The Euler system of Heegner points

David Kurniadi Angdinata

Spring 2022

Abstract

Gross and Zagier proved that the derivative of the Hasse-Weil L-function of an elliptic curve over an imaginary quadratic field is non-zero at 1 precisely when its Heegner point has infinite order, so that the elliptic curve has rank at least one. A few years later, Kolyvagin constructed a family of derived cohomology classes from Heegner points of higher conductors satisfying certain relations, which he terms an *Euler system*, and used these to prove that the elliptic curve has rank exactly one. His methodology involves computing the Selmer group using Galois cohomological techniques, and also gave bounds on the size of the Tate-Shafarevich group. This report outlines his main argument as documented by Gross, and is the final part in a series of three mini projects on the Birch and Swinnerton-Dyer conjecture.

Contents

1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$. The modularity theorem parameterises E with a surjective morphism $\mathrm{X}_0(N) \twoheadrightarrow E$ defined over $\mathbb{Q}$, where $N \in \mathbb{N}$ is the conductor of E and $\mathrm{X}_0(N)$ is the modular curve whose non-cuspidal points classify elliptic curves equipped with a cyclic N-isogeny.

Consider an imaginary quadratic field $F = \mathbb{Q}\left(\sqrt{-D}\right)$ satisfying the **Heegner hypothesis**, namely that all primes dividing N splits in F and its ring of integers $\mathcal{O}_F$ has unit group $\{\pm 1\}$. There are infinitely many such imaginary quadratic fields, since this is merely a congruence condition on D. Under this hypothesis, the theory of complex multiplication defines a point in $\mathrm{X}_0(N)$ rational over the Hilbert class field F^1 of F, which maps to a point $\mathfrak{h}^1 \in E\left(F^1\right)$ under the modular parameterisation. Applying the trace map $\mathrm{Tr}_1 : E\left(F^1\right) \to E(F)$ to $\mathfrak{h}^1$ yields a **basic Heegner point** $\mathfrak{h} \in E(F)$.

The Gross-Zagier formula [GZ86] establishes a direct relationship between the derivative of the Hasse-Weil L-function $\mathrm{L}_{E/F}(s)$ of E over F evaluated at $s = 1$ and the canonical height of $\mathfrak{h}$. In particular, $\mathrm{L}'_{E/F}(1)$ is non-zero precisely if $\mathfrak{h}$ has infinite order, so that the rank $\mathrm{rk}\, E(F)$ is at least one. Kolyvagin's seminal paper on Euler systems [Kol90] provides an upper bound to this.

Theorem 1.1. *If $\mathfrak{h} \in E(F)$ has infinite order, then $\mathrm{rk}\, E(F) = 1$.*

In fact, the exact statement proven by Kolyvagin included the finiteness of Tate-Shafarevich group $Ш(F, E)$, with a more precise formulation on its order [Kol90, Theorem A]. The cohomological techniques he used to bound the order of $Ш(F, E)$, which was a priori not known to be finite in any generality, became a staple example in the active study of Euler systems even to date [Rub00]. His main argument involves computing the ℓ-Selmer group $\mathrm{Sel}(F, E[\ell])$, which nests in a short exact sequence of $\mathbb{F}_\ell$-vector spaces

$$0 \to E(F)/\ell \xrightarrow{\delta} \mathrm{Sel}(F, E[\ell]) \to Ш(F, E)[\ell] \to 0.$$

Theorem 1.2. *If $\ell \in \mathbb{N}$ is an odd prime of good reduction such that $\mathrm{G}_{\mathbb{Q}(E[\ell])/\mathbb{Q}} \cong \mathrm{GL}_2 \mathbb{F}_\ell$ and $\mathfrak{h} \notin \ell E(F)$, then*

$$\mathrm{Sel}(F, E[\ell]) \cong \mathbb{F}_\ell \cdot \delta(\mathfrak{h}).$$

These assumptions on ℓ are mild, in the sense that they apply to almost all primes whenever $\mathfrak{h}$ has infinite order [Gro91, Section 2]. For instance, excluding the thirteen isomorphism classes of elliptic curves with complex multiplication, there are only finitely many primes ℓ whose ℓ-adic representation is not surjective, by Serre's theorem on the image of Galois. Under these assumptions, it follows immediately that $Ш(F, E)[\ell] = 0$, while the finiteness of all of $Ш(F, E)$ is a refinement of these arguments by further techniques to bound the orders of certain ideal class groups, of which will be omitted here.

The following short lemma will be useful to deduce Theorem 1.1 as well as for a later construction.

Lemma 1.3. *If $\ell \in \mathbb{N}$ is a prime such that $\mathrm{G}_{\mathbb{Q}(E[\ell])/\mathbb{Q}} \cong \mathrm{GL}_2 \mathbb{F}_\ell$ and K is a field linearly disjoint over $\mathbb{Q}$ to $\mathbb{Q}(E[\ell])$, then $E(K)[\ell] = 0$.*

Proof. Suppose for a contradiction that $0 \neq E(K)[\ell] \leq E[\ell] \cong \mathbb{F}_\ell^2$, so that either $E(K)[\ell] \cong \mathbb{F}_\ell$ or $E(K)[\ell] = E[\ell]$. The first case has $\mathrm{G}_{K(E[\ell])/K} \cong \mathrm{G}_{\mathbb{Q}(E[\ell])/\mathbb{Q}}$ fixing $\mathbb{F}_\ell$, while the second case has $\mathbb{Q}(E[\ell]) \subseteq K$ giving $\mathbb{Q}(E[\ell]) = \mathbb{Q}(E[\ell]) \cap K = \mathbb{Q}$, both of which are contradictions to $\mathrm{G}_{\mathbb{Q}(E[\ell])/\mathbb{Q}} \cong \mathrm{GL}_2 \mathbb{F}_\ell$. □

Theorem 1.1 then follows immediately by counting dimensions.

Proof of Theorem 1.1. Choose the odd prime ℓ such that $\ell \nmid D$, so that the primes of $\mathbb{Q}$ ramified in F and in $\mathbb{Q}(E[\ell])$ are disjoint by the Heegner hypothesis, and hence are linearly disjoint over $\mathbb{Q}$. Lemma 1.3 then implies that $E(F)[\ell] = 0$, so that $\mathrm{rk}\, E(F) = \dim_{\mathbb{F}_\ell}(E(F)/\ell)$ by tensoring over $\mathbb{F}_\ell$. This quantity is bounded below by 1 by the existence of $\mathfrak{h}$ and bounded above by 1 by Theorem 1.2. □

The remainder of this report will be a discussion of the proof of Theorem 1.2, following Weston's account [Wes01]. The following two sections will recall the construction of Selmer groups and Heegner points, defining appropriate generalisations and deriving a few basic properties from Tate duality and complex multiplication respectively. These Heegner points are used to construct a tower of cohomology classes satisfying compatibility relations, making them an Euler system, and an analysis of their local ramification behaviour places them in certain Selmer groups. The final section details a series of computations in Galois cohomology, which ultimately deduces the structure of $\mathrm{Sel}(F, E[\ell])$, thus proving Theorem 1.2.

Notation. All the assumptions in this section, particularly E, N, D, and ℓ, will prevail throughout the remaining sections. The reader is assumed to be familiar with Silverman's books on elliptic curves [Sil94; Sil09], so the notation used will be standard according to the textbooks. Any new notation introduced in the following sections will persist through the remainder of the report, unless specified otherwise. For instance, the fraktur versions of a letter denoting a prime will always be used to denote the primes above it.

2 Selmer groups and Tate duality

While the classical Selmer group may sometimes be rather difficult to compute directly, it may be nested between two generalised Selmer groups, defined by relaxing or restricting certain local conditions, which are more readily computed with an appropriate choice of local conditions. This section will define these Selmer groups and provide relevant consequences due to class field theory.

2.1 Generalised Selmer groups

Recall that the multiplication by ℓ isogeny induces the global Kummer exact sequence

$$0 \to E(F)/\ell \xrightarrow{\delta} \mathrm{H}^1(F, E[\ell]) \xrightarrow{\sigma} \mathrm{H}^1(F, E)[\ell] \to 0,$$

and for each place $v \in \mathrm{M}_F$, the local Kummer exact sequence

$$0 \to E(F_v)/\ell \xrightarrow{\delta_v} \mathrm{H}^1(F_v, E[\ell]) \xrightarrow{\sigma_v} \mathrm{H}^1(F_v, E)[\ell] \to 0.$$

For almost all places $v \in \mathrm{M}_F$, there is an alternative description of $\mathrm{H}^1(F_v, E)[\ell]$ in terms of $\mathrm{G}_v^{\mathrm{ur}} \coloneqq \mathrm{G}_v/\mathrm{I}_v$.

Lemma 2.1. *If $v \in \mathrm{M}_F^0$ is a prime of good reduction such that $v(\ell) = 0$, then*

$$\mathrm{H}^1(F_v, E)[\ell] = \mathrm{Hom}(\mathrm{I}_v, E[\ell])^{\mathrm{G}_v^{\mathrm{ur}}}.$$

Proof. Since $\mathrm{G}_v^{\mathrm{ur}} \cong \widehat{\mathbb{Z}}$ has cohomological dimension one, the inflation-restriction exact sequence reads

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{H}^1(\mathrm{G}_v^{\mathrm{ur}}, E[\ell]) & \xrightarrow{\inf_{F_v^{\mathrm{ur}}/F_v}} & \mathrm{H}^1(F_v, E[\ell]) & \xrightarrow{\mathrm{res}_{F_v^{\mathrm{ur}}/F_v}} & \mathrm{H}^1(\mathrm{I}_v, E[\ell])^{\mathrm{G}_v^{\mathrm{ur}}} & \xrightarrow{\mathrm{tra}_{F_v^{\mathrm{ur}}/F_v}} & \mathrm{H}^2\left(\mathrm{G}_v^{\mathrm{ur}}, E[\ell]^{\mathrm{I}_v}\right) \\ & & \| & & & & \| & & \| \\ & & E(F_v)/\ell & & & & \mathrm{Hom}(\mathrm{I}_v, E[\ell])^{\mathrm{G}_v^{\mathrm{ur}}} & & 0 \end{array},$$

by the assumption on v, which identifies the two cokernels. □

The classical Selmer group $\mathrm{Sel}(F, E[\ell])$ arises as the kernel of $\prod_{v \in \mathrm{M}_F} (\cdot)^v$ in the exact diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(F)/\ell & \xrightarrow{\delta} & \mathrm{H}^1(F, E[\ell]) & \xrightarrow{\sigma} & \mathrm{H}^1(F, E)[\ell] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle (\cdot)_v} & \searrow^{(\cdot)^v} & \downarrow & & \\ 0 & \longrightarrow & E(F_v)/\ell & \xrightarrow[\delta_v]{} & \mathrm{H}^1(F_v, E[\ell]) & \xrightarrow[\sigma_v]{} & \mathrm{H}^1(F_v, E)[\ell] & \longrightarrow & 0 \end{array}.$$

Two generalised Selmer groups obtained by relaxing or restricting local conditions is defined as follows.

