THE EULER SYSTEM OF HEEGNER POINTS

TOM WESTON

Contents

1. Introduction

Let E be an elliptic curve over $\mathbf{Q}$ of conductor N and let K be an imaginary quadratic field in which all primes dividing N split. The theory of complex multiplication and a modular parameterization $X_0(N) \to E$ can be used to define a point $y_K \in E(K)$, called a *Heegner point.* y_K depends on some choices, but it is well-defined up to sign and torsion, so that its canonical height $\hat{h}(y_K)$ is well-defined independent of any choices. If $L(E/K, s)$ is the L-function of E over K, one has

$L(E/K,1) = 0$ for trivial reasons, and Gross and Zagier proved the spectacular formula

$$L'(E/K,1) = \left(\frac{1}{\sqrt{D}}\int_{E(\mathbf{C})} \omega \wedge \overline{i\omega}\right) \cdot \hat{h}(y_K).$$

Here D is the discriminant of $K/\mathbf{Q}$ and ω is the differential on E coming from the modular parameterization. In particular, $L'(E/K,1) \neq 0$ if and only if y_K has infinite order.

Motivated by this and the conjecture of Birch and Swinnerton-Dyer, Gross and Zagier were led to the following conjecture (their conjecture is somewhat more precise):

Conjecture (Gross–Zagier)**.** *Assume that y_K has infinite order in $E(K)$. Then $E(K)$ has rank one and the Shafarevich-Tate group $\text{Ш}(E/K)$ has trivial p-primary component for any odd prime p such that:*

- *E has good reduction at p;*
- $\mathrm{Gal}(\mathbf{Q}(E[p])/\mathbf{Q}) \cong \mathrm{GL}_2(\mathbf{F}_p)$*;*
- *$y_K \notin pE(K)$.*

In this paper we give Kolyvagin's proof of this conjecture. The key idea is that the Heegner point y_K does not come alone: it lies at the bottom of a certain family of points of E defined over anti-cyclotomic extensions of K. These points satisfy relations which make them an *Euler system.* This allows one to use them and techniques from Galois cohomology to bound the Selmer group $\mathrm{Sel}(K, E[p])$ (and thus to obtain information on $E(K)/pE(K)$ and $\text{Ш}(E/K)[p]$) for appropriate primes p.

This paper could not exist without the magnificent paper [6]. In particular, Sections 5 and 6 of this paper follow the corresponding sections of [6] very closely. We deviate from Gross in our treatment of the Galois cohomology. Our exposition is intended to relate somewhat more directly to the more recent theories of Euler systems developed by Rubin, Kato and Perrin-Riou.

We present this Galois cohomology in Sections 2 and 3. We first define Selmer groups and recall the relevant duality results. Our treatment of Euler systems is based on the exact sequence (7) which divides the computation of a Selmer group into two parts. The first part is the computation of a certain restricted Selmer group. This can be done quite generally, and we present these results without reference to elliptic curves. The second part is the production of an Euler system. We give no general theory for this; we only explain it in the case of elliptic curves in Sections 6.

Section 4 contains the details of the proof of Kolyvagin's theorem; it assumes the existence of the cohomology classes constructed via the Euler system in Section 6. Section 4 is mostly a straightforward application of the results of Section 3; we try to emphasize that this part of the proof consists entirely in fairly routine Galois cohomology calculations.

We introduce Heegner points and their basic properties (which make them an Euler system) in Section 5. In Section 6 we explain how to use these properties to prove the results needed in Section 4.

It is our hope that this paper can serve as an introduction to Euler systems for a graduate student with some knowledge of Galois cohomology and the arithmetic of elliptic curves. Although Heegner points do not fit into most of the general theories of Euler systems, we regard it is an especially interesting and striking example of the fundamental ideas involved.

This paper grew out of one of the student projects at the 2001 Arizona Winter School. In the process of helping my student group to prepare their presentation on [6], it became clear to me that the Galois cohomology in Gross' argument could be simplified in several ways. This paper is my attempt to demonstrate that. Although it may seem strange that the allegedly simpler proof given here is somewhat longer than that given in [6], I believe that much of the extra bulk comes from the general treatment of the Galois cohomology and some elaboration on points Gross treats very quickly. (See [4] and [13] for another example of an intended simplification by this author which ended up being far longer than the original, especially considering that all of the hard parts were omitted.)

My Winter School student group consisted of Kirsten Eisentraeger, Chris Hall, Ling Long, Satya Mohit, Jorge Pineiro, Marat Sadykov and Michael Schein. I would like to express my sincere gratitude to each of them for preparing and giving an outstanding presentation of these ideas; I would also like to thank them for helping me to understand this proof far better than I ever had before. I hope that skipping the Desert Museum seemed at least a little worthwhile in the end. Robert Pollack provided invaluable insight throughout the project, and Mark Dickinson helped me work out some of the details in this write-up. The calculations presented in Section 7 were done by Kirsten Eisentraeger and Peter Green; William Stein helped with some of them as well. I would also like to thank the organizers of the Winter School for giving all of us this opportunity. Lastly, I would like to thank Barry Mazur for inviting me to share in his lectures at the Winter School and for all of the help and inspiration he provided. If nothing else, I hope that this paper can at least serve as the long-awaited conclusion to [7].

Notation. If H is an abelian group with $pH = 0$, we write $H^\vee$ for its Pontrjagin dual $\mathrm{Hom}_{\mathbf{F}_p}(H, \mathbf{F}_p)$. If H is an arbitrary abelian group, we write $H[p]$ for the p-torsion in H.

If K is a perfect field we will write G_K for the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$. If L is an extension of K and T is a $\mathrm{Gal}(L/K)$-module, we write $H^i(L/K, T)$ for the group cohomology $H^i(\mathrm{Gal}(L/K), T)$; if $L = \bar{K}$ we will just write this as $H^i(K, T)$. (All Galois modules we consider will be discrete so that there is no need to worry about topologies.) If T is a p-torsion G_K-module for some prime p, we write T^* for its *Cartier dual* $\mathrm{Hom}_{\mathbf{F}_p}(T, \mu_p)$ (where μ_p denotes the G_K-module of the p^{th} roots of unity) endowed with the adjoint Galois action. We write $K(T)$ for the fixed field of the kernel of the homomorphism $G_K \to \mathrm{Aut}(T)$.

We will identify non-archimedean places of number fields with prime ideals; we will usually use places when working abstractly and ideals when working somewhat more concretely. We will tend to ignore archimedean places; this will not be a problem since we almost always have $p \neq 2$.

We will have frequent use for the following construction: let M/L and L/K be Galois extensions and assume that $\mathrm{Gal}(M/L)$ is abelian. There is a natural action of $\mathrm{Gal}(L/K)$ on $\mathrm{Gal}(M/L)$ defined as follows: given $\tau \in \mathrm{Gal}(L/K)$ and $\sigma \in \mathrm{Gal}(M/L)$, let $\tilde{\tau}$ be any lift of τ to $\mathrm{Gal}(M/K)$. Then the action of τ on σ is given by ${}^\tau\sigma = \tilde{\tau}\sigma\tilde{\tau}^{-1}$. (The fact that $\mathrm{Gal}(M/L)$ is abelian implies that this is independent of the choice of $\tilde{\tau}$.) The action of $\mathrm{Gal}(L/K)$ on $\mathrm{Gal}(M/L)$ is trivial precisely when M is an abelian extension of K.

We will often be working with eigenspaces for involutions, and we make the following sign convention: whenever $\pm$ appears in a formula, it is to be regarded as a fixed choice of sign, and every other $\pm$ in that formula should agree with this choice; a $\mp$ indicates the opposite of this initial choice.

2. Local cohomology groups

2.1. **Basic facts.** Fix a prime l and let K be a finite extension of $\mathbf{Q}_l$. Let K^{ur} denote the maximal unramified extension of K; we write I_K for the inertia group $\mathrm{Gal}(\bar{K}/K^{\mathrm{ur}})$ and G_K^{ur} for $G_K/I_K \cong \mathrm{Gal}(K^{\mathrm{ur}}/K)$. Let T be a finite dimensional $\mathbf{F}_p$-vector space with a discrete action of G_K. We say that T is *unramified* if I_K acts trivially on T.

We will need the following facts about the Galois cohomology group $H^1(K,T)$.

Inflation-restriction: There is an exact sequence [10, Chapter 7, Section 6]

$$0 \to H^1(K^{\mathrm{ur}}/K, T^{I_K}) \xrightarrow{\mathrm{inf}} H^1(K,T) \xrightarrow{\mathrm{res}} H^1(I_K,T)^{G_K^{\mathrm{ur}}} \to 0. \tag{1}$$

(We will always use inflation to regard $H^1(K^{\mathrm{ur}}/K, T^{I_K})$ as a subspace of $H^1(K,T)$.)

Tate local duality: There is a perfect pairing of $\mathbf{F}_p$-vector spaces [8, Chapter I, Corollary 2.3]

$$H^1(K,T) \otimes_{\mathbf{F}_p} H^1(K,T^*) \to \mathbf{F}_p. \tag{2}$$

Unramified duality: If $l \neq p$ and T is unramified, then $H^1(K^{\mathrm{ur}}/K,T)$ and $H^1(K^{\mathrm{ur}}/K,T^*)$ are exact orthogonal complements under the Tate pairing; see [8, Chapter I, Theorem 2.6].

2.2. **Local Selmer structures.** By a *local Selmer structure* $\mathcal{F}$ (sometimes called a finite/singular structure) for T we simply mean a choice of $\mathbf{F}_p$-subspace $H^1_{f,\mathcal{F}}(K,T)$ of $H^1(K,T)$. We define the *singular quotient* $H^1_{s,\mathcal{F}}(K,T)$ as $H^1(K,T)/H^1_{f,\mathcal{F}}(K,T)$, so that there is an exact sequence

$$0 \to H^1_{f,\mathcal{F}}(K,T) \to H^1(K,T) \to H^1_{s,\mathcal{F}}(K,T) \to 0. \tag{3}$$

For $c \in H^1(K,T)$ we write c^s for the image of c in $H^1_{s,\mathcal{F}}(K,T)$.

We say that $\mathcal{F}$ is the *unramified structure* if $H^1_{f,\mathcal{F}}(K,T) = H^1(K^{\mathrm{ur}}/K,T^{I_K})$. In this case the sequence (3) identifies with the sequence (1).

Given a local Selmer structure $\mathcal{F}$ on T, we define the Cartier dual local Selmer structure $\mathcal{F}^*$ on T^* to be the exact orthogonal complement of $H^1_{f,\mathcal{F}}(K,T)$ under the Tate pairing (2). In particular, there is an induced perfect pairing

$$H^1_{s,\mathcal{F}}(K,T) \otimes_{\mathbf{F}_p} H^1_{f,\mathcal{F}}(K,T^*) \to \mathbf{F}_p. \tag{4}$$

Note that if T is unramified, $\mathcal{F}$ is the unramified structure and $l \neq p$, then T^* is unramified and $\mathcal{F}^*$ is the unramified structure.

2.3. **Local cohomology of elliptic curves.** Let E be an elliptic curve over the local field K. We will be studying the G_K-module $E[p] = E(\bar{K})[p]$; it is a two-dimensional $\mathbf{F}_p$-vector space. Recall that the Weil pairing on $E[p]$ is a perfect Galois equivariant pairing

$$E[p] \otimes_{\mathbf{F}_p} E[p] \to \mu_p;$$

see [11, Chapter 3, Section 8] It follows that $E[p]^*$ is canonically isomorphic to $E[p]$.

