covering curves*, L'Enseignement Mathématique. IIe Série **58** (2012).

[Fis13] Tom Fisher, *Minimisation and reduction of 5-coverings of elliptic curves*, Algebra & Number Theory **7** (2013), no. 5, 1179–1205.

[Gro84] B Gross, *Heegner points on $X_0(N)$*, 1984, pp. 87–106.

[Gro91] Benedict H Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989) **153** (1991), 235–256.

[Han09] Guillaume Hanrot, *Lll: a tool for effective diophantine approximation*, The LLL Algorithm, Springer, 2009, pp. 215–263.

[JLS09] Dimitar Jetchev, Kristin Lauter, and William Stein, *Explicit Heegner points: Kolyvagin's conjecture and non-trivial elements in the Shafarevich–Tate group*, Journal of Number Theory **129** (2009), no. 2, 284–302.

[Kol89] Viktor Alexandrovich Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(E,\mathbb{Q})$ for a subclass of Weil curves*, Mathematics of the USSR-Izvestiya **32** (1989), no. 3, 523.

[Rad21] Lazar Radicevic, *Capitulation discriminants of genus one curves*, Ph.D. thesis, University of Cambridge, 2021.

[Shi71] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, vol. 1, Princeton university press, 1971.

[Sil94] Joseph H Silverman, *Advanced topics in the arithmetic of elliptic curves*, vol. 151, Springer Science & Business Media, 1994.

[Sil09] ———, *The arithmetic of elliptic curves*, vol. 106, Springer Science & Business Media, 2009.

[Wat05] Mark Watkins, *Some remarks on Heegner point computations*, arXiv preprint math/0506325 (2005).

[Wes15] Tom Weston, *The Euler system of Heegner points*, 2015.

Max Planck, Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany
Email address: lazaradicevic@gmail.com