Definition. If $S \subseteq \mathrm{M}_F$ is a finite set of places, define the **relaxed Selmer group** by

$$\mathrm{Sel}^S(F, E[\ell]) \coloneqq \ker\left(\prod_{v \in \mathrm{M}_F \setminus S} (\cdot)^v : \mathrm{H}^1(F, E[\ell]) \to \prod_{v \in \mathrm{M}_F \setminus S} \mathrm{H}^1(F_v, E)[\ell]\right),$$

and define the **restricted Selmer group** by

$$\mathrm{Sel}_S(F, E[\ell]) \coloneqq \ker\left(\prod_{v \in S} (\cdot)_v : \mathrm{Sel}^S(F, E[\ell]) \to \prod_{v \in S} \mathrm{H}^1(F_v, E[\ell])\right).$$

Notation. For ease of notation in the remainder of this section only, since the parameters F, E, and ℓ are fixed, denote $\mathrm{Sel} \coloneqq \mathrm{Sel}(F, E[\ell])$, denote $\mathrm{Sel}^S \coloneqq \mathrm{Sel}^S(F, E[\ell])$, and denote $\mathrm{Sel}_S \coloneqq \mathrm{Sel}_S(F, E[\ell])$.

Remark. In a more general context of Euler systems [Rub00, Chapter I], Rubin defines the notion of a variable *global Selmer structure* compatible with *local Selmer structures* for a p-adic Galois representation over a local field, which are used to define Selmer groups that specialise in the case of $E[\ell]$ to those defined here. Lemma 2.1 is the agreement between the *singular quotients* of local Selmer structures, the *geometric structure* induced by the Kummer sequence and the *unramified structure* induced by inflation-restriction.

In other words, for a finite set of places $S \subseteq \mathrm{M}_F$, Sel^S allows a cohomology class $c \in \mathrm{H}^1(F, E[\ell])$ to satisfy $c^v \neq 0$ for $v \in S$, while Sel^S requires a cohomology class $c \in \mathrm{H}^1(F, E[\ell])$ to further satisfy $c_v = 0$ for $v \in S$. By including a finite set of problematic places as per Lemma 2.1, namely

$$S_0 \coloneqq \left\{v \in \mathrm{M}_F^0 \;\middle|\; E \text{ has bad reduction at } v\right\} \cup \left\{v \in \mathrm{M}_F^0 \;\middle|\; v(\ell) \neq 0\right\} \cup \mathrm{M}_F^\infty,$$

the relaxed Selmer group may also be given an alternative description in terms of $\mathrm{G}_S \coloneqq \mathrm{G}_{F_S/F}$, where F_S denotes the maximal extension of F unramified outside S.

Lemma 2.2. *If $S_0 \subseteq S \subseteq \mathrm{M}_F$ is a finite set of places, then*

$$\mathrm{Sel}^S = \mathrm{H}^1(\mathrm{G}_S, E[\ell]).$$

Proof. The description in Lemma 2.1 identifies the relaxed Selmer group with

$$\mathrm{Sel}^S = \ker\left(\mathrm{H}^1(F, E[\ell]) \to \prod_{v \in \mathrm{M}_F \setminus S} \mathrm{Hom}(\mathrm{I}_v, E[\ell])\right) = \ker\left(\mathrm{res} : \mathrm{H}^1(F, E[\ell]) \to \mathrm{H}^1(F_S, E[\ell])\right),$$

since G_{F_S} is determined by I_v for all $v \in \mathrm{M}_F \setminus S$, while the inflation-restriction exact sequence reads

$$0 \to \mathrm{H}^1(\mathrm{G}_S, E[\ell]) \xrightarrow{\inf_{F_S/F}} \mathrm{H}^1(F, E[\ell]) \xrightarrow{\mathrm{res}_{F_S/F}} \mathrm{H}^1(F_S, E[\ell]),$$

which identifies the two kernels. □

2.2 An application of Tate duality

Now let $S \subseteq S' \subseteq \mathrm{M}_F$ be finite sets of places. As a consequence of Tate duality, all three kinds of Selmer groups sit in an exact sequence. To establish this, first note that they clearly satisfy the inclusions

$$\mathrm{Sel}_{S'} \subseteq \mathrm{Sel}_S \subseteq \mathrm{Sel} \subseteq \mathrm{Sel}^S \subseteq \mathrm{Sel}^{S'},$$

with equalities when $S = S' = \emptyset$, and that there are tautological exact sequences

$$0 \to \mathrm{Sel}^S \to \mathrm{Sel}^{S'} \xrightarrow{\sigma_{S,S'}} \prod_{v \in S' \setminus S} \mathrm{H}^1(F_v, E)[\ell], \tag{1}$$

and

$$0 \to \mathrm{Sel}_{S'} \to \mathrm{Sel}_S \xrightarrow{\lambda_{S,S'}} \prod_{v \in S' \setminus S} \mathrm{im}\,\delta_v. \tag{2}$$

For each place $v \in \mathrm{M}_F$, local Tate duality says that $\mathrm{H}^1(F_v, E[\ell])$ is self-dual, which descends via the local Kummer sequence to a duality between $\mathrm{im}\,\delta_v \leq \mathrm{H}^1(F_v, E[\ell])$ and $\mathrm{H}^1(F_v, E[\ell]) / \mathrm{im}\,\delta_v \cong \mathrm{H}^1(F_v, E)[\ell]$. Taking the dual of (2) gives an exact sequence

$$\prod_{v \in S' \setminus S} \mathrm{H}^1(F_v, E)[\ell] \xrightarrow{\lambda^\vee_{S,S'}} \mathrm{Sel}^\vee_S \to \mathrm{Sel}^\vee_{S'} \to 0,$$

which splices with (1) to yield a five-term complex

$$0 \to \mathrm{Sel}^S \to \mathrm{Sel}^{S'} \xrightarrow{\sigma_{S,S'}} \prod_{v \in S' \setminus S} \mathrm{H}^1(F_v, E)[\ell] \xrightarrow{\lambda^\vee_{S,S'}} \mathrm{Sel}^\vee_S \to \mathrm{Sel}^\vee_{S'} \to 0. \tag{$\mathrm{Sel}(S, S')$}$$

This is exact everywhere except possibly at the middle term, whose exactness is supplied by global Tate duality. For simplicity of notation and to compute Sel, it suffices to show exactness of $\mathrm{Sel}(\emptyset, S)$.

Proposition 2.3. *The sequence* $\mathrm{Sel}\,(\emptyset, S)$ *is exact.*

Proof. It suffices to show that $\mathrm{Sel}\,(S, S')$ is exact for $S' \coloneqq S \cup S_0$, since it furnishes an exact diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Sel}^{S'} / \mathrm{Sel} & \xrightarrow{\sigma_{\emptyset,S'}} & \displaystyle\prod_{v\in S'} \mathrm{H}^1\left(F_v, E\right)[\ell] & \xrightarrow{\lambda^\vee_{\emptyset,S'}} & \left(\mathrm{Sel} / \mathrm{Sel}_{S'}\right)^\vee & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Sel}^{S'} / \mathrm{Sel}^{S} & \xrightarrow[\sigma_{S,S'}]{} & \displaystyle\prod_{v\in S'\setminus S} \mathrm{H}^1\left(F_v, E\right)[\ell] & \xrightarrow[\lambda^\vee_{S,S'}]{} & \left(\mathrm{Sel}_S / \mathrm{Sel}_{S'}\right)^\vee & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array},$$

and an application of the snake lemma yields a short exact sequence

$$0 \to \mathrm{Sel}^{S} / \mathrm{Sel} \xrightarrow{\sigma_{\emptyset,S}} \prod_{v\in S'\setminus S} \mathrm{H}^1\left(F_v, E\right)[\ell] \xrightarrow{\lambda^\vee_{\emptyset,S}} \left(\mathrm{Sel} / \mathrm{Sel}_S\right)^\vee \to 0,$$

which is precisely the content of $\mathrm{Sel}\,(\emptyset, S)$. Now under the assumption that $S_0 \subseteq S'$, the middle three terms of the Poitou-Tate exact sequence for S', by Lemma 2.2, are identified with

$$\mathrm{Sel}^{S'} \xrightarrow{\tau_{S'}} \prod_{v\in S'} \mathrm{H}^1\left(F_v, E\left[\ell\right]\right) \xrightarrow{\tau^\vee_{S'}} \mathrm{Sel}^{S'\vee}.$$

These maps, along with the local Kummer sequence for $S' \setminus S$ and (1) for $(\emptyset, S')$, furnishes an exact diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \ker \sigma^\vee_{S,S'} & & \operatorname{im} \tau_{S'} & & \ker \lambda^\vee_{S,S'} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \displaystyle\prod_{v\in S'\setminus S} \operatorname{im}\delta_v \oplus \prod_{v\in S} \mathrm{H}^1\left(F_v, E\left[\ell\right]\right) & \xrightarrow{\iota} & \displaystyle\prod_{v\in S'} \mathrm{H}^1\left(F_v, E\left[\ell\right]\right) & \longrightarrow & \displaystyle\prod_{v\in S'\setminus S} \mathrm{H}^1\left(F_v, E\right)[\ell] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \sigma^\vee_{S,S'}} & & \downarrow{\scriptstyle \tau^\vee_{S'}} & & \downarrow{\scriptstyle \lambda^\vee_{S,S'}} & & \\
0 & \longrightarrow & \operatorname{im}\sigma^\vee_{S,S'} \oplus \displaystyle\prod_{v\in S} \mathrm{H}^1\left(F_v, E\left[\ell\right]\right) & \xrightarrow[\sigma^\vee_{\emptyset,S'}]{} & \mathrm{Sel}^{S'\vee} & \longrightarrow & \mathrm{Sel}^\vee_S & \longrightarrow & 0 \\
 & & \downarrow & & & & & & \\
 & & 0 & & & & & &
\end{array},$$

so another application of the snake lemma links the top row in a short exact sequence

$$0 \to \ker \sigma^\vee_{S,S'} \xrightarrow{\iota} \operatorname{im}\tau_{S'} \to \ker \lambda^\vee_{S,S'} \to 0.$$

Thus $\ker \lambda^\vee_{S,S'}$ is precisely the image of $\mathrm{Sel}^{S'}$ in $\prod_{v\in S'\setminus S} \mathrm{H}^1\left(F_v, E\right)[\ell]$, which is precisely $\operatorname{im}\sigma_{S,S'}$. □

Remark. Gross's proof only uses local Tate duality, instead appealing to an exact sequence in global class field theory in a later step [Gro91, Proposition 8.2], which is subsumed under the Poitou-Tate exact sequence.

Note that the exact sequence respects the action of complex conjugation $\mathfrak{c} \in \mathrm{G}_{F/\mathbb{Q}}$, so this entire argument works under a fixed eigenspace. Now the right half of $\mathrm{Sel}\,(\emptyset, S)$ induces a short exact sequence

$$0 \to \operatorname{coker}\sigma_{\emptyset,S} \xrightarrow{\lambda^\vee_{S,S'}} \mathrm{Sel}^\vee \to \mathrm{Sel}^\vee_S \to 0.$$

Since these are all finite-dimensional $\mathbb{F}_\ell$-vector spaces, their duals have the same dimensions, so Sel is determined completely by $\operatorname{coker}\sigma_{\emptyset,S}$ and Sel_S for an appropriate choice of $S \subseteq \mathrm{M}_F$.

2.3 An application of Chebotarev density

Computing these generalised Selmer groups is only realistic with an appropriate set of primes S that satisfy congruence conditions, which are in turn guaranteed by Chebotarev density. For the remainder of the report, denote the eigenspaces of the action of complex conjugation $\mathfrak{c} \in \mathrm{G}_{F/\mathbb{Q}}$ by superscript signs. For instance, write $\mathrm{G}_{K'/K} = \mathrm{G}^{+}_{K'/K} \oplus \mathrm{G}^{-}_{K'/K}$ and $E[\ell] = E[\ell]^{+} \oplus E[\ell]^{-}$, noting that both eigenspaces of the latter are one-dimensional $\mathbb{F}_\ell$-vector spaces by virtue of the Galois equivariance of the Weil pairing $E[\ell] \times E[\ell] \to \mu_\ell$.