We have an exact sequence

$$0 \to E[p] \to E(\bar{K}) \xrightarrow{p} E(\bar{K}) \to 0$$

of G_K-modules. The associated long exact sequence in G_K-cohomology yields a short exact sequence

$$0 \to E(K)/pE(K) \xrightarrow{\kappa} H^1(K, E[p]) \to H^1(K, E)[p] \to 0;$$

here by $H^1(K, E)$ we mean $H^1\big(K, E(\bar{K})\big)$. The Kummer map is given explicitly as follows: for $P \in E(K)$, fix $Q \in E(\bar{K})$ such that $pQ = P$. Then the cocycle $\kappa(P)$ sends $\sigma \in G_K$ to $\sigma(Q) - Q \in E[p]$. (One checks that changing the choice of Q changes this cocycle by a coboundary.)

We define the *geometric* local Selmer structure $\mathcal{F}$ on $E[p]$ by setting

$$H_{f,\mathcal{F}}(K, E[p]) = \operatorname{im} \kappa.$$

We will need the following two facts (see [1, Chapter 1]):

Duality: The Cartier dual of the geometric structure is the geometric structure. (This makes sense since $E[p]^* \cong E[p]$.)

Compatibility: If E has good reduction over K and $l \neq p$, then $E[p]$ is an unramified $E[p]$-module and the geometric structure agrees with the unramified structure.

3. Global cohomology groups

3.1. **Selmer groups.** Let K be a number field. For a place v of K we write K_v for the completion of K at v; we write G_v and I_v for the absolute Galois group and inertia group of K_v, respectively. We also write $\mathbf{F}_v$ for the residue field of $\mathcal{O}_{K_v}$. We fix an embedding $\bar{K} \hookrightarrow \bar{K}_v$ for every v; this yields a restriction map $G_v \hookrightarrow G_K$.

Let T be a finite-dimensional $\mathbf{F}_p$-vector space with a discrete action of G_K. For any place v we can regard T as a G_v-module via the injection $G_v \hookrightarrow G_K$; we say that T is *unramified at* v if it is unramified as a G_v-module. Since T is finite and discrete it is unramified at almost all places v. Note that for any place v we have a restriction map

$$\begin{aligned} \operatorname{res}_v : H^1(K, T) &\to H^1(K_v, T) \\ c &\mapsto c_v \end{aligned}$$

which is in fact independent of the choice of embedding $G_v \hookrightarrow G_K$.

We define a *global Selmer structure* $\mathcal{F}$ on T to be a choice of local Selmer structures for every place of K; we further require these structures to be unramified at almost all places. Thus a global Selmer structure $\mathcal{F}$ on T is a choice of $\mathbf{F}_p$-subspace

$$H^1_{f,\mathcal{F}}(K_v, T) \subseteq H^1(K_v, T)$$

for every place of v, such that

$$H^1_{f,\mathcal{F}}(K_v, T) = H^1(K_v^{\mathrm{ur}}/K_v, T^{I_v})$$

for almost all v.

We define the *Selmer group* $\operatorname{Sel}_{\mathcal{F}}(K, T)$ to be the set of all $c \in H^1(K, T)$ such that c_v lies in $H^1_{f,\mathcal{F}}(K_v, T)$ for every place v of T. That is,

$$\operatorname{Sel}_{\mathcal{F}}(K, T) = \ker\big(H^1(K, T) \to \oplus_v H^1_{s,\mathcal{F}}(K_v, T)\big).$$

3.2. **Global cohomology of elliptic curves.** Let E be an elliptic curve over K. Since the coordinates of the p-torsion points $E[p]$ generate a finite extension of K, the Galois module $E[p]$ is discrete; in particular, it is unramified almost everywhere. (In fact, by our local discussion we know that $E[p]$ is unramified at all places of good reduction which do not divide p.) We define the *geometric* global Selmer structure $\mathcal{F}$ on $E[p]$ by letting it agree with the geometric local Selmer structure at every place of K. By our local discussion we know that this really will be a Selmer structure (since it it is the unramified structure at all places of good reduction not dividing p). We also know that the geometric structure is self-dual under the Weil pairing identification $E[p]^* \cong E[p]$.

We claim that the Selmer group $\mathrm{Sel}_{\mathcal{F}}(K, E[p])$ agrees with the usual p-torsion Selmer group $\mathrm{Sel}(K, E[p])$ (see [11, Chapter 10, Section 4]) of E sitting in an exact sequence

$$0 \to E(K)/pE(K) \to \mathrm{Sel}(K, E[p]) \to \text{Ш}(K, E)[p] \to 0 \tag{5}$$

with

$$\text{Ш}(K, E) = \ker\bigl(H^1(K, E) \to \prod_v H^1(K_v, E)\bigr).$$

Indeed, the classical $\mathrm{Sel}(K, E[p])$ is defined to be the subspace of $H^1(K, E[p])$ of classes whose restriction to $H^1(K_v, E[p])$ lie in the image of the local Kummer map κ_v for every v. This is precisely our definition of $\mathrm{Sel}_{\mathcal{F}}(K, E[p])$.

3.3. **Global duality.** Fix a G_K-module T as in Section 3.1 and a global Selmer structure $\mathcal{F}$ on T; this induces a Cartier dual Selmer structure $\mathcal{F}^*$ on T^*. We will omit these structures from our notation for the remainder of the section.

For any ideal $\mathfrak{a}$ of the ring of integers $\mathcal{O}_K$, we define groups

$$\mathrm{Sel}_{\mathfrak{a}}(K, T) = \{c \in H^1(K, T) \mid c_v \in H^1_{f,\mathcal{F}}(K_v, T) \text{ for all } v \nmid \mathfrak{a}\};$$

$$\mathrm{Sel}^{\mathfrak{a}}(K, T^*) = \{c \in H^1(K, T^*) \mid c_v \in H^1_{f,\mathcal{F}}(K_v, T^*) \text{ for all } v \text{ and } c_v = 0 \text{ for } v|\mathfrak{a}\}.$$

From these definitions we have exact sequences

$$0 \to \mathrm{Sel}(K, T) \to \mathrm{Sel}_{\mathfrak{a}}(K, T) \to \bigoplus_{v|\mathfrak{a}} H^1_s(K_v, T)$$

$$0 \to \mathrm{Sel}^{\mathfrak{a}}(K, T^*) \to \mathrm{Sel}(K, T^*) \to \bigoplus_{v|\mathfrak{a}} H^1_f(K_v, T^*).$$

The dualities (2) induce a duality between

$$\bigoplus_{v|\mathfrak{a}} H^1_s(K_v, T) \qquad \text{and} \qquad \bigoplus_{v|\mathfrak{a}} H^1_f(K_v, T^*).$$

Combining these facts, we obtain a sequence

$$\begin{aligned} 0 \to \mathrm{Sel}(K, T) \to \mathrm{Sel}_{\mathfrak{a}}(K, T) \to \bigoplus_{v|\mathfrak{a}} H^1_s(K_v, T) & \\ \to \mathrm{Sel}(K, T^*)^\vee \to \mathrm{Sel}^{\mathfrak{a}}(K, T^*)^\vee \to 0 & \end{aligned} \tag{6}$$

which is obviously exact except possibly in the middle.

Proposition 3.1. *The sequence (6) is exact.*

Proof. A proof is given in [8, Chapter 1, Theorem 4.10]; see also [9, Theorem 1.7.3]. □

It follows that for any ideal $\mathfrak{a}$ we have a short exact sequence

$$0 \to \big(\bigoplus_{v|\mathfrak{a}} H^1_s(K_v,T)\big)/\operatorname{im}\operatorname{Sel}_{\mathfrak{a}}(K,T) \to \operatorname{Sel}(K,T^*)^\vee \to \operatorname{Sel}^{\mathfrak{a}}(K,T^*)^\vee \to 0. \tag{7}$$

In particular, if we can choose $\mathfrak{a}$ so that we can compute both of the flanking terms, we will immediately determine $\operatorname{Sel}(K,T^*)$. In the next section we will show that for appropriate $\mathfrak{a}$ it is easy to obtain a bound on $\operatorname{Sel}^{\mathfrak{a}}(K,T^*)$; this part of the argument only depends on the coarse structure of T. The difficult part is to exhibit elements in $\operatorname{Sel}_{\mathfrak{a}}(K,T)$ so as to bound the cokernel of the map

$$\operatorname{Sel}_{\mathfrak{a}}(K,T) \to \bigoplus_{v|\mathfrak{a}} H^1_s(K_v,T).$$

This is accomplished, in a few special cases, via Euler systems.

3.4. **Bounds on restricted Selmer groups I.** We will prove the result we actually need for our applications to elliptic curves in the next section. In this section we present a less cluttered version which is often useful.

We now assume that p is an odd prime. Let L/K be a finite extension of number fields and let T be a finite-dimensional $\mathbf{F}_p$-vector space with an action of $\operatorname{Gal}(L/K)$. (Of course, we can also regard T as a discrete G_K-module.) We assume that T is irreducible as a $\operatorname{Gal}(L/K)$-module; that is, T has no proper subspaces which are stable under the action of $\operatorname{Gal}(L/K)$. We wish to exhibit ideals $\mathfrak{a}$ for which we can bound $\operatorname{Sel}^{\mathfrak{a}}(K,T)$ in terms of L. (The T of this section corresponds to the T^* of the previous section.) In fact, we will use nothing special about the subspace $\operatorname{Sel}(K,T)$ of $H^1(K,T)$, so we proceed in somewhat more generality.

Suppose that $\tau \in \operatorname{Gal}(L/K)$ is an involution; that is, $\tau^2 = 1$. Associated to τ we have a decomposition $T = T^+ \oplus T^-$ where

$$T^\varepsilon = \{t \in T \mid \tau t = \varepsilon t\}$$

for $\varepsilon \in \{\pm\}$. We say that τ is *non-scalar* if both T^+ and T^- are non-zero.

Let S be a finite-dimensional $\mathbf{F}_p$-subspace of $H^1(K,T)$. If $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, we write

$$S^{\mathfrak{a}} = \{s \in S \mid s_v = 0 \text{ in } H^1(K_v,T) \text{ for all } v|\mathfrak{a}\}.$$

Since S is finite we can choose a finite Galois extension M of L such that S lies in the image of $H^1(M/K,T)$ under inflation. We fix such an M and we assume that τ extends to an involution in $\operatorname{Gal}(M/K)$ which we still write as τ. Let $\{\gamma_1,\dots,\gamma_r\}$ be a set of generators of $\operatorname{Gal}(M/L)$.

Proposition 3.2. *With notation as above, let $w_1,\dots,w_r$ be places of M such that $\operatorname{Frob}_{M/K} w_i = \tau\gamma_i$. Let v_i denote the restriction of w_i to K and set $\mathfrak{a} = v_1\cdots v_r$. Then $S^{\mathfrak{a}}$ lies in the image of $H^1(L/K,T)$ under inflation.*

The power of this result lies in the fact that in practice $H^1(L/K,T)$ is generally easily computable if L is chosen appropriately. For example, let E be an elliptic curve over $\mathbf{Q}$ and set $T = E[p]$. Take τ to be (a choice of) complex conjugation; since $p \neq 2$ it follows from the existence of the Weil pairing that τ is non-scalar on $E[p]$. Set $S = \operatorname{Sel}(\mathbf{Q},E[p])$; it is finite by the weak Mordell-Weil theorem. Let $L = \mathbf{Q}(E[p])$. If $\operatorname{Gal}(L/\mathbf{Q})$ is isomorphic to $\operatorname{GL}_2(\mathbf{F}_p)$, which is true for almost all primes p, we will see later that $H^1(L/\mathbf{Q},E[p]) = 0$. Thus in this case the proposition says that for appropriately chosen ideals $\mathfrak{a}$ of $\mathbf{Z}$, we have $\operatorname{Sel}^{\mathfrak{a}}(\mathbf{Q},E[p]) = 0$.

Proof. We begin with the inflation-restriction exact sequence

$$0 \to H^1(L/K, T) \to H^1(M/K, T) \to H^1(M/L, T)^{\mathrm{Gal}(L/K)}.$$

Since $S \subseteq H^1(M/K, T)$, to prove the proposition we must show that the image $\tilde{s} \in H^1(M/L, T)$ of any $s \in S^{\mathfrak{a}}$ is zero.