Lemma 2.4. *Let L be a finite extension of $F(E[\ell])$ such that*

$$\mathrm{Sel}(F, E[\ell]) \subseteq \inf_{L/F} \mathrm{H}^1(L/F, E[\ell]).$$

Let $F(E[\ell]) \subseteq K \subseteq K' \subseteq L$ be intermediate extensions, and let $\sigma \in \mathrm{G}^{-}_{K'/K}$ be a non-trivial automorphism. Then there is a finite set of primes $S \subseteq \mathrm{M}_F$ such that

$$\left(\frac{\mathfrak{p}|_{\mathbb{Q}}}{K'/\mathbb{Q}}\right) = \mathfrak{c}\sigma, \qquad \mathfrak{p} \in S,$$

and

$$\mathrm{Sel}_S(F, E[\ell]) \subseteq \inf_{K'/F} \mathrm{H}^1(K'/F, E[\ell]).$$

Proof. Let $n = [L : K']$, and let $\mathrm{G}_{L/K'} = \{\sigma_1, \ldots, \sigma_n\}$. Chebotarev density ensures the existence of infinitely many finite sets of primes $S' \coloneqq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq \mathrm{M}_L$ such that

$$\left(\frac{\mathfrak{p}_i}{L/\mathbb{Q}}\right) = \mathfrak{c}\sigma\sigma_i, \qquad i \in \{1, \ldots, n\},$$

so that any prime $\mathfrak{p} \in S \coloneqq \{\mathfrak{p}_1|_F, \ldots, \mathfrak{p}_n|_F\} \subseteq \mathrm{M}_F$ satisfies

$$\left(\frac{\mathfrak{p}|_{\mathbb{Q}}}{K'/\mathbb{Q}}\right) = \left(\frac{\mathfrak{p}|_{\mathbb{Q}}}{L/\mathbb{Q}}\right)\Big|_{K'} = \mathfrak{c}\sigma,$$

by construction. It remains to show, under the inflation-restriction exact sequence

$$0 \to \mathrm{H}^1(K'/F, E[\ell]) \xrightarrow{\inf} \mathrm{H}^1(L/F, E[\ell]) \xrightarrow{\mathrm{res}} \mathrm{H}^1(L/K', E[\ell])^{\mathrm{G}_{K'/F}},$$

that $\mathrm{res}\,\mathrm{Sel}_S(F, E[\ell]) = 0$, in other words that $(\mathrm{res}\, c)(\sigma_i) = 0$ for any $c \in \mathrm{Sel}_S(F, E[\ell])$ and any $i \in \{1, \ldots, n\}$. Note that $\mathfrak{p}_i$ remains inert in $F/\mathbb{Q}$ and splits completely in K/F, since

$$\left(\frac{\mathfrak{p}_i|_F}{F/\mathbb{Q}}\right) = \left(\frac{\mathfrak{p}_i}{L/\mathbb{Q}}\right)\Big|_F = \mathfrak{c}, \qquad \left(\frac{\mathfrak{p}_i|_K}{K/F}\right) = \left(\frac{\mathfrak{p}_i}{L/\mathbb{Q}}\right)\Big|^2_K = \mathfrak{c}^2 = 1,$$

so its inertia degree in $K/\mathbb{Q}$ is exactly two. Now the restricted condition on S implies that $(\mathrm{res}\, c)\left(\frac{\mathfrak{p}_i}{L/K'}\right) = 0$, and hence $(\mathrm{res}\, c)\left(\frac{\mathfrak{p}_i}{L/K}\right) = 0$ since $\mathrm{res}\, c$ extends to a homomorphism $\mathrm{G}_{L/K} \to E[\ell]$. Since

$$\left(\frac{\mathfrak{p}_i}{L/K}\right) = \left(\frac{\mathfrak{p}_i}{L/\mathbb{Q}}\right)^2 = (\mathfrak{c}\sigma\sigma_i)^2 = \sigma^{-1}(\mathfrak{c}\sigma_i\mathfrak{c})\,\sigma\sigma_i,$$

this is equivalent to

$$-(\mathrm{res}\, c)(\sigma_i) = (\mathrm{res}\, c)(\mathfrak{c}\sigma_i\mathfrak{c}) = \mathfrak{c}\,(\mathrm{res}\, c)(\sigma_i),$$

so $c \in \mathrm{Sel}_S(F, E[\ell])$ and $(\mathrm{res}\, c)(\sigma_i) \in E[\ell]$, and hence all of $(\mathrm{res}\, c)\left(\mathrm{G}_{L/K}\right)$, live in opposite eigenspaces under complex conjugation. The Galois invariance of $\mathrm{res}\, c \in \mathrm{H}^1(L/K, E[\ell])$ translates to Galois equivariance as a homomorphism $\mathrm{res}\, c : \mathrm{G}_{L/K} \to E[\ell]$, so $(\mathrm{res}\, c)\left(\mathrm{G}_{L/K}\right)$ is a $\mathrm{G}_{K/F}$-module. Since $E[\ell] \cong \mathbb{F}_\ell^2$ is irreducible as a $\mathrm{G}_{F(E[\ell])/F} \cong \mathrm{GL}_2\,\mathbb{F}_\ell$-module, and hence as a $\mathrm{G}_{K/F}$-module, this is only possible if $(\mathrm{res}\, c)\left(\mathrm{G}_{L/K}\right) = 0$. □

Again, this entire argument works under a fixed eigenspace. The ambient field L here is only necessary for the proof, and not for the purposes of application, since such a field always exists.

3 The Euler system of Heegner points

The basic Heegner point lies in the bottom of a tower of generalised Heegner points, which are used to derive a family of cohomology classes satisfying certain relations that make them an Euler system. This section will outline the construction of Heegner points of higher conductors, explicitly define the aforementioned Euler system, and prove local ramification behaviour of the derived classes. In an attempt to deviate from the general literature, many of the proofs in this section will be omitted for a reference or given as sketches, while the statements will be illustrated with a detailed example.

Example. The example in consideration in this section will be the elliptic curve over $\mathbb{Q}$ of conductor $N = 101$ with Cremona label 101a1, given by the minimal Weierstrass equation

$$E : y^2 + y = x^3 + x^2 - x - 1,$$

which is a model of the modular curve $\mathrm{X}_0(101)$ modulo its Fricke involution w_{101}. Its Mordell-Weil group is $\mathbb{Z} \cdot (1, 0)$, it has a prime 101 of non-split multiplicative reduction, and its ℓ-adic representations have maximal images for all primes $\ell \in \mathbb{N}$, so $\ell = 3$ is chosen arbitrarily, and its associated eigenform is

$$f_E(q) = q - 2q^3 - 2q^4 - q^5 - 2q^7 + q^9 - 2q^{11} + 4q^{12} + q^{13} + 2q^{15} + 4q^{16} + 3q^{17} - 5q^{19} + \dots,$$

so the modular parameterisation sends $\tau \in \mathrm{X}_0(101)(\mathbb{C})$ to

$$q - \frac{2}{3}q^3 - \frac{1}{2}q^4 - \frac{1}{5}q^5 - \frac{2}{7}q^7 + \frac{1}{9}q^9 - \frac{2}{11}q^{11} + \frac{1}{3}q^{12} + \frac{1}{13}q^{13} + \frac{2}{15}q^{15} + \frac{1}{4}q^{16} + \frac{3}{17}q^{17} - \frac{5}{19}q^{19} + \dots \in \mathbb{C},$$

where $q \coloneqq e^{2\pi i \tau}$. The imaginary quadratic field chosen is $F = F^1 = \mathbb{Q}\left(\sqrt{-43}\right)$, which has trivial ideal class group and has unit group $\{\pm 1\}$, and satisfies the Heegner hypothesis since $-43 \equiv 19^2 \mod 101$.

Remark. These choices were made as part of a brute-force search in SageMath and LMFDB, under the standard hypotheses, as well as assumptions for computational simplicity, namely a trivial class group for F, a Kolyvagin conductor of $p = 2$, and a maximal Galois image for $\ell = 3$. Out of the few remaining options, it seems that this is the only one with a rational y-coordinate of its Heegner point.

3.1 Heegner points of higher conductors

Recall that under the Heegner hypothesis, the theory of complex multiplication for $\mathcal{O}_F$ defines the basic Heegner point $\mathfrak{h} \in E(F)$. This construction can be generalised to define Heegner points for non-maximal orders of F. For proofs of the assertions in this section, refer to Cox's book [Cox89].

Let $\mathcal{O}_{F,n} \coloneqq \mathbb{Z} + n\mathcal{O}_F$ be the order of F of conductor $n \in \mathbb{N}$. The generalised ideal class group of $\mathcal{O}_{F,n}$ is $\mathrm{Cl}\,\mathcal{O}_{F,n} \coloneqq \mathrm{I}_{F,n}/\mathrm{P}_{F,n}$, where $\mathrm{I}_{F,n}$ is the group of fractional ideals coprime to $n\mathcal{O}_F$ and $\mathrm{P}_{F,n}$ is its subgroup generated by principal fractional ideals congruent to some integer modulo $n\mathcal{O}_F$. By the existence theorem of class field theory, there is a unique abelian extension F^n of F, called the **ring class field of F of conductor** n, whose Galois group $\mathrm{G}_{F^n/F}$ over F is isomorphic to $\mathrm{Cl}\,\mathcal{O}_{F,n}$ via the Artin map, and whose Galois group $\mathrm{G}_{F^n/\mathbb{Q}}$ over $\mathbb{Q}$ is isomorphic to $\mathrm{G}_{F^n/F} \rtimes \mathrm{G}_{F/\mathbb{Q}}$ via $\mathfrak{c}\sigma\mathfrak{c} = \sigma^{-1}$. A prime ramified in F^n/F necessarily divides $n\mathcal{O}_F$, while a prime inert in $F/\mathbb{Q}$ lies in $\mathrm{P}_{F,n}$ and hence splits completely in F^n/F. Since $\mathcal{O}_F^\times = \{\pm 1\}$, there is an isomorphism $\mathrm{G}^n \coloneqq \mathrm{G}_{F^n/F^1} \cong (\mathcal{O}_F/n)^\times / (\mathbb{Z}/n)^\times$ induced by the short exact sequence

$$1 \to (\mathbb{Z}/n)^\times \to (\mathcal{O}_F/n\mathcal{O}_F)^\times \to (\mathrm{I}_{F,n} \cap \mathrm{P}_F)/\mathrm{P}_{F,n} \to 1,$$

so that by the Chinese remainder theorem, $\mathrm{G}^n \cong \prod_{p|n} \mathrm{G}^p$ whenever n is square-free. If p remains inert in $F/\mathbb{Q}$, then clearly $\mathrm{G}^p \cong \mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times \cong \mathbb{Z}/(p+1)$, and denote its generator by $\sigma_p \in \mathrm{G}^p$.