Fix an $s \in S^{\mathfrak{a}}$. Since $\mathrm{Gal}(M/L)$ acts trivially on T, we have $H^1(M/L, T) = \mathrm{Hom}(\mathrm{Gal}(M/L), T)$. We may therefore regard $\tilde{s}$ as a homomorphism $\mathrm{Gal}(M/L) \to T$. In this language, $\mathrm{Gal}(L/K)$-invariance translates to $\mathrm{Gal}(L/K)$-equivariance of $\tilde{s}$ for the conjugation action on $\mathrm{Gal}(M/L)$ and the usual action on T.

Fix one of the places $w = w_i$ of M corresponding to $\gamma = \gamma_i$ as in the statement of the proposition; that is, $\mathrm{Frob}_{M/K}\, w = \tau\gamma$. We will also write w for the induced place of L and v for the induced place of K. We have

$$\mathrm{Frob}_{L/K}\, w = \mathrm{Frob}_{M/K}\, w|_L = \tau,$$

which has order 2. Thus

$$\mathrm{Frob}_{M/L}\, w = (\mathrm{Frob}_{M/K}\, w)^2 = (\tau\gamma)^2.$$

Since $s \in S^{\mathfrak{a}}$, we know that the restriction of s to $H^1(M_w/K_v, T)$ is a coboundary. Thus the homomorphism $\tilde{s}|_{\mathrm{Gal}(M_w/L_w)}$ is zero. In particular, $\tilde{s}(\mathrm{Frob}_{M/L}\, w) = 0$; that is,

$$\tilde{s}(\tau\gamma\tau\gamma) = 0. \tag{8}$$

Since τ is an involution, $\tau\gamma\tau$ is nothing other than ${}^{\tau}\gamma$. We can thus rewrite (8) as $\tilde{s}({}^{\tau}\gamma) = -\tilde{s}(\gamma)$. Since $\tilde{s}$ is $\mathrm{Gal}(L/K)$-equivariant, this means that $\tau\tilde{s}(\gamma) = -\tilde{s}(\gamma)$. We conclude that $\tilde{s}(\gamma)$ lies in the eigenspace T^- for the action of τ on T.

Since the γ_i generate $\mathrm{Gal}(M/L)$, by applying the above argument to each of $\gamma_1, \ldots, \gamma_r$ we see that the $\mathbf{F}_p$-span of the image of $\tilde{s} : \mathrm{Gal}(M/L) \to T$ lies in T^-. Let us write this span as W. Since $\tilde{s}$ is $\mathrm{Gal}(L/K)$-equivariant and $\mathrm{Gal}(M/L)$ is stable under the conjugation action of $\mathrm{Gal}(L/K)$, W is stable under the action of $\mathrm{Gal}(L/K)$.

We have now shown that W is $\mathrm{Gal}(L/K)$-stable and lies in T^-. However, since τ is non-scalar by hypothesis, we have $T^- \neq T$; thus $W \neq T$. T is irreducible as a $\mathrm{Gal}(L/K)$-module, so this implies that $W = 0$. Thus $\tilde{s} = 0$, as desired. □

3.5. **Bounds on restricted Selmer groups II.** As in the previous section, let T be an irreducible $\mathbf{F}_p[\mathrm{Gal}(L/K)]$-module and let S be a finite-dimensional subspace of $H^1(M/K, T)$ for some finite Galois extension M of L. We introduce an intermediate field L_0 of the extension L/K, Galois over K, and we assume that the action of $\mathrm{Gal}(L/K)$ on T factors through $\mathrm{Gal}(L_0/K)$. We also assume that K is a quadratic extension of a field K_0 and that the $\mathrm{Gal}(L_0/K)$-action on T is the restriction of a $\mathrm{Gal}(L_0/K_0)$-action.

We now let τ denote an involution of $\mathrm{Gal}(M/K_0)$ which projects to the non-trivial element of $\mathrm{Gal}(K/K_0)$. (In particular, $\tau \notin \mathrm{Gal}(M/K)$.) As before we have a decomposition $T = T^+ \oplus T^-$ and we assume that both of these factors are non-zero. Note that τ also acts on $H^1(M/K, T)$ (via conjugation on $\mathrm{Gal}(M/K)$ and the usual action on T) and we have a decomposition

$$H^1(M/K, T) = H^1(M/K, T)^+ \oplus H^1(M/K, T)^-.$$

We assume that $S \subseteq H^1(M/K, T)^{\varepsilon}$ for some $\varepsilon \in \{\pm\}$.

Finally, let σ be an element of $\mathrm{Gal}(M/L_0)$ such that $\tau\sigma\tau^{-1} = \sigma^{-1}$. As before we let $\{\gamma_1, \ldots, \gamma_r\}$ be a set of generators of $\mathrm{Gal}(M/L)$.

Proposition 3.3. *With notation as above, let $w_1, \ldots, w_r$ be places of M such that $\mathrm{Frob}_{M/K_0} w_i = \tau\sigma\gamma_i$. Let v_i denote the restriction of w_i to K and set $\mathfrak{a} = v_1 \cdots v_r$. Then $S^{\mathfrak{a}}$ lies in the image of $H^1(L/K, T)^{\varepsilon}$.*

The Tchebatorev density theorem guarantees the existence of an infinite number of choices for each of the w_i above. In particular, we obtain the following corollary.

Corollary 3.4. *There is an ideal $\mathfrak{a}$ of K, divisible only by primes λ lying over primes λ_0 of K_0 with Frobenius conjugate to $\tau\sigma$ on L, such that $S^{\mathfrak{a}} \subseteq H^1(L/K, T)^{\varepsilon}$.*

In our applications to an elliptic curve E over $\mathbf{Q}$, we will take $K_0 = \mathbf{Q}$ and K will be an appropriate imaginary quadratic field. T will be the p-torsion representation $E[p]$, τ will be a complex conjugation and S will be $\mathrm{Sel}(K, E[p])^{\varepsilon}$ for some ε. We will take L_0 to be the field $K(E[p])$ or an extension of it of degree p^2; in either case, L will be a certain extension of L_0 of degree p^2. We will need the extra flexibility provided by taking σ to be non-trivial to insure that the Euler system part of our argument succeeds.

Proof. Since $S = S^{\varepsilon}$, it suffices to show that $S^{\mathfrak{a}}$ lies in the inflation of $H^1(L/K, T)$. As before, by the inflation-restriction sequence we must show that for any $s \in S^{\mathfrak{a}}$ the induced $\mathrm{Gal}(L/K)$-homomorphism $\tilde{s} : \mathrm{Gal}(M/L) \to T$ is zero. Note also that $\tilde{s}$ extends to a homomorphism $\mathrm{Gal}(M/L_0) \to T$.

Fix one of the places $w = w_i$ of M corresponding to $\gamma = \gamma_i$. We will also write w for the induced places of L and L_0 and v for the induced places of K and K_0. Note that v is inert in K/K_0 and splits completely in L_0/K. Since $\mathrm{Frob}_{M/K_0} w = \tau\sigma\gamma$ and K/K_0 is quadratic, we thus have $\mathrm{Frob}_{M/L_0} w = (\tau\sigma\gamma)^2$. Since τ is an involution we have

$$(\tau\sigma\gamma)^2 = \tau\sigma\tau\tau\gamma\tau\sigma\gamma = {}^{\tau}\sigma \cdot {}^{\tau}\gamma \cdot \sigma \cdot \gamma.$$

Since ${}^{\tau}\sigma = \sigma^{-1}$, we conclude that

$$\mathrm{Frob}_{M/L_0} w = \sigma^{-1} \cdot {}^{\tau}\gamma \cdot \sigma \cdot \gamma. \tag{9}$$

As before, since $s \in S^{\mathfrak{a}}$ we must have $\tilde{s}(\mathrm{Frob}_{M/L_0} w) = 0$. Since $\tilde{s}$ is a homomorphism on $\mathrm{Gal}(M/L_0)$, (9) now implies that

$$\tilde{s}(\sigma^{-1}) + \tilde{s}({}^{\tau}\gamma) + \tilde{s}(\sigma) + \tilde{s}(\gamma) = 0.$$

Since $\tilde{s}(\sigma^{-1}) = -\tilde{s}(\sigma)$, this implies that

$$\tilde{s}({}^{\tau}\gamma) = -\tilde{s}(\gamma). \tag{10}$$

$\tilde{s}$ need not be equivariant for the action of τ since $\tau \notin \mathrm{Gal}(L/K)$. However, since $s \in H^1(L/K, T)^{\varepsilon}$, we do have

$$\tilde{s}({}^{\tau}\gamma) = \varepsilon\tau\tilde{s}(\gamma)$$

by the definition of the τ-action on $H^1(L/K, T)$. Combining this with (10) we see that $\tilde{s}(\gamma)$ lies in $T^{-\varepsilon}$.

Let $W \subseteq T$ be the $\mathbf{F}_p$-span of $\tilde{s}(\mathrm{Gal}(M/L))$; it is $\mathrm{Gal}(L/K)$-stable since $\tilde{s}$ is $\mathrm{Gal}(L/K)$-equivariant. By the above argument applied to each of $\gamma_1, \ldots, \gamma_r$ we see that $W \subseteq T^{-\varepsilon}$. But we are assuming both that T is irreducible and that $T^{-\varepsilon} \neq T$. Thus W must be zero, and $\tilde{s} = 0$, as desired. $\square$

4. Galois cohomology calculations

4.1. **Statements.** Let E be an elliptic curve over $\mathbf{Q}$ of conductor N and let ε be the negative of the sign of the functional equation of E over $\mathbf{Q}$. We fix a modular parameterization $X_0(N) \to E$ and we let K be an imaginary quadratic field in which every prime dividing N splits. In the next section we will construct a point y_K in $E(K)$ which is mapped to $\varepsilon \cdot y_K$ (up to torsion) under complex conjugation. (If $E(K)$ has no p-torsion, then this implies that $y_K \in \left(E(K)/pE(K)\right)^{\varepsilon}$.) The main result of this paper is the following.

Theorem 4.1. *Let p be an odd prime such that:*
- *E has good reduction at p;*
- $\mathrm{Gal}(\mathbf{Q}(E[p])/\mathbf{Q}) \cong \mathrm{GL}_2(\mathbf{F}_p)$*;*
- *$y_K \notin pE(K)$.*

Then $\mathrm{Sel}(K, E[p])$ *has order p; it is generated by the image of y_K under the Kummer map.*

By Lemma 6.3 below, the second condition implies that $\mathrm{Gal}(K(E[p])/K) \cong \mathrm{GL}_2(\mathbf{F}_p)$ as well. In particular, E has no K-rational p-torsion.

Note that if y_K has infinite order then the conditions of the theorem hold for almost all p (while if y_K is torsion, then the conditions of the theorem never hold). In particular, by (5) we have the following corollary.

Corollary 4.2. *If y_K has infinite order, then $E(K)$ has rank one and $Ш(E/K)$ has trivial p-primary part for all p satisfying the conditions of the theorem.*

In this section we will use Corollary 3.4 to reduce the proof of the theorem to the construction of certain classes in $H^1(K, E[p])$. Before we can apply Corollary 3.4, however, we must compute the relevant Galois cohomology groups.

4.2. **Preliminaries.** The proof proceeds differently for the different eigenspaces of $\mathrm{Sel}(K, E[p])$ under complex conjugation. Fix a complex conjugation $\tau \in G_{\mathbf{Q}}$ and a prime p as in the theorem. We begin with the following fundamental fact.

Lemma 4.3. $\dim_{\mathbf{F}_p} E[p]^{\pm} = 1$.