Now let $n \in \mathbb{N}$ be coprime to ND, and let $\mathcal{N}_F \trianglelefteq \mathcal{O}_F$ be an ideal of norm N, which exists by the Heegner hypothesis, so that the ideal $\mathcal{N}_{F,n} = \mathcal{N}_F \cap \mathcal{O}_{F,n} \leq \mathcal{O}_{F,n}$ satisfies $\mathcal{O}_{F,n}/\mathcal{N}_{F,n} \cong \mathbb{Z}/N$. Since the fractional ideals $\mathcal{O}_F$ and $\mathcal{N}_F^{-1}$ are lattices in $\mathbb{C}$, they define complex elliptic curves $\mathbb{C}/\mathcal{O}_{F,n}$ and $\mathbb{C}/\mathcal{N}_{F,n}^{-1}$ related by a cyclic N-isogeny, and hence a point in $\mathrm{X}_0(N)(\mathbb{C})$ under its moduli interpretation. By construction, both $\mathbb{C}/\mathcal{O}_{F,n}$ and $\mathbb{C}/\mathcal{N}_{F,n}^{-1}$ have complex multiplication by $\mathcal{O}_F$, so the first main theorem of complex multiplication applies to give $\mathrm{j}(\mathbb{C}/\mathcal{O}_{F,n}), \mathrm{j}\left(\mathbb{C}/\mathcal{N}_{F,n}^{-1}\right) \in F^n$, where j is the j-invariant function, but these are exactly the coordinates of the point in $\mathrm{X}_0(N)(\mathbb{C})$. Applying the modular parameterisation $\mathrm{X}_0(N) \twoheadrightarrow E$ yields the **Heegner point $\mathfrak{h}_n \in E(F^n)$ of conductor** n. The basic Heegner point is then simply $\mathfrak{h} \coloneqq \mathrm{Tr}_1 \mathfrak{h}_1$.

Example. Let $\delta \coloneqq \frac{1+\sqrt{-43}}{2}$, and consider the ideal

$$\mathcal{N}_F \coloneqq \langle 101, \delta - 10 \rangle \trianglelefteq \mathcal{O}_F,$$

so that $\mathcal{O}_F/\mathcal{N}_F \cong \mathbb{Z}/101$. Then $\mathcal{N}_F$ corresponds to the point $\tau \coloneqq \frac{\delta-10}{202} \in \mathrm{X}_0(N)(\mathbb{C})$, which maps under the modular parameterisation to the basic Heegner point

$$\mathfrak{h} \coloneqq (1,0) \in E(F),$$

which happens to be twice the generator $-(0,1) \in E(\mathbb{Q})$. Now let $n = 2$, and consider the ideal

$$\mathcal{N}_{F,2} \coloneqq \langle 101, 2\delta - 20 \rangle \trianglelefteq \mathcal{O}_{F,2},$$

so that $\mathcal{O}_{F,2}/\mathcal{N}_{F,2} \cong \mathbb{Z}/101$ as well. Similarly, $\mathcal{N}_{F,2}$ corresponds to the point $\frac{\delta-10}{101} \in \mathrm{X}_0(N)(\mathbb{C})$, which maps under the modular parameterisation to the Heegner point of conductor two

$$\mathfrak{h}_2 \coloneqq (\alpha, 1) \in E\left(F^2\right),$$

where α is a generator over F of the ring class field $F^2 \coloneqq F[X]/\left\langle X^3 + X^2 - X - 3 \right\rangle$ of conductor two.

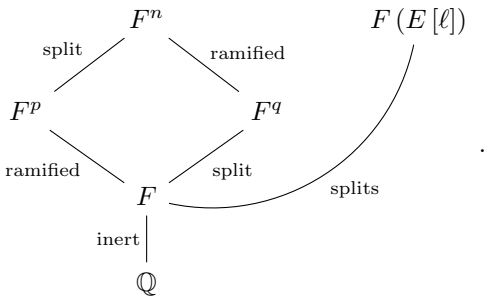
While a lot more can be said about Heegner points of any conductor, for the purposes of this report it suffices to consider **Kolyvagin conductors**, namely the square-free $n \in \mathbb{N}$ coprime to $ND\ell$ such that

$$p \mid n \text{ prime} \qquad \Longrightarrow \qquad \left(\frac{p}{F(E[\ell])/\mathbb{Q}}\right) \sim \mathfrak{c}.$$

For the remainder of this report, let $n = pq$ be a Kolyvagin conductor for some prime $p \in \mathbb{N}$ and some $q \in \mathbb{N}$. The assumption of n being a Kolyvagin conductor has several immediate consequences. In terms of ramification behaviour, p remains inert in $F/\mathbb{Q}$ since $\left(\frac{p}{F/\mathbb{Q}}\right) = \mathfrak{c}$, so that the corresponding prime $\mathfrak{p} \coloneqq p\mathcal{O}_F$ of M_F splits completely in F^q/F and totally ramifies in F^p/F. Additionally, since

$$\left(\frac{\mathfrak{p}}{F(E[\ell])/F}\right) = \left(\frac{p}{F(E[\ell])/\mathbb{Q}}\right)^2 = \mathfrak{c}^2 = 1,$$

the prime $\mathfrak{p}$ also splits completely in $F(E[\ell])/F$. All this is summarised in the diagram



.

Now since ℓ is odd and $\left(\frac{p}{F/\mathbb{Q}}\right) = \mathfrak{c}$, their characteristic polynomials $X^2 - \mathrm{a}_p X + p = 0$ and $X^2 - 1 = 0$ acting on $E[\ell] \cong \mathbb{F}_\ell^2$ are congruent modulo ℓ, so there are congruences

$$\mathrm{a}_p \equiv 0 \mod \ell, \qquad p + 1 \equiv 0 \mod \ell.$$

The action of $\mathfrak{c}$ also decomposes $\widetilde{E}(\mathbb{F}_\mathfrak{p}) = \widetilde{E}\left(\mathbb{F}_{p^2}\right)$ into eigenspaces $\widetilde{E}(\mathbb{F}_\mathfrak{p})^+ \oplus \widetilde{E}(\mathbb{F}_\mathfrak{p})^-$, with

$$\#\widetilde{E}(\mathbb{F}_\mathfrak{p})^+ = \#\widetilde{E}(\mathbb{F}_p) = p + 1 - \mathrm{a}_p, \qquad \#\widetilde{E}(\mathbb{F}_\mathfrak{p})^- = \deg(\mathrm{Frob}_p + [1]) = \det \mathrm{Frob}_p + 1 + \mathrm{Tr}\,\mathrm{Frob}_p = p + 1 + \mathrm{a}_p,$$

which are both divisible by ℓ, so that $\dim_{\mathbb{F}_\ell} \widetilde{E}(\mathbb{F}_\mathfrak{p})[\ell]^\pm = 1$.

Example. The prime $p = 2$ is a Kolyvagin conductor. For instance, if $\frac{a+b\sqrt{-43}}{2} \in \mathcal{O}_F$ for some $a, b \in \mathbb{Z}$ of the same parity, then $1 \equiv \sqrt{-43} \mod 2$ implies that $\left(\frac{a+b\sqrt{-43}}{2}\right)^2 \equiv \frac{a-b\sqrt{-43}}{2} = \mathfrak{c}\left(\frac{a+b\sqrt{-43}}{2}\right) \mod 2$. Since $-43 \equiv 5 \mod 8$, 2 remains inert in F, and totally ramifies in F^2 as $2 = (\alpha+1)^3$. Furthermore,

$$\widetilde{E}(\mathbb{F}_4)^+ = \{0, (1,0), (1,1)\}, \qquad \widetilde{E}(\mathbb{F}_4)^- = \{0, (0,X), (0,X+1)\},$$

where X is the generator of $\mathbb{F}_4$ over $\mathbb{F}_2$, which agrees with $\#\widetilde{E}(\mathbb{F}_4)^+ = \#\widetilde{E}(\mathbb{F}_4)^- = 3$ since $\mathrm{a}_2 = 0$.

Most importantly, the Heegner points of Kolyvagin conductors satisfy the following compatibility relations that Kolyvagin terms the axioms of an **AX3 Euler system**.

Proposition 3.1.

- $\mathrm{Tr}_p\, \mathfrak{h}_n = [\mathrm{a}_p]\, \mathfrak{h}_q$ *in* $E(F^q)$, *where* $\mathrm{Tr}_p = \sum_{i=0}^{p} \sigma_p^i$.
- $\widetilde{\mathfrak{h}_n} = \left(\frac{\mathfrak{p}_q}{F^q/F}\right) \widetilde{\mathfrak{h}_q}$ *in* $\widetilde{E}\left(\mathbb{F}_{\mathfrak{p}_q}\right)$, *where* $\mathfrak{p}_q \in \mathrm{M}_{F^q}$ *is a prime above* $\mathfrak{p}$.

Proof. This is a consequence of Eichler-Shimura theory [Gro91, Proposition 3.7]. □

Example. Let $n = p = 2$. In $E\left(F^2\right)$,

$$\mathrm{Tr}_2\, \mathfrak{h}_2 = \mathfrak{h}_2 + \sigma_2\mathfrak{h}_2 + \sigma_2^2\mathfrak{h}_2 = -\sigma_2^2\mathfrak{h}_2 + \sigma_2^2\mathfrak{h}_2 = 0 = [0]\, \mathfrak{h}.$$

In $\widetilde{E}(\mathbb{F}_4)$, the Frobenius is simply multiplication by [2], so

$$\mathfrak{h}_2 \equiv (-1,1) \equiv (13,-49) = [2]\, \mathfrak{h} \mod \alpha + 1.$$

Finally, let ϵ be the eigenvalue of the Fricke involution w_N on the eigenform f_E, which is also the negative of the sign in the functional equation satisfied by the completed Hasse-Weil L-function $\Lambda_{E/\mathbb{Q}}(s)$. The following characterises the action of complex conjugation on Heegner points in terms of ϵ.

Lemma 3.2. $\mathfrak{c}\mathfrak{h}_n = \epsilon\sigma\mathfrak{h}_n$ *in* $E(F^n)/E(F^n)_{\mathrm{tors}}$ *for some* $\sigma \in \mathrm{G}^n$.

Proof. This is an analysis of the action of w_N on $\mathrm{X}_0(N)$ [Gro91, Proposition 5.3]. □

Example. Let $n = 2$. Note that $-\epsilon$ can also be computed as the product of all local root numbers, which consists of 1 for the prime 101 of non-split multiplicative reduction and -1 for the unique archimedean place, so that $\epsilon = 1$. Then $\mathfrak{h}_2$ involves a choice between three generators of F^2 over F, so complex conjugation acts as the identity or sends one choice to another, but G^2 acts transitively on these choices.

For the remaining sections, denote $\epsilon_n \coloneqq (-1)^k \epsilon$, where k is the number of prime factors of n.

3.2 Kolyvagin derivatives and Kolyvagin classes

With a tower of Heegner points $\mathfrak{h}_n \in E(F^n)$ at hand, one may obtain cohomology classes in $\mathrm{H}^1(F, E[\ell])$ by simply taking the trace map $\mathrm{Tr}_n : E(F^n) \to E(F)$ then applying the Kummer map $\delta^n : E(F^n) \to \mathrm{H}^1(F, E[n])$, yet this brutal approach does not yield interesting cohomology classes. Instead, Kolyvagin first defines an operator on $E(F^n)$ to construct G^n-invariant elements, before applying a trace map.

Definition. If $n \in \mathbb{N}$, define the **Kolyvagin derivative** by

$$\mathrm{D}_n \coloneqq \prod_{p|n} \sum_{i=1}^{p} i\sigma_p^i \in \mathbb{Z}[\mathrm{G}^n],$$

and define the **derived Heegner point** by $\mathcal{H}_n \coloneqq \mathrm{Tr}_n\, \mathrm{D}_n \mathfrak{h}_n \in E(F^n)$, where

$$\mathrm{Tr}_n \coloneqq \sum_{\sigma \in S_n} \sigma \in \mathbb{Z}\left[\mathrm{G}_{F^n/F}\right],$$

and S_n is any set of coset representatives of $\mathrm{G}^n \leq \mathrm{G}_{F^n/F}$.

Note that $\mathcal{H}_1 = \mathfrak{h}$. By construction, the Kolyvagin derivative and the trace map satisfy formal identities in $\mathbb{Z}[\mathrm{G}^n]$, which translates to crucial properties for the derived Heegner point as a class in $E(F^n)/\ell$.

Lemma 3.3. *The operators* D_n *and* Tr_n *satisfy the telescoping identities*

$$(\sigma_p - 1)\,\mathrm{D}_p = p + 1 - \mathrm{Tr}_p, \qquad \mathfrak{c}\mathrm{D}_p = p\,\mathrm{Tr}_p - \sigma_p \mathrm{D}_p \mathfrak{c},$$

so that

$$[\mathcal{H}_n] \in (E(F^n)/\ell)^{\mathrm{G}_{F^n/F}, \epsilon_n}.$$

Proof. The identities are completely explicit computations, while the latter statement follows from another computation using Proposition 3.1 and Lemma 3.2 [Gro91, Proposition 3.6 and Proposition 5.4] □

Example. For simplicity, let $n = p = 2$, so that $\epsilon_2 = -1$, although the general case when $n > p$ is not significantly more complicated. Then

$$(\sigma_2 - 1)\,\mathrm{D}_2 = (\sigma_2 - 1)\left(\sigma_2 + 2\sigma_2^2\right) = \sigma_2^2 + 2 - \sigma_2 - 2\sigma_2^2 = 3 - \left(1 + \sigma_2 + \sigma_2^2\right) = 3 - \mathrm{Tr}_2,$$

and since $\mathfrak{c}\left(1 + \sigma_2 + \sigma_2^2\right) = 1 + \sigma_2 + \sigma_2^2$,

$$\mathfrak{c}\mathrm{D}_2 = \mathfrak{c}\left(\sigma_2 + 2\sigma_2^2\right) = 2\mathfrak{c}\left(1 + \sigma_2 + \sigma_2^2\right) - \sigma_2^2\mathfrak{c} - 2\mathfrak{c} = 2\left(1 + \sigma_2 + \sigma_2^2\right) - \sigma_2\left(\sigma_2 + 2\sigma_2^2\right)\mathfrak{c} = 2\,\mathrm{Tr}_2 - \sigma_2 \mathrm{D}_2 \mathfrak{c}.$$

By Proposition 3.1,

$$(\sigma_2 - [1])\,\mathrm{D}_2\mathfrak{h}_2 = [3]\,\mathfrak{h}_2 - \mathrm{Tr}_2\,\mathfrak{h}_2 = [3]\,\mathfrak{h}_2 \equiv 0 \mod 3E\left(F^2\right),$$

so G^2 fixes $\mathrm{D}_2\mathfrak{h}_2$, and hence $\mathrm{G}_{F^2/F}$ fixes $\mathcal{H}_2$. By Lemma 3.2, there is some $\sigma \in \mathrm{G}^2$ such that

$$\mathfrak{c}\mathcal{H}_2 = \mathrm{Tr}_2^{-1}\,\mathfrak{c}\mathrm{D}_2\mathfrak{h}_2 = \mathrm{Tr}_2^{-1}\,[2]\,\mathrm{Tr}_2\,\mathfrak{h}_2 - \mathrm{Tr}_2^{-1}\,\sigma_2\mathrm{D}_2\mathfrak{c}\mathfrak{h}_2 = -\sigma\sigma_2\,\mathrm{Tr}_2^{-1}\,\mathrm{D}_2\mathfrak{h}_2 \mod 3E\left(F^2\right).$$

Since $\mathrm{D}_2\mathfrak{h}_2$ is G^2-invariant, $\mathrm{Tr}_2^{-1}\,\mathrm{D}_2\mathfrak{h}_2 = \mathcal{H}_2$ is $\mathrm{G}_{F^2/F}$-invariant, so σ and σ_2 act trivially. Thus $\mathfrak{c}\mathcal{H}_2 \equiv -\mathcal{H}_2 \mod 3E\left(F^2\right)$, and so $\mathcal{H}_2$ lies in the negative eigenspace of $\mathfrak{c}$.

Since $E(F^n)[\ell] = 0$ by Lemma 1.3, the global Kummer sequences for F and F^n and the inflation-restriction exact sequence fit in an exact diagram

$$\begin{array}{ccccccccc}
 & & & & \mathrm{H}^1\left(\mathrm{G}_{F^n/F}, E(F^n)[\ell]\right) = 0 & & & & \\
 & & & & \downarrow{\scriptstyle \inf_{F^n/F}} & & & & \\
0 & \longrightarrow & E(F)/\ell & \xrightarrow{\delta} & \mathrm{H}^1(F, E[\ell]) & \longrightarrow & \mathrm{H}^1(F,E)[\ell] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}_{F^n/F}} & & \downarrow & & \\
0 & \longrightarrow & (E(F^n)/\ell)^{\mathrm{G}_{F^n/F}} & \xrightarrow[\delta^n]{} & \mathrm{H}^1(F^n, E[\ell])^{\mathrm{G}_{F^n/F}} & \longrightarrow & \mathrm{H}^1(F^n,E)[\ell]^{\mathrm{G}_{F^n/F}} & & \\
 & & & & \downarrow{\scriptstyle \mathrm{tra}_{F^n/F}} & & & & \\
 & & & & \mathrm{H}^2\left(\mathrm{G}_{F^n/F}, E(F^n)[\ell]\right) = 0 & & & &
\end{array},$$

so $\mathrm{res}_{F^n/F}$ is an isomorphism.

Definition. The **Kolyvagin class** $\mathrm{c}(n) \in \mathrm{H}^1(F, E[\ell])$ is the unique class such that

$$\mathrm{res}_{F^n/F}\,\mathrm{c}(n) = \delta^n\left([\mathcal{H}_n]\right).$$

Since δ^n and $\mathrm{res}_{F^n/F}$ respect the action of complex conjugation, Kolyvagin classes belongs to the ϵ_n-eigenspace of $\mathfrak{c}$ by Lemma 3.3. It is easy to see that it can be explicitly described by the cocycle

$$\begin{array}{rccl}
\mathrm{c}(n) & : & \mathrm{G}_F & \longrightarrow & E[\ell] \\
 & & \sigma & \longmapsto & \sigma\left[\dfrac{1}{\ell}\right]\mathcal{H}_n - \left[\dfrac{1}{\ell}\right]\mathcal{H}_n - \left[\dfrac{1}{\ell}\right](\sigma - [1])\,\mathcal{H}_n
\end{array},$$

which is well-defined again by Lemma 3.3. Unfortunately, cohomology classes are rather cumbersome to illustrate with an example, so the assertions in the remaining sections will be given proofs.

3.3 Local triviality of Kolyvagin classes

It remains to study the local ramification behaviour of Kolyvagin classes $\mathrm{c}(n) \in \mathrm{H}^1(F, E[\ell])$ under the maps $(\cdot)_v : \mathrm{H}^1(F, E[\ell]) \to \mathrm{H}^1(F_v, E[\ell])$ and $(\cdot)^v : \mathrm{H}^1(F, E[\ell]) \to \mathrm{H}^1(F_v, E)[\ell]$ to place them in appropriate Selmer groups, starting by proving that they vanish locally at the places away from n.

Lemma 3.4. *If $v \in \mathrm{M}_F$ and $v \nmid n$, then $\mathrm{c}(n)^v = 0$.*

Proof. Assume that v is a prime of good reduction such that $v(\ell) = 0$. Under this assumption, Lemma 2.1 identifies $\mathrm{c}(n)^v$ with a homomorphism $\mathrm{I}_v \to E[\ell]$. Since $F_{v_n}^n$ is unramified over F_v, $\left(\mathrm{res}_{F^n/F}\,\mathrm{c}(n)\right)^{v_n}$ is exactly the same homomorphism, but this is zero by exactness in the definition of $\mathrm{c}(n)$. On the other hand, the archimedean case is trivial, while the remaining finitely many cases involve a careful analysis of a Néron model of E, which is too far afield and will be omitted for a reference [Gro91, Proposition 6.2]. □

In terms of Selmer groups, this says that $\mathrm{c}(n) \in \mathrm{Sel}^S(F, E[\ell])^{\epsilon_n}$ for the finite set of primes $S = \{p\mathcal{O}_F \in \mathrm{M}_F \mid p \mid n\}$. The Kolyvagin classes for the primes dividing n do not necessarily vanish locally, but the following key computation encodes a crucial relationship between local triviality and local ℓ-divisibility.

Lemma 3.5. *If $p \mid n$ and $n = pq$, then $\mathrm{c}(n)^{\mathfrak{p}} = 0$ if and only if $\mathcal{H}_q \in \ell E(F_{\mathfrak{p}})$.*

Proof. Similarly to Lemma 3.4, Lemma 2.1 identifies $\left(\mathrm{res}_{F^n/F}\,\mathrm{c}(n)\right)^{\mathfrak{p}_n}$ with a homomorphism $\mathrm{I}_{\mathfrak{p}_n} \to E[\ell]$ that is zero by exactness, so it identifies $\mathrm{c}(n)^{\mathfrak{p}}$ with a homomorphism $\mathrm{I}_{\mathfrak{p}}/\mathrm{I}_{\mathfrak{p}_n} \to E[\ell]$. Since p splits completely in F^q/F and totally ramifies in F^n/F^q, there are canonical isomorphisms

$$\mathrm{I}_{\mathfrak{p}}/\mathrm{I}_{\mathfrak{p}_n} \cong \mathrm{G}_{F_{\mathfrak{p}_n}^{n,\mathrm{ur}}/F_{\mathfrak{p}}^{\mathrm{ur}}} \cong \mathrm{G}_{F_{\mathfrak{p}_n}^n/F_{\mathfrak{p}}} = \mathrm{G}_{F_{\mathfrak{p}_n}^n/F_{\mathfrak{p}_q}^q} \cong \mathrm{G}_{F^n/F^q} \cong \mathrm{G}^p,$$

so that $\mathrm{c}(n)^{\mathfrak{p}} = 0$ precisely if $\mathrm{c}(n)(\sigma_p) = 0$. Since the reduction map $\widetilde{\cdot} : E[\ell] \to \widetilde{E}\left(\overline{\mathbb{F}_{\mathfrak{p}}}\right)$ is injective, this is precisely if $\widetilde{\mathrm{c}(n)(\sigma_p)} = 0$ in $\widetilde{E}\left(\overline{\mathbb{F}_{\mathfrak{p}}}\right)$, which reduces under the explicit description of $\mathrm{c}(n)$ to $\left[\frac{1}{\ell}\right](\sigma_p - [1])\,\widetilde{\mathcal{H}_n} = 0$, since $\sigma_p \in \mathrm{I}_F$ acts trivially on $\widetilde{E}\left(\overline{\mathbb{F}_{\mathfrak{p}}}\right)$. Now note by Proposition 3.1 that there is an identity

$$\widetilde{\sigma\mathfrak{h}_n} = \sigma\left(\frac{\sigma^{-1}\mathfrak{p}_q}{F^q/F}\right)\widetilde{\mathfrak{h}_q} = \left(\frac{\mathfrak{p}_q}{F^q/F}\right)\widetilde{\sigma\mathfrak{h}_q}, \qquad \sigma \in \mathrm{G}_{F^q/F},$$