Proof. Recall that the Weil pairing is a Galois equivariant perfect pairing $E[p] \otimes E[p] \to \mu_p$. Since τ acts on μ_p as inversion, the Galois equivariance implies that the Weil pairing yields a perfect pairing $E[p]^+ \otimes E[p]^- \to \mu_p$. Since at least one of $E[p]^{\pm}$ is non-zero, the result follows. □

The maps of (6) respect the action of complex conjugation; we therefore obtain exact sequences

(11)
$$\mathrm{Sel}_{\mathfrak{a}}(K, E[p])^{\pm} \to \bigoplus_{v \mid \mathfrak{a}} H^1_s(K_v, E[p])^{\pm} \to \mathrm{Sel}(K, E[p])^{\pm\vee} \to \mathrm{Sel}^{\mathfrak{a}}(K, E[p])^{\pm\vee} \to 0.$$

We will prove the theorem by choosing $\mathfrak{a}$ in such a way that we can compute all of the terms above.

Let l be a prime of $\mathbf{Q}$ which is inert in K; set $\lambda = l\mathcal{O}_K$. Then τ yields the non-trivial element of $\mathrm{Gal}(K_\lambda/\mathbf{Q}_l)$, so that we can define a conjugation action of τ on $G_\lambda = \mathrm{Gal}(\bar{K}_\lambda/K_\lambda)$ and thus on $H^1(K_\lambda, E[p])$. Furthermore, the action of τ respects $H^1_f(K_\lambda, E[p])$ (as always we are using the geometric Selmer structure for $E[p]$) so that that the eigenspaces $H^1_s(K_\lambda, E[p])^{\pm}$ are defined.

Lemma 4.4. *Let l be a prime of $\mathbf{Q}$ such that:*

- *E has good reduction at l;*
- *$l \neq p$;*
- *$\mathrm{Frob}_{K(E[p])/\mathbf{Q}}\, l$ is conjugate to τ.*

Then $H^1_s(K_\lambda, E[p])^\pm$ is a one-dimensional $\mathbf{F}_p$-vector space.

Proof. Note that l as above is inert in $K/\mathbf{Q}$ and splits completely in $K(E[p])/K$. In particular, $E[p] \subseteq E(K_\lambda)$; it follows by the Weil pairing that $\mu_p \subseteq K_\lambda^\times$. Since the geometric structure at l agrees with the unramified structure and $E[p]$ is unramified at λ, we have

$$H^1_s(K_\lambda, E[p]) \cong H^1(I_\lambda, E[p])^{G_\lambda^{\mathrm{ur}}} \cong \mathrm{Hom}(I_\lambda, E[p])^{G_\lambda^{\mathrm{ur}}}.$$

By the basic Galois theory of local fields [5, Section 8]

$$I_\lambda/pI_\lambda \cong \mathrm{Gal}(K_\lambda^{\mathrm{ur}}(l^{1/p})/K_\lambda^{\mathrm{ur}}) \cong \mu_p$$

as G_λ^{ur}-modules. Since G_λ^{ur} acts trivially on $E[p]$ and μ_p (both are defined over K_λ) we conclude that

$$H^1_s(K_\lambda, E[p]) \cong \mathrm{Hom}(\mu_p, E[p]).$$

This isomorphism respects the action of τ; since τ acts on μ_p as inversion, we find that

$$H^1_s(K_\lambda, E[p])^\pm \cong E[p]^\mp.$$

Lemma 4.3 now completes the proof. $\square$

4.3. **The $-\varepsilon$-eigenspace.** We now prepare to apply Corollary 3.4. Fix $z \in E(\bar{K})$ with $pz = y_K$. Set $K_0 = \mathbf{Q}$, $L_0 = K(E[p])$ and $L = L_0(z)$. By Lemma 4.3, τ is non-scalar on $E[p]$. Let $\kappa : E(K)/pE(K) \to H^1(K, E[p])$ be the Kummer map. Note that $\kappa(y_K)$ is non-zero (since κ is injective and $y_K \notin pE(K)$ by assumption) and lies in $H^1(L/K, E[p])$. Our first task is to compute the group $H^1(L/K, E[p])$; this is done in the next three lemmas.

Lemma 4.5. *$H^i(L_0/K, E[p]) = 0$ for all i.*

Proof. Since $\mathrm{Gal}(L_0/K) \cong \mathrm{GL}_2(\mathbf{F}_p)$, the cohomology groups we must calculate are simply $H^i\big(\mathrm{GL}_2(\mathbf{F}_p), \mathbf{F}_p^2\big)$ with the natural action of $\mathrm{GL}_2(\mathbf{F}_p)$ on $\mathbf{F}_p^2$. Let $Z = \mathbf{F}_p^\times$ be the normal subgroup of $\mathrm{GL}_2(\mathbf{F}_p)$ of scalars; there is a spectral sequence

$$H^p\big(\mathrm{PGL}_2(\mathbf{F}_p), H^q(Z, \mathbf{F}_p^2)\big) \Rightarrow H^{p+q}\big(\mathrm{GL}_2(\mathbf{F}_p), \mathbf{F}_p^2\big). \tag{12}$$

Since Z has order $p-1$, $H^q(Z, \mathbf{F}_p^2) = 0$ for $q > 0$; since $p \neq 2$, one computes that $H^0(Z, \mathbf{F}_p^2) = 0$ as well. The desired vanishing now follows from (12). $\square$

Lemma 4.6. *$\mathrm{Gal}(L/L_0)$ is isomorphic to $E[p]$ as a $\mathrm{Gal}(L_0/K)$-module. This isomorphism may not respect the action of τ, but one does have $\dim_{\mathbf{F}_p} \mathrm{Gal}(L/L_0)^\pm = 1$.*

Proof. The cocycle $\kappa(y_K) : G_K \to E[p]$ is given by $\sigma \mapsto \sigma(z) - z$. Thus if we let $c : G_{L_0} \to E[p]$ be the $\mathrm{Gal}(L_0/K)$-equivariant restriction of $\kappa(y_K)$ to G_{L_0}, the field L is precisely the kernel of c. We must show that c is surjective.

It follows from Lemma 4.5 that restriction yields an isomorphism

$$H^1(K, E[p]) \cong \mathrm{Hom}(G_{L_0}, E[p])^{\mathrm{Gal}(L_0/K)}.$$

Since $y_K \notin pE(K)$ we have $\kappa(y_K) \neq 0$; thus the homomorphism c is non-zero as well. Since it is $\mathrm{Gal}(L_0/K)$-equivariant and $\mathrm{Gal}(L_0/K)$ acts transitively on $E[p]$, the surjectivity follows. $\square$

Lemma 4.7. $H^1(L/K, E[p]) \cong \mathbf{F}_p \cdot \kappa(y_K)$.

Proof. Lemma 4.5 and the inflation-restriction sequence for the tower $L/L_0/K$ yield an isomorphism

$$H^1(L/K, E[p]) \cong H^1(L/L_0, E[p])^{\mathrm{Gal}(L_0/K)}.$$

$\mathrm{Gal}(L/L_0)$ acts trivially on $E[p]$, so by Lemma 4.6 this is just the $\mathrm{Gal}(L_0/K)$-invariants of $\mathrm{Hom}(E[p], E[p])$. Since $\mathrm{Gal}(L_0/K) \cong \mathrm{GL}_2(\mathbf{F}_p)$, one computes directly that these invariants consist precisely of the one-dimensional space of scalars in $\mathrm{Hom}(E[p], E[p])$. Thus $H^1(L/K, E[p])$ has dimension one as an $\mathbf{F}_p$-vector space. Since $\kappa(y_K)$ is a non-zero element of $H^1(L/K, E[p])$, this completes the proof. $\square$

We will give the proof of the next proposition in Section 6.

Proposition 4.8. *Assume that $y_K \notin pE(K)$. Let l be a prime of $\mathbf{Q}$ which has $\mathrm{Frob}_{L_0/\mathbf{Q}}\, l$ conjugate to complex conjugation and which does not split completely in L/L_0; set $\lambda = l\mathcal{O}_K$. Then there exists a cohomology class $c(l) \in \mathrm{Sel}_\lambda(K, E[p])^{-\varepsilon}$ with $c(l)^s_\lambda \neq 0$ in $H^1_s(K_\lambda, E[p])$.*

We can now give the proof of the following portion of the main theorem.

Theorem 4.9. $\mathrm{Sel}(K, E[p])^{-\varepsilon} = 0$.

Proof. By Lemma 4.6 we can choose a nontrivial $\sigma \in \mathrm{Gal}(L/L_0)^-$; thus $\tau\sigma\tau^{-1} = \sigma^{-1}$. We may now apply Corollary 3.4 with $S = \mathrm{Sel}(K, E[p])^{-\varepsilon}$. (Note that $E[p]$ is irreducible as a $\mathrm{Gal}(L_0/K)$-module since $\mathrm{Gal}(L_0/K) \cong \mathrm{GL}_2(\mathbf{F}_p)$.) We conclude that there exist primes $l_1, \dots, l_r$ of $\mathbf{Q}$ with $\mathrm{Frob}_{L/\mathbf{Q}}\, l_i$ conjugate to $\tau\sigma$ and such that

$$\mathrm{Sel}^{\mathfrak{a}}(K, E[p])^{-\varepsilon} \subseteq H^1(L/K, E[p])^{-\varepsilon};$$

here $\mathfrak{a} = \lambda_1 \cdots \lambda_r$ with $\lambda_i = l_i\mathcal{O}_K$. By Lemma 4.7 we know that $H^1(L/K, E[p])$ has dimension one, with generator $\kappa(y_K)$. Since κ commutes with complex conjugation and $y_K \in \big(E(K)/pE(K)\big)^\varepsilon$, we have $\kappa(y_K) \in H^1(L/K, E[p])^\varepsilon$. Thus

$$H^1(L/K, E[p])^{-\varepsilon} = \mathrm{Sel}^{\mathfrak{a}}(K, E[p])^{-\varepsilon} = 0.$$

This takes care of one of the terms in (11).

By Lemma 4.4, the vector space

$$V = \oplus_{i=1}^r H^1_s(K_{\lambda_i}, E[p])^{-\varepsilon}$$

has dimension r. Since $\mathrm{Frob}_{L/\mathbf{Q}}\, l_i$ is conjugate to $\tau\sigma$ and $\sigma \neq 1$, the primes l_i satisfy the conditions of Proposition 4.8. This yields classes $c(l_1), \dots, c(l_r) \in \mathrm{Sel}_{\mathfrak{a}}(K, E[p])^{-\varepsilon}$. Since the image of $c(l_i)$ in V is supported precisely in the one-dimensional space $H^1_s(K_\lambda, E[p])^{-\varepsilon}$, the images of $c(l_1), \dots, c(l_r)$ in V are linearly independent. Therefore they span V. Thus the map $\mathrm{Sel}_{\mathfrak{a}}(K, E[p])^{-\varepsilon} \to V$ is surjective; applying (11) completes the proof. $\square$

4.4. **The ε-eigenspace.** We now consider $\mathrm{Sel}(K, E[p])^{\varepsilon}$; the proof here is complicated somewhat by the fact that $\mathrm{Sel}(K, E[p])^{\varepsilon}$ is manifestly non-trivial, as it contains $\kappa(y_K)$.

We continue with the notation of the previous section. We begin by choosing an auxiliary prime q as in Proposition 4.8; the role it plays will only become clear in Section 6. This yields a class $c(q) \in \mathrm{Sel}_{\mathfrak{q}}(K, E[p])^{-\varepsilon}$ with $c(q)^s_{\mathfrak{q}} \neq 0$, (where $\mathfrak{q}$ is the prime of K above q). Note that $\kappa(y_K)$ and $c(q)$ are linearly independent in $H^1(K, E[p])$ since $\kappa(y_K)^s_{\mathfrak{q}} = 0$. Let L' be the fixed field of the kernel of the homomorphism $G_L \to E[p]$ obtained by restricting $c(q)$; L' is the smallest extension of L such that $c(q) \in H^1(L'/K, E[p])$.