so that $\mathrm{Tr}_n\,\mathrm{D}_q\widetilde{\mathfrak{h}_n} = [p+1]\left(\frac{\mathfrak{p}_q}{F^q/F}\right)\widetilde{\mathcal{H}_q}$ as well. By this identity along with Proposition 3.1 again,

$$(\sigma_p - [1])\,\widetilde{\mathcal{H}_n} = \mathrm{Tr}_n\,\mathrm{D}_q\,(\sigma_p - [1])\,\mathrm{D}_p\widetilde{\mathfrak{h}_n} = [p+1]\,\mathrm{Tr}_n\,\mathrm{D}_q\widetilde{\mathfrak{h}_n} - \mathrm{Tr}_p\,\widetilde{\mathcal{H}_q} = \left([p+1]\left(\frac{\mathfrak{p}_q}{F^q/F}\right) - [\mathrm{a}_p]\right)\widetilde{\mathcal{H}_q},$$

so that $\left[\frac{1}{\ell}\right](\sigma_p - [1])\,\widetilde{\mathcal{H}_n} \in \widetilde{E}\left(\mathbb{F}_{\mathfrak{p}_q}\right) = \widetilde{E}(\mathbb{F}_{\mathfrak{p}})$ since $\mathrm{a}_p \equiv p + 1 \equiv 0 \mod \ell$. Furthermore, the Frobenius of $\mathfrak{p}_q$ is conjugate to $\mathfrak{c}$, so it acts on $\widetilde{\mathcal{H}_q}$ as $[\epsilon_q]$ by Lemma 3.2. On the other hand, $\widetilde{\mathcal{H}_q}$ generates the cyclic group $\widetilde{E}(\mathbb{F}_{\mathfrak{p}})^{\epsilon_q}/\ell \cong \widetilde{E}(\mathbb{F}_{\mathfrak{p}})[\ell]^{\epsilon_q} \cong \mathbb{F}_\ell$ by Lemma 3.3. Since $\#\widetilde{E}(\mathbb{F}_{\mathfrak{p}})^{\epsilon_q} = |(p+1)\,\epsilon_q - \mathrm{a}_p|$, it follows immediately that $\left[\frac{1}{\ell}\right](\sigma_p - 1)\,\widetilde{\mathcal{H}_n} = 0$ precisely if $\widetilde{\mathcal{H}_q} = 0$ in $\widetilde{E}(\mathbb{F}_{\mathfrak{p}})/\ell$. Now since $p \neq \ell$, there is an exact sequence

$$0 \longrightarrow \underset{\mathbb{R}}{\underset{E_1(F_{\mathfrak{p}})[\ell]}{E_1(F_{\mathfrak{p}})/\ell}} \longrightarrow E(F_{\mathfrak{p}}) \longrightarrow \widetilde{E}(\mathbb{F}_{\mathfrak{p}})[\ell] \longrightarrow 0,$$

whose first term vanishes by Lemma 1.3, so $\widetilde{\mathcal{H}_q} = 0$ in $\widetilde{E}(\mathbb{F}_{\mathfrak{p}})/\ell$ precisely if $\mathcal{H}_q = 0$ in $E(F_{\mathfrak{p}})/\ell$, or equivalently $\mathcal{H}_q \in \ell E(F_{\mathfrak{p}})$. Thus the lemma follows, through the equivalences

$$\begin{aligned} \mathrm{c}(n)^{\mathfrak{p}} = 0 \quad &\iff \quad \mathrm{c}(n)(\sigma_p) = 0 \quad \iff \quad \widetilde{\mathrm{c}(n)(\sigma_p)} = 0 \\ &\iff \quad \left[\frac{1}{\ell}\right](\sigma_p - [1])\,\widetilde{\mathcal{H}_n} = 0 \quad \iff \quad \widetilde{\mathcal{H}_q} \in \ell\widetilde{E}(\mathbb{F}_{\mathfrak{p}}) \quad \iff \quad \mathcal{H}_q \in \ell E(F_{\mathfrak{p}}). \end{aligned}$$

□

This gives an equivalent condition for $\mathrm{c}(n)^{\mathfrak{p}} = 0$ in terms of the local ℓ-divisibility of $\mathcal{H}_q$, which is reminiscent of the global ℓ-divisibility assumption $\mathfrak{h} \notin \ell E(F)$ that will be exploited in the following section.

4 Computing the Selmer group

With an Euler system of Heegner points lying in certain generalised Selmer groups, the classical Selmer group $\mathrm{Sel}(F, E[\ell])$ may then be computed using purely Galois cohomology, using the assumption $\mathfrak{h} \notin \ell E(F)$ for the first time. This section will introduce preliminary results and proceed to compute the $\pm\epsilon$ eigenspaces of the Selmer group to finally complete the proof of Theorem 1.2. Throughout, there will be a tower of fields $F \subseteq K^1 \subseteq K^2 \subseteq K^3$, where $K^1 \coloneqq F(E[\ell])$, $K^2 \coloneqq K^1\left(\left[\frac{1}{\ell}\right]\mathfrak{h}\right)$, and K^3 will be defined later. For these three fields, denote a choice of a prime in K^i above a prime $\mathfrak{p} \in \mathrm{M}_F$ by $\mathfrak{p}_{K^i} \in \mathrm{M}_{K^i}$.

4.1 Preliminary results

The following are three general lemmas, the first of which is a consequence of the Weil pairing.

Lemma 4.1. *If p is a Kolyvagin conductor, then* $\dim_{\mathbb{F}_\ell} \mathrm{H}^1(F_\mathfrak{p}, E)[\ell]^\pm = 1$.

Proof. By Galois equivariance of the Weil pairing, it suffices to show that $\mathrm{H}^1(F_\mathfrak{p}, E)[\ell]^\pm \cong E[\ell]^\mp$. The assumption of p being a Kolyvagin conductor implies that K^1/F has trivial inertia at $\mathfrak{p}$, so $E[\ell] \subseteq E(F_\mathfrak{p})$, and hence $\mu_\ell \subseteq F_\mathfrak{p}$ by the Weil pairing. Lemma 2.1 then identifies

$$\mathrm{H}^1(F_\mathfrak{p}, E)[\ell] = \mathrm{Hom}(\mathrm{I}_\mathfrak{p}, E[\ell])^{\mathrm{G}_\mathfrak{p}^{\mathrm{ur}}} = \mathrm{Hom}(\mathrm{I}_\mathfrak{p}/\ell, E[\ell])^{\mathrm{G}_\mathfrak{p}^{\mathrm{ur}}} \cong \mathrm{Hom}(\mu_\ell, E[\ell])^{\mathrm{G}_\mathfrak{p}^{\mathrm{ur}}} = \mathrm{Hom}(\mu_\ell, E[\ell]),$$

as $\mathbb{F}_\ell$-vector spaces, which respects the action of $\mathfrak{c}$, except that it acts on μ_ℓ by inversion. □

The second lemma rephrases the vanishing of a Hochschild-Lyndon-Serre spectral sequence.

Lemma 4.2. $\mathrm{H}^1\left(K^1/F, E[\ell]\right) = \mathrm{H}^2\left(K^1/F, E[\ell]\right) = 0$.

Proof. Since $\mathrm{G}_{K^1/F} \cong \mathrm{GL}_2 \mathbb{F}_\ell$, its centre $Z \coloneqq \mathrm{Z}\left(\mathrm{G}_{K^1/F}\right) \cong \mathbb{F}_\ell^\times$ has order $\ell - 1$ coprime to the order ℓ^2 of $E[\ell] \cong \mathbb{F}_\ell^2$ since $\ell > 2$, so $\mathrm{H}^i(Z, E[\ell]) = 0$ for all $i \in \mathbb{N}$. In particular, $E[\ell]^Z = 0$, so $\mathrm{H}^i(I, E[\ell]) = 0$ for all $i \in \mathbb{N}$ as well, where $I \coloneqq \mathrm{G}_{K^1/F}/Z$. The inflation-restriction exact sequence then reads

$$\begin{array}{ccccc} \mathrm{H}^1\left(I, E[\ell]^Z\right) & \xrightarrow{\inf} & \mathrm{H}^1\left(K^1/F, E[\ell]\right) & \xrightarrow{\mathrm{res}} & \mathrm{H}^1(Z, E[\ell])^I \\ \rotatebox{90}{$\cong$} & & & & \rotatebox{90}{$\cong$} \\ 0 & & & & 0 \end{array},$$

so that $\mathrm{H}^1\left(K^1/F, E[\ell]\right) = 0$, and the vanishing of $\mathrm{H}^1(Z, E[\ell])$ yields another application

$$\begin{array}{ccccc} \mathrm{H}^2\left(I, E[\ell]^Z\right) & \xrightarrow{\inf} & \mathrm{H}^2\left(K^1/F, E[\ell]\right) & \xrightarrow{\mathrm{res}} & \mathrm{H}^2(Z, E[\ell])^I \\ \rotatebox{90}{$\cong$} & & & & \rotatebox{90}{$\cong$} \\ 0 & & & & 0 \end{array},$$

so that $\mathrm{H}^2\left(K^1/F, E[\ell]\right) = 0$ as well. □

It is clear by induction that $\mathrm{H}^i\left(K^1/F, E[\ell]\right) = 0$ for all $i \in \mathbb{N}$, but only the first two dimensions will be necessary. The third lemma computes the Galois invariant endomorphisms of $E[\ell]$.

Lemma 4.3. *Under the standard* $\mathrm{G}_{K^1/F}$*-action,* $\dim_{\mathbb{F}_\ell} \mathrm{Hom}(E[\ell], E[\ell])^{\mathrm{G}_{K^1/F}} = 1$.

Proof. Since $\mathrm{G}_{K^1/F} \cong \mathrm{GL}_2 \mathbb{F}_\ell$, this is just $\mathrm{Hom}\left(\mathbb{F}_\ell^2, \mathbb{F}_\ell^2\right)^{\mathrm{GL}_2 \mathbb{F}_\ell}$, so the Galois invariance of $\mathrm{Hom}(E[\ell], E[\ell])$ translates to the equivariant homomorphisms, which clearly includes the one-dimensional subspace of scalar maps. It is easy to see that these are all the homomorphisms, by considering the matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2 \mathbb{F}_\ell,$$

so that the dimension is exactly one. □

The following two sections will proceed very similarly via invoking Lemma 2.4 to obtain certain Kolyvagin classes. By first showing that the Galois group structure of a field extension is isomorphic to $E[\ell]$, the dimension of its cohomology group over F, and hence of the restricted Selmer group, can be determined. The relaxed Selmer group is bounded by the local triviality of these Kolyvagin classes under the assumption $\mathfrak{h} \notin \ell E(F)$, and these compute the classical Selmer group by the exact sequence in Proposition 2.3.

4.2 The zero eigenspace

Apply Lemma 2.4 to the fields $K' = K^2$ and $K = K^1$ to obtain a finite set of primes $S \subseteq \mathrm{M}_F$ such that

$$\left(\frac{p}{K^2/\mathbb{Q}}\right) = \mathfrak{c}\sigma, \qquad \mathfrak{p} \in S,$$

and

$$\mathrm{Sel}_S\left(F, E\left[\ell\right]\right)^{-\epsilon} \subseteq \inf\nolimits_{K^2/F}\left(\mathrm{H}^1\left(K^2/F, E\left[\ell\right]\right)\right)^{-\epsilon}.$$

This requires a choice of a non-trivial $\sigma \in \mathrm{G}^-_{K^2/K^1}$, which is guaranteed by the following.

Lemma 4.4. *There is an isomorphism of $\mathrm{G}_{K^1/F}$-modules $\mathrm{G}_{K^2/K^1} \xrightarrow{\sim} E\left[\ell\right]$ induced by $\delta\left(\mathfrak{h}\right)$.*

Proof. By Lemma 4.2, the inflation-restriction exact sequence reads

$$\begin{array}{ccccccc} \mathrm{H}^1\left(K^1/F, E\left[\ell\right]\right) & \xrightarrow{\inf_{K^1/F}} & \mathrm{H}^1\left(F, E\left[\ell\right]\right) & \xrightarrow{\mathrm{res}_{K^1/F}} & \mathrm{H}^1\left(K^1, E\left[\ell\right]\right)^{\mathrm{G}_{K^1/F}} & \xrightarrow{\mathrm{tra}_{K^1/F}} & \mathrm{H}^2\left(K^1/F, E\left[\ell\right]\right) \\ \rotatebox{90}{$\cong$} & & & & \rotatebox{90}{$\cong$} & & \rotatebox{90}{$\cong$} \\ 0 & & & & \mathrm{Hom}\left(\mathrm{G}_{K^1}, E\left[\ell\right]\right)^{\mathrm{G}_{K^1/F}} & & 0 \end{array}.$$

The cocycle $\delta\left(\mathfrak{h}\right) \in \mathrm{H}^1\left(F, E\left[\ell\right]\right)$ restricts to a homomorphism $\mathrm{res}_{K^1/F}\,\delta\left(\mathfrak{h}\right) \in \mathrm{Hom}\left(\mathrm{G}_{K^1}, E\left[\ell\right]\right)^{\mathrm{G}_{K^1/F}}$, whose kernel is exactly G_{K^2} by definition, inducing an injection $\rho : \mathrm{G}_{K^2/K^1} \hookrightarrow E\left[\ell\right]$. Let $\sigma \in \mathrm{G}_{K^1/F}$ be such that $\rho\left(\sigma\right) \neq 0$, which is possible since $\mathfrak{h} \notin \ell E\left(F\right)$. For any $P \in E\left[\ell\right]$, there is some $\sigma' \in \mathrm{G}_{K^1/F}$ such that $P = \sigma'\left(\rho\left(\sigma\right)\right)$, since $\mathrm{G}_{K^1/F} \cong \mathrm{GL}_2\,\mathbb{F}_\ell$ acts transitively on $E\left[\ell\right] \setminus \{0\} \cong \mathbb{F}_\ell^2 \setminus \{(0,0)\}$. The Galois invariance of $\mathrm{res}_{K^1/F}\,\delta\left(\mathfrak{h}\right)$ translates to the Galois equivariance of ρ, so $P = \rho\left(\sigma'^{-1}\sigma\sigma'\right)$. Thus ρ is surjective. □

With such a choice, all primes $\mathfrak{p} \in S$ are Kolyvagin conductors since

$$\left(\frac{p}{K^1/\mathbb{Q}}\right) = \left(\frac{p}{K^2/\mathbb{Q}}\right)\Big|_{K^1} = \mathfrak{c}\sigma|_{K^1} = \mathfrak{c}.$$

As an almost immediate consequence, the cohomology group over F is generated by $\delta\left(\mathfrak{h}\right)$.

Lemma 4.5. $\mathrm{H}^1\left(K^2/F, E\left[\ell\right]\right) \cong \mathbb{F}_\ell \cdot \delta\left(\mathfrak{h}\right)$.

Proof. By Lemma 4.2, Lemma 4.3, and Lemma 4.4, the inflation-restriction exact sequence reads

$$\begin{array}{ccccccc} \mathrm{H}^1\left(K^1/F, E\left[\ell\right]\right) & \xrightarrow{\inf_{K^1/F}} & \mathrm{H}^1\left(K^2/F, E\left[\ell\right]\right) & \xrightarrow{\mathrm{res}_{K^1/F}} & \mathrm{H}^1\left(K^2/K^1, E\left[\ell\right]\right)^{\mathrm{G}_{K^1/F}} & \xrightarrow{\mathrm{tra}_{K^1/F}} & \mathrm{H}^2\left(K^1/F, E\left[\ell\right]\right) \\ \rotatebox{90}{$\cong$} & & & & \rotatebox{90}{$\cong$} & & \rotatebox{90}{$\cong$} \\ 0 & & & & \mathbb{F}_\ell & & 0 \end{array},$$

but $\mathrm{H}^1\left(K^2/F, E\left[\ell\right]\right)$ already contains $\delta\left(\mathfrak{h}\right)$. □

This bounds the restricted part, while the relaxed part is constrained via local ramification behaviour.

Lemma 4.6. *If $\mathfrak{p} \in S$, then*

1. $\mathrm{c}\left(p\right)^v = 0$ *for all $v \notin S$, and*
2. $\mathrm{c}\left(p\right)^{\mathfrak{p}} \neq 0$.

Proof.

1. This follows immediately from Lemma 3.4.
2. Since $\sigma \neq \mathfrak{c}$ by choice, $\mathfrak{p}$ splits completely in K^2/F by the computation

$$\left(\frac{\mathfrak{p}}{K^2/F}\right) = \left(\frac{p}{K^2/\mathbb{Q}}\right) = \mathfrak{c}\sigma,$$

so $\mathrm{f}\left(K^2_{\mathfrak{p}_{K^2}}/F_{\mathfrak{p}}\right) > 1$, and hence $\mathfrak{h} \notin \ell E\left(F_{\mathfrak{p}}\right)$. Thus $\mathrm{c}\left(p\right)^{\mathfrak{p}} \neq 0$ by Lemma 3.5.

□

In particular, $\mathrm{c}(p) \in \mathrm{Sel}^{\{\mathfrak{p}\}}(F, E[\ell])^{-\epsilon}$ by Lemma 3.3. The $-\epsilon$ eigenspace is now easy to compute.

Proposition 4.7. $\mathrm{Sel}(F, E[\ell])^{-\epsilon} = 0$.

Proof. By Lemma 3.3, $\delta(\mathfrak{h}) \in \mathrm{H}^1\left(K^2/F, E[\ell]\right)^{\epsilon}$, so $\mathrm{Sel}_S(F, E[\ell])^{-\epsilon} \subseteq \mathrm{H}^1\left(K^2/F, E[\ell]\right)^{-\epsilon} = 0$ by Lemma 4.5. By Lemma 4.6, $\mathrm{c}(p)^{\mathfrak{p}}$ are the only non-zero elements generating the one-dimensional $\mathbb{F}_\ell$-vector spaces $\mathrm{H}^1(F_{\mathfrak{p}}, E)[\ell]^{-\epsilon}$ by Lemma 4.1, so $\operatorname{coker}\sigma_{\emptyset,S} = 0$. Thus Proposition 2.3 yields

$$\begin{array}{ccccc} \operatorname{coker}\sigma_{\emptyset,S} & \longrightarrow & \mathrm{Sel}(F, E[\ell])^{-\epsilon\vee} & \longrightarrow & \mathrm{Sel}_S(F, E[\ell])^{-\epsilon\vee} \\ \rotatebox{90}{$\cong$} & & & & \rotatebox{90}{$\cong$} \\ 0 & & & & 0 \end{array}.$$

□

4.3 The non-zero eigenspace

Now let $\mathfrak{p} \in S$ be an arbitrary choice of a prime, and let K^3 be the fixed field of $\ker(\mathrm{res}_{K^2}\mathrm{c}(p) : \mathrm{G}_{K^2} \to E[\ell])$. Apply Lemma 2.4 to the fields $K' = K^3$ and $K = K^2$ to obtain a finite set of primes $S' \subseteq \mathrm{M}_F$ such that

$$\left(\frac{q}{K^3/\mathbb{Q}}\right) = \mathfrak{c}\sigma, \qquad \mathfrak{q} \in S',$$

and

$$\mathrm{Sel}_{S'}(F, E[\ell])^{\epsilon} \subseteq \inf_{K^3/F}\left(\mathrm{H}^1\left(K^3/F, E[\ell]\right)\right)^{\epsilon}.$$

This requires a choice of a non-trivial $\sigma \in \mathrm{G}^-_{K^3/K^2}$, which is guaranteed by the following.

Lemma 4.8. *There is an isomorphism of* $\mathrm{G}_{K^2/F}$*-modules* $\mathrm{G}_{K^3/K^2} \xrightarrow{\sim} E[\ell]$ *induced by* $\mathrm{c}(p)$.

Proof. By Lemma 4.5, the inflation-restriction exact sequence reads

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{H}^1\left(K^2/F, E[\ell]\right) & \xrightarrow{\inf_{K^2/F}} & \mathrm{H}^1(F, E[\ell]) & \xrightarrow{\mathrm{res}_{K^2/F}} & \mathrm{H}^1\left(K^2, E[\ell]\right) \\ & & \rotatebox{90}{$\cong$} & & & & \\ & & \mathbb{F}_\ell \cdot \delta(\mathfrak{h}) & & & & \end{array}.$$

Then $\mathrm{res}_{K^2/F}\mathrm{c}(p) \neq 0$, otherwise $\mathrm{c}(p)$ lies in the linear span of $\inf_{K^2/F}\delta(\mathfrak{h})$, which lie in different eigenspaces by Lemma 3.3. The proof then proceeds identically to Lemma 4.4, replacing K^2/K^1 with K^3/K^2 and $\delta(\mathfrak{h})$ with $\mathrm{c}(p)$, and working under the assumption $\mathfrak{h} \notin \ell E(F)$. □

With such a choice, all primes $\mathfrak{q} \in S'$ are Kolyvagin conductors since

$$\left(\frac{q}{K^2/\mathbb{Q}}\right) = \left(\frac{q}{K^3/\mathbb{Q}}\right)\Big|_{K^2} = \mathfrak{c}\sigma|_{K^2} = \mathfrak{c}.$$

As an almost immediate consequence, the cohomology group over F is generated by $\delta(\mathfrak{h})$ and $\mathrm{c}(p)$.

Lemma 4.9. $\mathrm{H}^1\left(K^3/F, E[\ell]\right) \cong \mathbb{F}_\ell \cdot \delta(\mathfrak{h}) \oplus \mathbb{F}_\ell \cdot \mathrm{c}(p)$.

Proof. By Lemma 4.5 and Lemma 4.8, the inflation-restriction exact sequence reads

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{H}^1\left(K^2/F, E[\ell]\right) & \xrightarrow{\inf} & \mathrm{H}^1\left(K^3/F, E[\ell]\right) & \xrightarrow{\mathrm{res}} & \mathrm{H}^1\left(K^3/K^2, E[\ell]\right)^{\mathrm{G}_{K^2/F}} \\ & & \rotatebox{90}{$\cong$} & & & & \rotatebox{90}{$\cong$} \\ & & \mathbb{F}_\ell \cdot \delta(\mathfrak{h}) & & & & \mathrm{Hom}\left(E[\ell], E[\ell]\right)^{\mathrm{G}_{K^2/F}} \end{array}.$$

Since $\mathrm{G}_{K^1/F} \cong \mathrm{GL}_2\mathbb{F}_\ell$ is a quotient of $\mathrm{G}_{K^2/F}$, $\mathrm{Hom}\left(E[\ell], E[\ell]\right)^{\mathrm{G}_{K^2/F}}$ is at most one-dimensional, by Lemma 4.3, but $\mathrm{H}^1\left(K^3/F, E[\ell]\right)$ already contains $\inf_{K^2/F}\delta(\mathfrak{h})$ and $\mathrm{c}(p)$, linearly independent by Lemma 3.3. □

This bounds the restricted part, while the relaxed part is constrained via local ramification behaviour.