Lemma 4.10. *$\mathrm{Gal}(L'/L)$ is isomorphic to $E[p]$ as a $\mathrm{Gal}(L/K)$-module. Furthermore, we have $\dim_{\mathbf{F}_p} \mathrm{Gal}(L'/L)^{\pm} = 1$.*

Proof. Since $c(q)$ is linearly independent from $\kappa(y_K)$, it follows from inflation-restriction and Lemma 4.7 that the restriction of $c(q)$ to G_L is non-zero. From here the proof proceeds as in Lemma 4.6; we omit the details. □

Lemma 4.11. *$H^1(L'/K, E[p]) \cong \mathbf{F}_p \cdot \kappa(y_K) \oplus \mathbf{F}_p \cdot c(q)$.*

Proof. The proof of this is quite similar to the proof of Lemma 4.7: one shows via inflation-restriction for the tower $L'/L/K$ that $H^1(L'/K, E[p])$ has dimension 2 over $\mathbf{F}_p$. The elements $\kappa(y_K)$ and $c(q)$ are linearly independent, so they must be a basis. □

We give the proof of the next proposition in Section 6. It will require the use of Theorem 4.9.

Proposition 4.12. *Assume that $y_K \notin pE(K)$. Let l be a prime of $\mathbf{Q}$ which has $\mathrm{Frob}_{L/\mathbf{Q}}\, l$ conjugate to complex conjugation and which does not split completely in L'/L; set $\lambda = l\mathcal{O}_K$. Then there exists a cohomology class $c(ql) \in \mathrm{Sel}_{\lambda}(K, E[p])^{\varepsilon}$ with $c(ql)^s_{\lambda} \neq 0$ in $H^1_s(K_{\lambda}, E[p])$.*

We can now complete the proof of the main theorem.

Theorem 4.13. $\mathrm{Sel}(K, E[p])^{\varepsilon} = \mathbf{F}_p \cdot \kappa(y_K)$.

Proof. By Lemma 4.10 we can choose a nontrivial $\sigma \in \mathrm{Gal}(L'/L)^{-}$. We now apply Corollary 3.4 with $S = \mathrm{Sel}(K, E[p])^{\varepsilon}$ and the tower of fields $L'/L/K/\mathbf{Q}$. We conclude that there exist primes $l_1, \ldots, l_r$ of $\mathbf{Q}$ such that $\mathrm{Frob}_{L'/\mathbf{Q}}\, l_i$ is conjugate to $\tau\sigma$ and such that

$$\mathrm{Sel}^{\mathfrak{a}}(K, E[p])^{\varepsilon} \subseteq H^1(L'/K, E[p])^{\varepsilon};$$

here $\mathfrak{a} = \lambda_1 \cdots \lambda_r$ with $\lambda_i = l_i \mathcal{O}_K$.

By Lemma 4.11 we know that $H^1(L'/K, E[p])$ has dimension two, with basis $\kappa(y_K)$ and $c(q)$. However, $c(q)$ lies in the $-\varepsilon$-eigenspace, so we conclude that $\mathrm{Sel}_{\mathfrak{a}}(K, E[p])^{\varepsilon}$ has dimension at most one.

As before,

$$V = \oplus_{i=1}^{r} H^1_s(K_{\lambda_i}, E[p])^{\varepsilon}$$

has dimension r. Proposition 4.12 implies that we have r elements

$$c(ql_1), \ldots, c(ql_r) \in \mathrm{Sel}_{\mathfrak{a}}(K, E[p])^{\varepsilon}$$

whose images span V. Thus the map $\mathrm{Sel}_{\mathfrak{a}}(K, E[p])^{\varepsilon} \to V$ is surjective.

We conclude by (11) that

$$\mathrm{Sel}(K, E[p])^{\varepsilon} \cong \mathrm{Sel}_{\mathfrak{a}}(K, E[p])^{\varepsilon}$$

and that these are $\mathbf{F}_p$-vector spaces of dimension at most one. Since $\kappa(y_K)$ is a non-zero element of $\mathrm{Sel}(K, E[p])^{\varepsilon}$, the theorem follows. □

It is perhaps worth noting that we can also prove Theorem 4.13 with the ideal $\mathfrak{a}\mathfrak{q} = \lambda_1 \cdots \lambda_r \mathfrak{q}$; one then has $\mathrm{Sel}^{\mathfrak{a}\mathfrak{q}}(K, E[p])^{\varepsilon} = 0$, but now the cokernel of

$$\mathrm{Sel}_{\mathfrak{a}\mathfrak{q}}(K, E[p])^{\varepsilon} \to \bigoplus_{v \mid \mathfrak{a}\mathfrak{q}} H^1_s(K_{\lambda}, E[p])^{\varepsilon}$$

has dimension 1.

It remains, then, to prove Propositions 4.8 and 4.12. This will be done via Heegner points.

5. Heegner points

5.1. **Ring class fields.** The class field theory of the field $\mathbf{Q}$ is fairly straightforward: all abelian extensions of $\mathbf{Q}$ are contained in cyclotomic extensions of $\mathbf{Q}$. An imaginary quadratic field K, however, has two kinds of abelian extensions: the cyclotomic extensions (which are still abelian over $\mathbf{Q}$) and the anti-cyclotomic extensions (which are not abelian over $\mathbf{Q}$). These anti-cyclotomic extensions are the ring class fields of K.

For proofs of the assertions of this section see [2, Section 9]. Fix an imaginary quadratic field K. For any integer n let $\mathcal{O}_n = \mathbf{Z} + n\mathcal{O}_K$ be the order of conductor n in $\mathcal{O}_K$. Let $I(n)$ denote the group of fractional ideals of $\mathcal{O}_K$ relatively prime to n and let $P(n)$ be the subgroup generated by principal ideals $\alpha\mathcal{O}_K$ where $\alpha \in \mathcal{O}_K$ is congruent to a rational integer modulo $n\mathcal{O}_K$. It is an elementary fact that the ideal class group $\mathrm{Pic}(\mathcal{O}_n)$ is isomorphic to the quotient $I(n)/P(n)$. This is a generalized ideal class group for K, so class field theory yields an abelian extension K_n/K, unramified away from n, such that there is an isomorphism

$$\mathrm{Pic}(\mathcal{O}_n) \xrightarrow{\simeq} \mathrm{Gal}(K_n/K) \tag{13}$$

sending a prime ideal $\lambda \in I(n)$ to its Frobenius element. This K_n is the *ring class field* of K of conductor n. Note that if l is a prime of $\mathbf{Q}$, relatively prime to n, which is inert in K, then $\lambda = l\mathcal{O}_K$ lies in $P(n)$, so it splits completely in K_n/K. As we have said, K_n is not abelian over $\mathbf{Q}$: the conjugation action of the non-trivial $\tau \in \mathrm{Gal}(K/\mathbf{Q})$ sends $\sigma \in \mathrm{Gal}(K_n/K)$ to σ^{-1}.

K_1 is simply the Hilbert class field of K. We will write G_n for $\mathrm{Gal}(K_n/K_1)$; one computes from the definitions that there is a canonical isomorphism

$$G_n \cong \mathrm{Pic}(\mathcal{O}_n)/\mathrm{Pic}(\mathcal{O}_K) \cong (\mathcal{O}_K/n\mathcal{O}_K)^{\times}/(\mathbf{Z}/n\mathbf{Z})^{\times}. \tag{14}$$

In particular, for an odd prime l which is unramified in $K/\mathbf{Q}$, G_l is cyclic and

$$[K_l : K_1] = \begin{cases} l-1 & l \text{ splits in } K; \\ l+1 & l \text{ inert in } K. \end{cases}$$

In this case K_l/K_1 is totally ramified as well. (We should at least comment that the notation G_l could in principle conflict with our earlier notation for $\mathrm{Gal}(\bar{\mathbf{Q}}_l/\mathbf{Q}_l)$. Since this latter group will never appear below, this should cause no confusion.)

Suppose that n is squarefree. By ramification considerations (or else the Chinese remainder theorem applied to (14)) we find that there is a canonical isomorphism

$$G_n \cong \prod_{l|n} G_l \tag{15}$$

which will be useful later.

5.2. **Complex multiplication.** Let N be a positive integer and consider the modular curve $X_0(N)$. (See [14] and the references given there for more details on modular curves.) Recall that the non-cuspidal $\mathbf{C}$-valued points of $X_0(N)$ classify isomorphism classes of cyclic N-isogenies $E \to E'$ of elliptic curves over $\mathbf{C}$. (A *cyclic N-isogeny* is simply a map of algebraic curves which respects the group laws and has kernel cyclic of order N.) $X_0(N)$ is a smooth projective curve which admits a model over $\mathbf{Q}$ and has good reduction at primes not dividing N. If K is a number field, the non-cuspidal K-points of $X_0(N)$ correspond to cyclic N-isogenies $E \to E'$ defined over K, but only up to isomorphism over $\bar{K}$; this subtlety can be safely ignored below.

We now fix a quadratic imaginary field K such that every prime dividing N splits completely in $K/\mathbf{Q}$. It follows that we can choose an ideal $\mathcal{N}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbf{Z}/N\mathbf{Z}$. Let D denote the discriminant of $K/\mathbf{Q}$.

Let n be an integer which is relatively prime to ND and consider the order $\mathcal{O}_n$ in K. The ideal $\mathcal{N}_n = \mathcal{N} \cap \mathcal{O}_n$ still satisfies $\mathcal{O}_n/\mathcal{N}_n \cong \mathbf{Z}/N\mathbf{Z}$. We can therefore consider the cyclic N-isogeny

$$\mathbf{C}/\mathcal{O}_n \to \mathbf{C}/\mathcal{N}_n^{-1}$$

of elliptic curves over $\mathbf{C}$ induced by the identity map on $\mathbf{C}$. We denote the corresponding $\mathbf{C}$-point of $X_0(N)$ by x_n; it is the *Heegner point* of conductor n for K. (Note that the point x_n depends on the choice of ideal $\mathcal{N}$, so it is not entirely canonical.)

The theory of complex multiplication (see [12, Chapter 2] and the references given there for more details) yields the following information on the action of $\mathrm{Aut}(\mathbf{C}/K)$ on x_n: consider the restriction of $\sigma \in \mathrm{Aut}(\mathbf{C}/K)$ to $\mathrm{Gal}(K_n/K)$ with K_n the ring class field of K of conductor N. $\sigma|_{K_n}$ corresponds to an ideal class in $\mathrm{Pic}(\mathcal{O}_n)$ under the isomorphism (13); let a_σ be any ideal in this class. Then the cyclic N-isogeny corresponding to σx_n is

$$\mathbf{C}/\mathfrak{a}_\sigma^{-1} \to \mathbf{C}/\mathcal{N}_n^{-1}\mathfrak{a}_\sigma^{-1}.$$

It follows in particular that x_n is a K_n-rational point of $X_0(N)$.

For any field $L \subseteq \bar{K}$ we let $\mathrm{Div}\, X_0(N)(L)$ denote the group of divisors on $X_0(N)(\bar{K})$ which are stable under the action of $\mathrm{Gal}(\bar{K}/L)$. For a prime l not dividing N we have the l^{th} *Hecke correspondence*

$$T_l : \mathrm{Div}\, X_0(N)(L) \to \mathrm{Div}\, X_0(N)(L)$$

sending a cyclic N-isogeny $E \to E'$ to the formal sum

$$\sum_{C \subseteq E[l]} (E/C \to E'/C)$$

of $l+1$ cyclic N-isogenies.

Let n be an integer relatively prime to ND and let l be a prime not dividing nND. There is a natural trace map

$$\mathrm{Tr}_l : \mathrm{Div}\, X_0(N)(K_{nl}) \to \mathrm{Div}\, X_0(N)(K_n)$$

sending a point of $X_0(N)(K_{nl})$ to the formal sum of its $\mathrm{Gal}(K_{nl}/K_n)$-conjugates. It follows from the main theorem of complex multiplication as given above and the definition of the Hecke correspondence that $\mathrm{Tr}_l\, x_{nl} = T_l x_n$.