Lemma 4.10. *If $\mathfrak{q} \in S'$, then*

1. $\mathrm{c}(pq)^{v} = 0$ *for all* $v \notin S'$, *and*
2. $\mathrm{c}(pq)^{\mathfrak{q}} \neq 0$.

Proof.

1. Lemma 3.4 reduces this to showing that $\mathrm{c}(pq)^{\mathfrak{p}} = 0$ for all $\mathfrak{p} \in S$, and Lemma 3.5 reduces this to showing that $\mathcal{H}_q \in \ell E(F_{\mathfrak{p}})$. Now $\mathfrak{q}$ splits completely in K^2/F by the computation

$$\left(\frac{\mathfrak{q}}{K^2/F}\right) = \left(\frac{q}{K^2/\mathbb{Q}}\right)^2 = \mathfrak{c}^2 = 1,$$

   so $\mathrm{f}\left(K^2_{\mathfrak{q}_{K^2}}/F_{\mathfrak{p}}\right) = 1$, and hence $\mathfrak{h} \in \ell E(F_{\mathfrak{q}})$. By Lemma 3.3, Lemma 3.4, and Lemma 3.5, $\mathrm{c}(q) \in \mathrm{Sel}(F, E[\ell])^{-\epsilon}$, which is zero by Proposition 4.7, so $0 = \mathrm{res}_{F^q/F}\,\mathrm{c}(q) = \delta^q([\mathcal{H}_q])$. Thus $\mathcal{H}_q \in \ell E(F^q) \subseteq \ell E\left(F^q_{\mathfrak{p}}\right) = \ell E(F_{\mathfrak{p}})$, as required.

2. Since $\sigma \neq \mathfrak{c}$ by choice, $\mathfrak{q}_{K^2}$ splits completely in K^3/K^2 by the computation

$$\left(\frac{\mathfrak{q}_{K^2}}{K^3/K^2}\right) = \left(\frac{q}{K^3/\mathbb{Q}}\right) = \mathfrak{c}\sigma \neq 1,$$

   so the localisation $\mathrm{c}(p)_{\mathfrak{q}} : \mathrm{G}_{K^3_{\mathfrak{q}_{K^3}}/K^2_{\mathfrak{q}_{K^2}}} \xrightarrow{\sim} E[\ell]$ of the isomorphism in Lemma 4.8 is not trivial. On the other hand, $\mathfrak{q}$ splits completely in F^p/F, so the restriction $\mathrm{G}_F \to \mathrm{G}_{F_{\mathfrak{q}}}$ factors in a diagram

$$\begin{array}{ccccc} E(F)/\ell & \longrightarrow & E(F^p)/\ell & \longrightarrow & E(F_{\mathfrak{q}})/\ell \\ \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta^p} & & \downarrow{\scriptstyle \delta_{\mathfrak{q}}} \\ \mathrm{H}^1(F, E[\ell]) & \longrightarrow & \mathrm{H}^1(F^p, E[\ell]) & \longrightarrow & \mathrm{H}^1(F_{\mathfrak{q}}, E[\ell]) \end{array}$$

   Commutativity says $\delta_{\mathfrak{q}}([\mathcal{H}_p]) = \mathrm{c}(p)_{\mathfrak{q}} \neq 0$, so $\mathcal{H}_p \notin \ell E(F_{\mathfrak{q}})$, and hence $\mathrm{c}(pq)^{\mathfrak{q}} \neq 0$ by Lemma 3.5.

□

In particular, $\mathrm{c}(pq) \in \mathrm{Sel}^{\{\mathfrak{q}\}}(F, E[\ell])^{\epsilon}$ by Lemma 3.3. The ϵ eigenspace is now easy to compute.

Proposition 4.11. $\mathrm{Sel}(F, E[\ell])^{\epsilon} \cong \mathbb{F}_{\ell} \cdot \delta(\mathfrak{h})$.

Proof. By Lemma 3.3, $\delta(\mathfrak{h}) \in \mathrm{H}^1\left(K^3/F, E[\ell]\right)^{\epsilon}$, so $\mathrm{Sel}_{S'}(K, E[\ell])^{\epsilon} \subseteq \mathrm{H}^1\left(K^3/F, E[\ell]\right)^{\epsilon} \cong \mathbb{F}_{\ell} \cdot \delta(\mathfrak{h})$ by Lemma 4.9. By Lemma 4.10, $\mathrm{c}(pq)^{\mathfrak{q}}$ are the only non-zero elements generating the one-dimensional $\mathbb{F}_{\ell}$-vector spaces $\mathrm{H}^1(F_{\mathfrak{q}}, E)[\ell]^{\epsilon}$ by Lemma 4.1, so $\operatorname{coker}\sigma_{\emptyset,S'} = 0$. Thus Proposition 2.3 yields

$$\begin{array}{ccccccc} \operatorname{coker}\sigma_{\emptyset,S'} & \longrightarrow & \mathrm{Sel}(F, E[\ell])^{\epsilon\vee} & \longrightarrow & \mathrm{Sel}_{S'}(F, E[\ell])^{\epsilon\vee} & \longrightarrow & 0 \\ \| & & & & & & \\ 0 & & & & & & \end{array},$$

which is an isomorphism since $\mathrm{Sel}(F, E[\ell])^{\epsilon}$ already contains $\delta(\mathfrak{h})$ by exactness. □

The proof of Theorem 1.2 is now complete.

Proof of Theorem 1.2. This follows immediately from Proposition 4.7 and Proposition 4.11. □

5 The Birch and Swinnerton-Dyer conjecture

The works of Gross-Zagier and Kolyvagin have huge implications on the Birch and Swinnerton-Dyer conjecture [Dar04, Theorem 3.22]. Recall that ϵ is the negative of the sign in the functional equation satisfied by the completed Hasse-Weil L-function $\Lambda_{E/F}(s)$. Depending on ϵ, an imaginary quadratic field $F = \mathbb{Q}\left(\sqrt{-D}\right)$ satisfying the Heegner hypothesis may be constructed while simultaneously satisfying a non-zero condition on the Hasse-Weil L-function $\mathrm{L}_{E_D/\mathbb{Q}}(s)$ for the quadratic twist E_D of E over $\mathbb{Q}$.

Lemma 5.1.

- *If $\epsilon = +$, there is an imaginary quadratic field $F = \mathbb{Q}\left(\sqrt{-D}\right)$ satisfying the Heegner hypothesis such that $\mathrm{L}_{E_D/\mathbb{Q}}(1) \neq 0$.*
- *If $\epsilon = -$, there is an imaginary quadratic field $F = \mathbb{Q}\left(\sqrt{-D}\right)$ satisfying the Heegner hypothesis such that $\mathrm{L}'_{E_D/\mathbb{Q}}(1) \neq 0$.*

Proof. These are delicate analytic arguments on L-functions [Wal85; BFH90; MM91]. □

With this lemma, the weak Birch and Swinnerton-Dyer conjecture holds for analytic rank at most one.

Theorem 5.2. *If $\mathrm{ord}_{s=1}\mathrm{L}_{E/\mathbb{Q}}(s) \leq 1$, then*

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

Proof. Applying higher derivatives at $s = 1$ in the functional equation $\Lambda_{E/\mathbb{Q}}(s) = -\epsilon\Lambda_{E/\mathbb{Q}}(2-s)$ yields

$$\mathrm{L}^{(k)}_{E/\mathbb{Q}}(1) = -(-1)^k \epsilon \mathrm{L}^{(k)}_{E/\mathbb{Q}}(1),$$

and similarly for any quadratic twist of E over $\mathbb{Q}$. It necessitates to consider the cases $\epsilon = \pm$ separately.

- Let $\epsilon = +$. Then $\mathrm{L}_{E/\mathbb{Q}}(1) = 0$ for parity reasons, so $\mathrm{ord}_{s=1}\mathrm{L}_{E/\mathbb{Q}}(s) = 1$ by assumption. By Lemma 5.1, $\mathrm{L}_{E_D/\mathbb{Q}}(1) \neq 0$ for some $F = \mathbb{Q}\left(\sqrt{-D}\right)$, so $\mathrm{ord}_{s=1}\mathrm{L}_{E_D/\mathbb{Q}}(s) = 0$, and hence $\mathrm{ord}_{s=1}\mathrm{L}_{E/F}(s) = 1$. The Gross-Zagier formula implies that $\mathfrak{h} \in E(F)$ has infinite order, so Theorem 1.1 implies that $\mathrm{rk}\,E(F) = 1$. By Lemma 3.2, $\mathfrak{ch} = \mathfrak{h}$ in $E(F)/E(F)_{\mathrm{tors}}$, so $\mathfrak{h} \in E(\mathbb{Q})$, and thus $\mathrm{rk}\,E(\mathbb{Q}) = 1$.
- Let $\epsilon = -$. Then $\mathrm{L}'_{E/\mathbb{Q}}(1) = 0$ for parity reasons, so $\mathrm{ord}_{s=1}\mathrm{L}_{E/\mathbb{Q}}(s) = 0$ by assumption. By Lemma 5.1, $\mathrm{L}'_{E_D/\mathbb{Q}}(1) \neq 0$ for some $F = \mathbb{Q}\left(\sqrt{-D}\right)$, and $\mathrm{L}_{E_D/\mathbb{Q}}(1) = 0$ for parity reasons, so $\mathrm{ord}_{s=1}\mathrm{L}_{E_D/\mathbb{Q}}(s) = 1$, and hence $\mathrm{ord}_{s=1}\mathrm{L}_{E/F}(s) = 1$. The Gross-Zagier formula implies that $\mathfrak{h} \in E(F)$ has infinite order, so Theorem 1.1 implies that $\mathrm{rk}\,E(F) = 1$. By Lemma 3.2, $\mathfrak{ch} = -\mathfrak{h}$ in $E(F)/E(F)_{\mathrm{tors}}$, so $\mathfrak{h} \in E(F) \setminus E(\mathbb{Q})$, and thus $\mathrm{rk}\,E(\mathbb{Q}) = 0$.

□

It is conjectural that almost all rational elliptic curves have rank at most one, and there are recent advancements to show that this holds for a positive proportion of all rational elliptic curves when ordered by a naive height, and hence validates the weak conjecture due to Gross-Zagier and Kolyvagin. The precise bounds on the order of the Tate-Shafarevich group proven by Kolyvagin also provided some validation for the strong conjecture, although the full statement for rank at most one has yet to be proven to date.

References

[BFH90] D. Bump, S. Friedberg and J. Hoffstein. *Nonvanishing theorems for L-functions of modular forms and their derivatives*. 1990.

[Cox89] D. Cox. *Primes of the form x2+ny2*. 1989.

[Dar04] H. Darmon. *Rational points on modular elliptic curves*. 2004.

[Gro91] B. Gross. *Kolyvagin's work on modular elliptic curves*. 1991.

[GZ86] B. Gross and D. Zagier. *Heegner points and derivatives of L-series*. 1986.

[Kol90] V. Kolyvagin. *Euler systems*. 1990.

[MM91] M. R. Murty and V. K. Murty. *Mean values of derivatives of modular L-series*. 1991.

[Rub00] K. Rubin. *Euler systems*. 2000.

[Sil09] J. Silverman. *The arithmetic of elliptic curves*. 2009.

[Sil94] J. Silverman. *Advanced topics in the arithmetic of elliptic curves*. 1994.

[Wal85] Waldspurger. *Sur les valeurs de certaines fonctions L automorphes en leur centre de symetrie*. 1985.

[Wes01] T. Weston. *The Euler system of Heegner points*. 2001.