Heegner points also satisfy a certain congruence which we now explain. If $L/\mathbf{Q}$ is any extension and λ is a prime of L with residue field $\mathbf{F}_\lambda$, we write

$$\mathrm{red}_\lambda : E(L_\lambda) \to E(\mathbf{F}_\lambda)$$

for reduction modulo λ.

Let l be inert in K and set $\lambda = l\mathcal{O}_K$; λ splits completely in K_n/K and is totally ramified in K_{nl}/K_n. Let λ_n be a prime of K_n above λ and let λ_{nl} be the unique prime of K_{nl} over λ_n. The residue fields $\mathbf{F}_{\lambda_n}$ and $\mathbf{F}_{\lambda_{nl}}$ at these primes are canonically isomorphic to the residue field $\mathbf{F}_\lambda = \mathcal{O}_K/\lambda$; $\mathbf{F}_\lambda$ is isomorphic to $\mathbf{F}_{l^2}$, although not canonically.

We consider the image of the Heegner points x_n, x_{nl} under the reduction maps red_{λ_n} and $\mathrm{red}_{\lambda_{nl}}$; note that both maps land in $E(\mathbf{F}_\lambda)$. The congruence (which is a fairly direct consequence of the Eichler-Shimura relation) is

$$\mathrm{red}_{\lambda_{nl}}(x_{nl}) = \mathrm{red}_{\lambda_n}\bigl(\mathrm{Frob}_{K_n/K}\,\lambda_n \cdot x_n)\bigr).$$

See [6, Proposition 3.7] for details.

We summarize these results in the following proposition.

Proposition 5.1. *Let K be as above. For every integer n relatively prime to ND there is a point $x_n \in X_0(N)(K_n)$ such that:*

- *If l is a prime not dividing nND, then we have an equality $\mathrm{Tr}_l\, x_{nl} = T_l x_n$ of divisors on $X_0(N)(K_{nl})$;*
- *If l is a prime not dividing nND which is inert in K, then we have*

$$\mathrm{red}_{\lambda_{nl}}(x_{nl}) = \mathrm{red}_{\lambda_n}\bigl(\mathrm{Frob}_{K_n/K}\,\lambda_n \cdot x_n\bigr).$$

  for any prime λ_n of K_n over λ.

5.3. **Heegner points on elliptic curves.** Let E be an elliptic curve of conductor N and let

$$\varphi : X_0(N) \to E$$

be a modular parameterization of E; φ corresponds to a normalized newform $f = \sum a_n q^n$ on $\Gamma_0(N)$. Recall that for a prime l not dividing N we have

$$a_l = l + 1 - \#E(\mathbf{F}_l).$$

Let ε be the negative of the sign of the functional equation of E over $\mathbf{Q}$; it is also the eigenvalue of f for the Atkin-Lehner involution w_N.

For any field L, φ induces a map

$$X_0(N)(L) \to E(L)$$

and we define the Heegner points of E by

$$y_n = \varphi(x_n) \in E(K_n).$$

The translation of Proposition 5.1 is the following. Note that we can regard the trace map Tr_l as a map $E(K_{nl}) \to E(K_n)$ (rather than as a map of divisors) by applying the group law on E.

Proposition 5.2. *Let E be an elliptic curve of conductor N (endowed with a fixed modular parameterization as above) and let K be an imaginary quadratic field of discriminant D in which every prime dividing N splits. Then for any integer n not dividing ND there is a point $y_n \in E(K_n)$ such that:*

- *If l is a prime not dividing nND, then $\mathrm{Tr}_l\, y_{nl} = a_l y_n$ in $E(K_n)$;*
- *If l is a prime not dividing nND which is inert in K, then we have*

$$\mathrm{red}_{\lambda_{nl}}(y_{nl}) = \mathrm{red}_{\lambda_n}\left(\mathrm{Frob}_{K_n/K}\,\lambda_n \cdot y_n\right)$$

for any prime λ_n of K_n over λ.

Furthermore, if τ is a complex conjugation, then there exists $\sigma \in \mathrm{Gal}(K_n/K)$ such that $\tau y_n = \varepsilon\sigma y_n$ in $E(K)/E(K)_{tors}$.

Proof. The fact that $\varphi \circ T_l = a_l\varphi$ is a consequence of Eichler-Shimura theory; see [3, Section 13] for a discussion. Given this, the first two statements follow from Proposition 5.1. The last statement follows from the behavior of x_n under the Atkin-Lehner involution w_N; see [6, Proposition 5.3]. □

We conclude this section by defining the *basic Heegner point y_K*. It is simply the image of $y_1 \in E(K_1)$ under the trace map

$$\mathrm{Tr}_{K_1/K} : E(K_1) \to E(K).$$

We let complex conjugation act on $E(K)/pE(K)$ in the usual way.

Lemma 5.3. *Assume that $E(K)$ has no p-torsion. Then $y_K \in \left(E(K)/pE(K)\right)^{\varepsilon}$.*

Proof. Since $E(K)$ has no p-torsion, Proposition 5.2 implies that there is a $\sigma \in \mathrm{Gal}(K_1/K)$ such that $\tau y_1 = \varepsilon\sigma y_1 \in E(K)/pE(K)$. Let Tr denote the trace from K_1 to K. We have

$$\mathrm{Tr}\,\tau y_1 = \varepsilon\,\mathrm{Tr}\,\sigma y_1 \in E(K)/pE(K). \tag{16}$$

Since the conjugation action of τ on $\mathrm{Gal}(K_1/K)$ is inversion and Tr is stable under this operation, we have $\mathrm{Tr}\,\tau = \tau\,\mathrm{Tr}$. Since $\sigma \in \mathrm{Gal}(K_1/K)$, we also have $\mathrm{Tr}\,\sigma = \mathrm{Tr}$. Thus (16) becomes

$$\tau\,\mathrm{Tr}\,y_1 = \varepsilon\,\mathrm{Tr}\,y_1 \in E(K)/pE(K),$$

which is the statement of the lemma. □

6. The Euler system

6.1. **Kolyvagin's derivative operator.** We now fix an elliptic curve E of conductor N, a modular parameterization $X_0(N) \to E$, an imaginary quadratic field K and a prime p as in Section 4. This data defines a basic Heegner point $y_K \in E(K)$ and Heegner points $y_n \in E(K_n)$ for every n relatively prime to ND, with D the discriminant of $K/\mathbf{Q}$. We are also assuming that E has good reduction at p and that $\mathrm{Gal}(\mathbf{Q}(E[p])/\mathbf{Q}) \cong \mathrm{GL}_2(\mathbf{F}_p)$. We will not invoke the assumption $y_K \notin pE(K)$ until the very end of the argument.

We will now convert the Heegner points $y_n \in E(K_n)/pE(K_n)$ into cohomology classes in $H^1(K, E[n])$. The most brutal way to do this is to simply take the trace of y_n from K_n down to K and then apply the Kummer map. This approach, however, does not yield interesting cohomology classes. Instead we will apply a certain derivative operator to the y_n to obtain $\mathrm{Gal}(K_n/K_1)$-invariant elements. Applying the trace from K_1 to K will yield the desired cohomology classes.

Let $\mathcal{R}$ be the set of squarefree integers which are relatively prime to pND and which are products of primes l such that $\mathrm{Frob}_{K(E[p])/\mathbf{Q}}\, l$ is conjugate to complex conjugation. Note that such an l is inert in $K/\mathbf{Q}$ and splits completely in $K(E[p])/K$. We will only need to consider Heegner points y_n for $n \in \mathcal{R}$.

Lemma 6.1. *For every prime $l \in \mathcal{R}$, p divides $l+1$ and $a_l = l + 1 - \#E(\mathbf{F}_l)$.*

Proof. The characteristic polynomial of $\mathrm{Frob}\, l$ on $E[p]$ is $x^2 - a_l x + l$ and the characteristic polynomial of complex conjugation on $E[p]$ is $x^2 - 1$. Since $\mathrm{Frob}\, l$ is conjugate to complex conjugation on $E[p]$, these polynomials must be congruent modulo p; the lemma follows. □

For a prime $l \in \mathcal{R}$, the group $G_l = \mathrm{Gal}(K_l/K_1)$ is cyclic of order $l+1$. Fix a generator σ_l and define operators

$$D_l = \sum_{i=1}^{l} i\sigma_l^i, \qquad \mathrm{Tr}_l = \sum_{i=0}^{l} \sigma_l^i \in \mathbf{Z}[G_l].$$

Tr_l is just the trace operator for K_l/K_1. These are related by the telescoping identity

$$(\sigma_l - 1)D_l = l + 1 - \mathrm{Tr}_l\,. \tag{17}$$

For general $n \in \mathcal{R}$, we have $G_n \cong \prod_{l|n} G_l$, and we define

$$D_n = \prod_{l|n} D_l \in \mathbf{Z}[G_n].$$

We will need two more operators. Fix a set of coset representatives for the subgroup $\mathrm{Gal}(K_n/K_1)$ of $\mathrm{Gal}(K_n/K)$; let Tr (resp. Tr^{-1}) be the sum of these representatives (resp. of their inverses). If M is a $\mathbf{Z}[\mathrm{Gal}(K_n/K)]$-module and $m \in M^{G_n}$, then $\mathrm{Tr}\, m$ lies in $M^{\mathrm{Gal}(K_n/K)}$ and is independent of the choice of coset representatives above; in particular, $\mathrm{Tr}\, m = \mathrm{Tr}^{-1} m$.

We can regard all of the above operators as elements of the commutative group ring $\mathbf{Z}[\mathrm{Gal}(K_n/K)]$. These operators do not commute with complex conjugation τ; indeed, since conjugation by τ is inversion on $\mathrm{Gal}(K_n/K)$, one finds, for example, that

$$\tau\,\mathrm{Tr} = \mathrm{Tr}^{-1}\tau; \qquad \tau D_l = l\,\mathrm{Tr}_l - \sigma_l D_l \tau. \tag{18}$$

6.2. **Derived cohomology classes.** There is a natural action of the group ring $\mathbf{Z}[\mathrm{Gal}(K_n/K)]$ on $E(K_n)/pE(K_n)$. The following lemma is the main step in the construction of our desired cohomology classes.

Lemma 6.2. *For any $n \in \mathcal{R}$ we have $D_n y_n \in \big(E(K_n)/pE(K_n)\big)^{G_n}$.*

Proof. Since G_n is generated by the σ_l for l dividing n, the statement of the lemma is equivalent to the statement that

$$(\sigma_l - 1)D_n y_n \in pE(K_n)$$

for all l dividing n. Using (17) we compute that

$$\begin{aligned}(\sigma_l - 1)D_n y_n &= D_{n/l}(\sigma_l - 1)D_l y_n \\ &= D_{n/l}(l + 1 - \mathrm{Tr}_l)y_n\end{aligned}$$

in $E(K_n)$. By Proposition 5.2 this equals $D_{n/l}\big((l+1)y_n - a_l y_{n/l}\big)$. By Lemma 6.1 this lies in $pE(K_n)$, which completes the proof. □

We now define

$$P_n = \operatorname{Tr} D_n y_n \in E(K_n);$$

by Lemma 6.2, the image of P_n in $E(K_n)/pE(K_n)$ is $\mathrm{Gal}(K_n/K)$-invariant and is independent of the choice of Tr. We will use the next two lemmas to produce an element of $H^1(K, E[p])$ from P_n.

Lemma 6.3. *E has no K_n-rational p-torsion for any $n \in \mathcal{R}$.*

Proof. This is basically the statement that the groups $\mathrm{GL}_2(\mathbf{F}_p)$ and $\mathrm{Gal}(K_n/\mathbf{Q})$ are not very compatible; see [6, Lemma 4.3] for details. □

Lemma 6.4. *The restriction map*

$$\operatorname{res} : H^1(K, E[p]) \to H^1(K_n, E[p])^{\mathrm{Gal}(K_n/K)}$$

is an isomorphism.

Proof. By inflation-restriction the kernel and cokernel of this map are the groups $H^i(K_n/K, E[p]^{\mathrm{Gal}(K_n/K)})$ for $i = 1, 2$ respectively. Both of these groups vanish by Lemma 6.3, so the restriction map is an isomorphism. □

Now consider the image of P_n under the Kummer map

$$\kappa : E(K_n)/pE(K_n) \to H^1(K_n, E[p]).$$

The Kummer map is Galois equivariant, so that $\kappa(P_n) \in H^1(K_n, E[p])^{\mathrm{Gal}(K_n/K)}$, and we define $c(n) \in H^1(K, E[p])$ to be the unique class such that $\operatorname{res} c(n) = \kappa(P_n)$.

These are the cohomology classes which we need to complete our proof. We begin our investigation of them by determining how they behave under complex conjugation.

Lemma 6.5. *Let $n \in \mathcal{R}$ have k prime factors. Then $c(n) \in H^1(K, E[p])^{(-1)^k \varepsilon}$.*

Proof. Since κ and res respect the action of complex conjugation, it suffices to show that $\tau P_n = (-1)^k \varepsilon P_n$ in $E(K_n)/pE(K_n)$. In the calculations below we always work in $E(K_n)/pE(K_n)$. By (18) we have

$$\tau P_n = \tau \operatorname{Tr} \prod_{l|n} D_l y_n = \operatorname{Tr}^{-1} \prod_{l|n} (l \operatorname{Tr}_l - \sigma_l D_l) \tau y_n.$$

By Proposition 5.2 there is a $\sigma \in \mathrm{Gal}(K_n/K)$ such that $\tau y_n = (-1)^k \varepsilon \sigma y_n$ in $E(K_n)/pE(K_n)$; thus

$$\tau P_n = (-1)^k \varepsilon \sigma \operatorname{Tr}^{-1} \prod_{l|n} (l \operatorname{Tr}_l - \sigma_l D_l) y_n.$$

For each l we have $\operatorname{Tr}_l y_n = a_l y_{n/l}$; by Proposition 5.2 this is zero in $E(K_n)/pE(K_n)$. It follows that only one term survives in the above product and

$$\tau P_n = (-1)^k \varepsilon \sigma \Big(\prod_{l|n} \sigma_l\Big) \operatorname{Tr}^{-1} D_n y_n. \tag{19}$$

But $D_n y_n$ is G_n-invariant, so that $\operatorname{Tr}^{-1} D_n y_n = \operatorname{Tr} D_n y_n = P_n$. Since P_n is $\mathrm{Gal}(K_n/K)$-invariant, the other group operations in (19) are trivial; we conclude that $\tau P_n = (-1)^k \varepsilon P_n$, as claimed. □

6.3. **Ramification of the derived classes.** We begin with the fact that the class $c(n)$ is unramified away from n.

Lemma 6.6. *Fix $n = l_1 \cdots l_r \in \mathcal{R}$ and set $\lambda_i = l_i \mathcal{O}_K$. Then*

$$c(n) \in \mathrm{Sel}_{\lambda_1 \cdots \lambda_r}(K, E[p]).$$

Proof. Let v be a place of K distinct from $\lambda_1, \ldots, \lambda_r$; we must show that $c(n)_v \in H^1_f(K_v, E[n])$, or equivalently that $c(n)^s_v = 0$ in $H^1_s(K_v, E[n])$. This is straightforward if E has good reduction at v. In this case we have $H^1_s(K_v, E[p]) = \mathrm{Hom}(I_v, E[p])^{G_v^{\mathrm{ur}}}$, so that $c(n)^s_v$ is zero exactly when the restriction of $c(n)$ to I_v is trivial.

Let w be a place of K_n over v. Since v does not divide n, $K_{n,w}/K_v$ is unramified. In particular, the inertia group of $K_{n,w}$ is also I_v. We therefore have a commutative diagram

$$\begin{array}{ccccc} & & H^1(K_v, E[p]) & \longrightarrow & \mathrm{Hom}(I_v, E[p]) \\ & & \big\downarrow{\scriptstyle \mathrm{res}} & & \big\| \\ E(K_{n,w})/pE(K_{n,w}) & \xrightarrow{\kappa} & H^1(K_{n,w}, E[p]) & \longrightarrow & \mathrm{Hom}(I_v, E[p]) \end{array}$$

in which the bottom row is exact. (Both rows are just portions of the exact sequence (3) over K_v and $K_{n,w}$, respectively.) We know that $\mathrm{res}\, c(n)_v = \kappa(P_n)$, so that exactness of the bottom row shows that $(\mathrm{res}\, c(n)_v)^s$ is trivial. But then $c(n)^s_v$ is trivial as well, as claimed.

The proof at places v of bad reduction for E is somewhat more subtle and involves an analysis of the Néron model of E. We refer to [6, Proposition 6.2] for the details. ☐

We now turn to the local behavior of a class $c(n)$ at primes dividing n. The key computation is given in Lemma 6.7 below; we first set some notation. Let $nl \in \mathcal{R}$ with l prime and set $\lambda = l\mathcal{O}_K$. Since $P_{nl} \in E(K_{nl})$ is $\mathrm{Gal}(K_{nl}/K)$-invariant in $E(K_{nl})/pE(K_{nl})$, we know that $(\sigma_l - 1)P_{nl} \in pE(K_{nl})$. Since also $E(K_{nl})$ has no p-torsion, this implies that there is a unique $Q_{n,l} \in E(K_{nl})$ with $pQ_{n,l} = (\sigma_l - 1)P_{nl}$. Indeed, it is clear from the proof of Lemma 6.2 that $Q_{n,l}$ is given by the formula

$$Q_{n,l} = \frac{l+1}{p}\,\mathrm{Tr}\, D_n y_{nl} - \frac{a_l}{p} P_n; \tag{20}$$

this makes sense since $l+1$ and a_l are divisible by p.

Recall that λ splits completely in K_n/K and is totally ramified in K_{nl}/K_n. For each prime λ_n of K_n over λ, we write λ_{nl} for the unique prime of K_{nl} over λ_n. We will consider the image of $Q_{n,l}$ under the reduction map

$$\mathrm{red}_{\lambda_{nl}} : E(K_{nl,\lambda_{nl}}) \to E(\mathbf{F}_\lambda);$$

recall that $\mathbf{F}_\lambda$ is the residue field of each of λ, λ_n and λ_{nl}. Note that we also have $K_{n,\lambda_n} = K_\lambda$, so that we can consider P_n as an element of $E(K_\lambda)$.

Lemma 6.7. $\mathrm{red}_{\lambda_{nl}}(Q_{n,l})$ *is trivial in $E(\mathbf{F}_\lambda)$ if and only if $P_n \in pE(K_\lambda)$.*

Proof. We first show that

$$\mathrm{red}_{\lambda_n}(\mathrm{Tr}\, D_n y_{nl}) = \mathrm{red}_{\lambda_n}\big(\mathrm{Frob}_{K_n/K}\, \lambda_n \cdot \mathrm{Tr}\, D_n y_n\big). \tag{21}$$

This reduces immediately to showing that

$$\operatorname{red}_{\lambda_n}(\sigma y_{nl}) = \operatorname{red}_{\lambda_n}\left(\operatorname{Frob}_{K_n/K}\lambda_n \cdot \sigma y_n\right) \tag{22}$$

for any $\sigma \in \operatorname{Gal}(K_n/K)$. Note that the case $\sigma = 1$ is given in Proposition 5.2. In general, we begin with the congruence of Proposition 5.2 for the ideal $\sigma^{-1}\lambda_n$:

$$\operatorname{red}_{\sigma^{-1}\lambda_{nl}}(y_{nl}) = \operatorname{red}_{\sigma^{-1}\lambda_n}\left(\operatorname{Frob}_{K_n/K}(\sigma^{-1}\lambda_n)\cdot y_n\right).$$

Since $\operatorname{red}_{\sigma^{-1}\lambda_n} = \operatorname{red}_{\lambda_n}\circ\sigma$, this is equivalent to

$$\operatorname{red}_{\lambda_{nl}}(\sigma y_{nl}) = \operatorname{red}_{\lambda_n}\left(\sigma \operatorname{Frob}_{K_n/K}(\sigma^{-1}\lambda_n)\cdot y_n\right).$$

But $\operatorname{Frob}_{K_n/K}(\sigma^{-1}\lambda_n) = \sigma^{-1}\operatorname{Frob}_{K_n/K}(\lambda_n)\sigma$, which now completes the proof of (22) and thus of (21) as well.

Combining (21) with (20) and the fact that $\operatorname{Tr} D_n y_n = P_n$, we conclude that

$$\operatorname{red}_{\lambda_{nl}}(Q_{n,l}) = \operatorname{red}_{\lambda_n}\left(\left(\frac{l+1}{p}\operatorname{Frob} - \frac{a_l}{p}\right)P_n\right) \tag{23}$$

where we now simply write Frob for $\operatorname{Frob}_{K_n/K}\lambda_n$.

We claim that $(l+1)\operatorname{Frob} - a_l$ annihilates $E(\mathbf{F}_\lambda)$. To see this, recall that $\mathbf{F}_\lambda \cong \mathbf{F}_{l^2}$; thus Frob is an involution and we have a decomposition $E(\mathbf{F}_\lambda) = E(\mathbf{F}_\lambda)^+ \oplus E(\mathbf{F}_\lambda)^-$. We have $E(\mathbf{F}_\lambda)^+ = E(\mathbf{F}_l)$, which has order $l+1-a_l$ by definition. The Weil conjectures for elliptic curves imply that $E(\mathbf{F}_\lambda)^-$ then has order $l+1+a_l$. In either case, we see that $\pm(l+1)-a_l$ annihilates $E(\mathbf{F}_\lambda)^\pm$, so that $(l+1)\operatorname{Frob} - a_l$ annihilates $E(\mathbf{F}_\lambda)$.

Since Frob is the reduction of a complex conjugation, by the proof of Lemma 6.5 we have $\operatorname{Frob} P_n = \nu P_n + pQ$ for some $\nu \in \{\pm 1\}$ and some $Q \in E(K_n)$. Since $(l+1)\operatorname{Frob} - a_l$ annihilates $E(\mathbf{F}_\lambda)$, it follows that

$$\operatorname{red}_{\lambda_{nl}}(Q_{n,l}) = \frac{(l+1)\nu - a_l}{p}\operatorname{red}_{\lambda_n}(P_n)$$

in $E(\mathbf{F}_\lambda)^\nu$. Since $E(\mathbf{F}_\lambda)^\nu$ has order equal to the absolute value of $(l+1)\nu - a_l$, it follows that $\operatorname{red}_{\lambda_{nl}}(Q_{n,l}) = 0$ if and only if $\operatorname{red}_{\lambda_n}(P_n) \in pE(K_{n,\lambda_n})$. Since $K_\lambda = K_{n,\lambda_n}$ and the kernel of the map $E(K_\lambda) \to E(\mathbf{F}_\lambda)$ is pro-l, this is equivalent to $P_n \in pE(K_\lambda)$, as claimed. $\square$

A consequence of this lemma is the following result which is the key to the entire proof. It relates the ramification of $c(n)$ at a prime l dividing n to the behavior of the local divisibility of the point $P_{n/l}$ at l.

Lemma 6.8. *Let $nl \in \mathcal{R}$ with l prime and set $\lambda = l\mathcal{O}_K$. Then $c(nl)^s_\lambda = 0$ if and only if $P_n \in pE(K_\lambda)$.*

Proof. Since $H^1_s(K_\lambda, E[p]) = \operatorname{Hom}(I_\lambda, E[p])$, we can regard $c(nl)^s_\lambda$ as a homomorphism $I_\lambda \to E[p]$. We claim that it factors through $I_\lambda/I_{\lambda_{nl}}$ for any prime λ_{nl} of K_{nl} above λ. To see this, let $\operatorname{res} : H^1(K, E[p]) \to H^1(K_{nl}, E[p])$ be the restriction map. By definition $\operatorname{res} c(nl)$ lies in the image of the Kummer map, so that $\operatorname{res} c(nl) \in \operatorname{Sel}(K_{nl}, E[p])$. In particular, $c(nl)^s_{\lambda_{nl}} = 0$. Since $H^1_s(K_{nl,\lambda_{nl}}, E[p])$ equals $\operatorname{Hom}(I_{\lambda_{nl}}, E[p])$, we see that $c(nl)(I_{\lambda_{nl}}) = 0$, as claimed.

Since G_l is the inertia group of $\operatorname{Gal}(K_{nl}/K)$ at λ, we have $I_\lambda/I_{\lambda_{nl}} \cong G_l$. In particular, we now see that $c(nl)^s_\lambda = 0$ if and only if $c(nl)(\sigma_l) = 0$.

We now need a formula for $c(nl)$. Fix $Q \in E(\bar{K})$ with $pQ = P_{nl}$. We claim that it is represented by the cocycle $G_K \to E[p]$ given by

$$\sigma \mapsto \sigma Q - Q - \frac{1}{p}(\sigma - 1)P_{nl} \in E[p].$$

Here we know that $(\sigma - 1)P_{nl} \in pE(K_{nl})$ by Lemma 6.2 and $\frac{1}{p}(\sigma - 1)P_{nl}$ is the unique (by Lemma 6.3) p^{th} root in $E(K_{nl})$. It is easy to see that the expression above is in $E[p]$, and to check that it represents $c(nl)$ one simply needs to check that $\operatorname{res} c(nl) = \kappa(P_{nl})$; this is clear since $(\sigma - 1)P_{nl} = 0$ for $\sigma \in G_{K_{nl}}$.

Note that $c(nl)(\sigma_l)$ equals

$$\sigma_l Q - Q - Q_{n,l}. \tag{24}$$

Fix a prime $\bar{\lambda}$ of $\bar{K}$ over λ and consider the corresponding reduction map

$$\text{red} : E(\bar{K}) \to E(\bar{k}_\lambda).$$

Since E has good reduction at p, we know that this map is injective on p-torsion. In particular, $c(nl)(\sigma_l) = 0$ if and only if the reduction of (24) is trivial.

Note that $\text{red}(\sigma_l Q - Q)$ and $\text{red}(Q_{n,l})$ both lie in $E[p]$ even though neither point does prior to reduction. In fact, $\text{red}(\sigma_l Q - Q) = 0$ since σ_l lies in inertia and thus acts trivially on the residue fields. Thus

$$\text{red}(\sigma_l Q - Q - Q_{n,l}) = \text{red}(Q_{n,l}).$$

We conclude that $c(nl)(\sigma_l) = 0$ (and thus $c(nl)^s_\lambda = 0$) if and only if $\text{red}(Q_{n,l}) = 0$. Lemma 6.7 now completes the proof. □

6.4. **Final considerations.** We are now in a position to prove Propositions 4.8 and 4.12. Recall that $L_0 = K(E[p])$ and $L = K(E[p], \frac{1}{p} y_K)$.

Proposition. *Assume that $y_K \notin pE(K)$. Let l be a prime of $\mathbf{Q}$ with $\text{Frob}_{L_0/\mathbf{Q}}\, l$ conjugate to complex conjugation and which does not split completely in L/L_0; set $\lambda = l\mathcal{O}_K$. Then there exists a cohomology class $c(l) \in \text{Sel}_\lambda(K, E[p])^{-\varepsilon}$ with $c(l)^s_\lambda \neq 0$ in $H^1_s(K_\lambda, E[p])$.*

Proof. We consider the class $c(l)$ defined above via Heegner points. The fact that $c(l) \in \text{Sel}_\lambda(K, E[p])^{-\varepsilon}$ follows from Lemmas 6.6 and 6.5. It remains to check that $c(l)^s_\lambda \neq 0$ in $H^1_s(K_\lambda, E[p])$. By Lemma 6.8 this is true if and only if $P_1 \notin pE(K_\lambda)$. Note that $P_1 \in E(K)$ is precisely the point y_K. Since L is the minimal extension of L_0 in which y_K is globally divisible by p, y_K is divisible by p in $E(K_\lambda)$ precisely if λ splits completely in L/L_0. Since we are assuming that λ does not split completely in L/L_0, we have $y_K \notin pE(K_\lambda)$, which implies that $c(l)^s_\lambda \neq 0$. □

For the next result, recall that we have chosen a non-trivial $c(q) \in H^1(K, E[p])$ and we let L'/L be the minimal extension over which $c(q)$ is defined. We need the following lemma.

Lemma 6.9. *Let l be a prime with $\text{Frob}_{L/\mathbf{Q}}\, l$ conjugate to complex conjugation; set $\lambda = l\mathcal{O}_K$. Then $P_q \in pE(K_\lambda)$ if and only if l splits completely in L'/L.*

Proof. We show that both conditions are equivalent to the vanishing of $c(q)_\lambda$ in $H^1(K_\lambda, E[p])$. Note first that if l has $\text{Frob}_{L/\mathbf{Q}}\, l$ conjugate to τ, then λ splits completely in L. In particular, $L_{\lambda_L} = K_\lambda$ where λ_L is any prime of L above λ. Fix such an l and λ_L and let $\lambda_{L'}$ be a prime of L' above λ_L.

Recall that $c(q)|_{G_L}$ yields an isomorphism $c : \mathrm{Gal}(L'/L) \xrightarrow{\simeq} E[p]$. $c(q)_\lambda$ is therefore trivial precisely when $\mathrm{Gal}(L'_{\lambda_{L'}}/L_{\lambda_L})$ is trivial. This in turn is the same as λ_L splitting completely in L', as claimed.

For the other equivalence, recall that λ splits completely in the ring class field K_q. In particular, the restriction map $H^1(K, E[p]) \to H^1(K_\lambda, E[p])$ factors through $H^1(K_q, E[p])$. We therefore have a commutative diagram

$$\begin{tikzcd}
 & H^1(K,E[p]) \arrow[d] \\
E(K_q)/pE(K_q) \arrow[r, hook] \arrow[d] & H^1(K_q,E[p]) \arrow[d] \\
E(K_\lambda)/pE(K_\lambda) \arrow[r, hook] & H^1(K_\lambda,E[p])
\end{tikzcd}$$

It now follows from the definitions that $c(q)_\lambda$ is the image of $P_q \in E(K_\lambda)/pE(K_\lambda)$ under the Kummer map. The second asserted equivalence follows. $\square$

Proposition. *Assume that $y_K \notin pE(K)$. Let l be a prime of $\mathbf{Q}$ which has $\mathrm{Frob}_{L/\mathbf{Q}}\, l$ conjugate to complex conjugation and which does not split completely in L'/L; set $\lambda = l\mathcal{O}_K$. Then there exists a cohomology class $c(ql) \in \mathrm{Sel}_\lambda(K, E[p])^\varepsilon$ with $c(ql)^s_\lambda \neq 0$ in $H^1_s(K_\lambda, E[p])$.*

Proof. By Lemmas 6.6 and 6.5 we have $c(ql) \in \mathrm{Sel}_{\mathfrak{q}\lambda}(K, E[p])^\varepsilon$. The fact that $c(ql)^s_\lambda \neq 0$ follows immediately from Lemmas 6.9 and 6.8.

It remains to check that $c(ql)^s_{\mathfrak{q}} = 0$. Consider the class $c(l) \in \mathrm{Sel}_\lambda(K, E[p])^{-\varepsilon}$. Since l splits completely in L/L_0, we have $y_K \in pE(K_\lambda)$ and thus by Lemma 6.8 we have $c(l)^s_\lambda = 0$. Thus $c(l) \in \mathrm{Sel}(K, E[p])^{-\varepsilon}$. But this group is zero by Theorem 4.9. Thus $c(l) = 0$. By the construction of $c(l)$ this implies that $P_l \in pE(K_l)$. But then certainly $P_l \in pE(K_{l,\mathfrak{q}})$, so that by Lemma 6.8 we have $c(ql)^s_{\mathfrak{q}} = 0$, as claimed. $\square$

7. Examples

In this section we give some examples for the elliptic curve

$$y^2 + y = x^3 - x^2 - 10x - 20,$$

(otherwise known as $X_0(11)$; see [14]) and the imaginary quadratic field $K = \mathbf{Q}(\sqrt{-7})$. Note that K has class number 1, so that $K_1 = K$. E has bad reduction only at 11, and it is known that $\mathrm{Gal}(\mathbf{Q}(E[p])/\mathbf{Q}) \cong \mathrm{GL}_2(\mathbf{F}_p)$ for $p \neq 5$.

Set $\alpha = \frac{1+\sqrt{-7}}{2}$. In the table below we give the minimal polynomials (over K) of the Heegner points $x_n = y_n$ for $1 \leq n \leq 4$. (We suppress the various choices required to define the Heegner points.)

n	x-coordinate of y_n	y-coordinate of y_n
1	$X - \alpha$	$X + (4 - 4\alpha)$
2	$X + (14 - 17\alpha)$	$X + (-120 + 34\alpha)$
3	$X^4 + (93 - 46\alpha)X^3 +$ $(-1530 - 519\alpha)X^2 +$ $(-1816 + 5545\alpha)X +$ $(1943 - 14460\alpha)$	$X^4 + (-347 - 475\alpha)X^3 +$ $(29550 - 38190\alpha)X^2 +$ $(-95394 - 782135\alpha)X +$ $(-6593671 + 715920\alpha)$
4	$X^2 + (216 - 290\alpha)X +$ $(-1649 + 3745\omega)$	$X^2 + (8414 - 2690\alpha)X +$ $(304382 - 191230\alpha)$

In particular, the basic Heegner point y_K is $\left(\frac{1+\sqrt{-7}}{2}, -2+2\sqrt{-7}\right)$. It can be shown (via height computations) that y_K has infinite order and is not divisible by any odd primes in $E(K)$. In particular, Theorem 4.1 thus shows that $E(K)$ has rank 1 and that $\text{Ш}(E/K)$ has trivial p-primary part for $p \neq 2, 5, 11$.

References

[1] J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, Narosa Publishing House, 2000.

[2] D. Cox, *Primes of the form $x^2 + ny^2$*, John Wiley and Sons, 1989.

[3] F. Diamond and J. Im, *Modular forms and modular curves*, pp. 39–133, in: *Seminar on Fermat's last theorem*, Canadian Mathematical Society Conference Proceedings **17**, American Mathematical Society, 1995.

[4] M. Flach, *A finiteness theorem for the symmetric square of an elliptic curve*, Inventiones Mathematicae **109** (1992), pp. 307–327.

[5] A. Fröhlich, *Local fields*, pp. 1–41, in: *Algebraic number theory (Brighton 1965)*, Academic Press, 1967.

[6] B. Gross, *Kolyvagin's work on modular elliptic curves*, pp. 235–256, in: *L-functions and arithmetic (Durham 1989)*, London Mathematical Soceity Lecture Note Series **153**, Cambridge University Press, 1991.

[7] B. Mazur and T. Weston, *Euler systems and arithmetic geometry*, lecture notes from a course given in 1997, available at `http://www.math.harvard.edu/~weston/mazur.html`

[8] J. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics **1**, Academic Press, 1986.

[9] K. Rubin, *Euler systems*, Annals of Mathematics Studies **147**, Princeton University Press, 2000.

[10] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics **67**, Springer-Verlag, 1967.

[11] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, 1986.

[12] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, 1994.

[13] T. Weston, *An overview of a theorem of Flach*, in: *Arithmetic algebraic geometry*, IAS/Park City Mathematics Series, American Mathematical Society, 2001.

[14] T. Weston, *The modular curves $X_0(11)$ and $X_1(11)$*, available from the author.

Department of Mathematics, University of Michigan, 48109-1109

E-mail address: `weston@math.lsa.umich.edu`