Proof of Kolyvagin's Theorem

Elie Studnia

October 1, 2023

These are somewhat expanded notes for my talk in the Euler System online seminar organized by Arshay Sheth. I take this opportunity to thank him again, as well as the other speakers. The references from the seminar bibliography are good, but I offer additional references for some of the needed intermediate results, which can be rather technical.

1 Setup

Let E be a modular elliptic curve over $\mathbb{Q}$ with conductor N, which does not have CM. It has a modular parametrization $\varphi : X_0(N) \to E$, chosen so that it maps $\infty_{X_0(N)}$ to 0_E.
Let $K/\mathbb{Q}$ be an imaginary quadratic number field satisfying the *Heegner assumption*: every prime $q \mid N$ splits in K. Let us fix once and for all a complex conjugation τ acting on $\overline{\mathbb{Q}}$.
We let, for every integer $n \geq 1$, H_n be the ring class field of $\mathbb{Z} + n\mathcal{O}_K$.
This lets us define, for every $n \geq 1$ coprime to N, Heegner points $x_n \in X_0(N)(H_n)$, and $y_n = \varphi(x_n) \in E(H_n)$. "The" Heegner point is $y_K = N_{H_1/K} y_1 \in E(K)$.

The theorem that we want to prove is:

Theorem 1.1 *Let p be a prime satisfying the following conditions:*

- $p > 2$,
- $y_K \notin pE(K)$,
- *for every $q \mid N$, p does not divide the number of connected components of the base change to $\overline{\mathbb{F}_q}$ of the Néron model of E,*
- $\overline{\rho_E} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ *is onto.*

Then $\mathrm{Sel}_p(E/K) \cong \mathbb{F}_p \delta(y_K)$.

Remarks:

1. As long as y_K is not a torsion point, the conditions are verified for all but finitely many p, by the Mordell-Weil theorem [10, Theorem VIII.6.7] and more importantly Serre's open image theorem [9].
2. Even for those primes p where not all the conditions hold, we can show in many cases, typically by working modulo p^n for larger n, that $\mathrm{Sel}_{p^\infty}(E/K)$ has corank one and bound its torsion part, see among others [5] or recent works of Castella such as [2, 1].
3. The third condition (which is not mentioned in Castella's lecture notes, and is only useful for Proposition 3.2) might in fact not be needed, but it seems that removing it requires some nontrivial information on the reduction at bad places of Heegner points. Such facts are discussed in [4, §III.3], but I am currently unable to determine whether this is enough to carry out the argument.
4. The first and last conditions imply that for any abelian extension L/K, $E(L)$ contains no p-torsion. Indeed, up to enlarging it, we can assume that L is Galois over $\mathbb{Q}$. Thus we have a surjection $\mathrm{Gal}(L/\mathbb{Q}) \to GL_2(\mathbb{F}_p)$ (coming from $\overline{\rho_E}$).

A collection of certain primes will be useful in the proof: the collection $\mathscr{L}$ of *Kolyvagin primes*, that is, primes $\ell \nmid 6pN\Delta_K$ that are inert in K, and such that p divides both $a_\ell(E)$ and

$\ell+1$. In other words, $\mathscr{L}$ is the set of primes $\ell \nmid 6pN\Delta$ such that $\mathrm{Frob}_\ell \in \mathrm{Gal}(K(E[p])/\mathbb{Q})$ is the class of the complex conjugation τ.

The set of (possibly empty) square-free products of Kolyvagin primes will be denoted by $\mathscr{N}$.

2 Further remarks on Galois cohomology

Given a local or global field $*$ of characteristic zero, we have a Kummer short exact sequence

$$0 \to E(*)/pE(*) \xrightarrow{\delta} H^1(*, E[p]) \to H^1(*, E(\overline{*}))[p] \to 0,$$

coming from the exact sequence of group schemes $0 \to E[p] \to E \xrightarrow{p} E \to 0$.

Definition: Let v be a finite place of K and take $* = K_v$. We denote by $H^1_f(K_v, E[p])$ the image of δ and we call its elements the *geometric* classes.

Recall that $\mathrm{Sel}_p(E/K)$ is the subspace of $H^1(K, E[p])$ consisting of those classes whose localization at every place v of K is geometric ("classes that are geometric at every place").

We have a perfect symmetric pairing coming from local Tate duality:

$$(-,-)_v : H^1(K_v, E[p]) \times H^1(K_v, E[p]) \xrightarrow{\cup} H^2(K_v, E[p] \otimes E[p]) \xrightarrow{\text{Weil}} H^2(K_v, \mu_p) \overset{\text{inv}}{\cong} \mathbb{F}_p.$$

Recall that *global* duality implies that for every $c, c' \in H^1(K, E[p])$, the following formula is well defined and true:

$$\sum_v \left(\mathrm{loc}_v(c), \mathrm{loc}_v(c')\right)_v = 0.$$

Proposition 2.1 *If v does not divise Np, then $H^1_f(K_v, E[p])$ is exactly the kernel of the restriction $H^1(K_v, E[p]) \to H^1(K_v^{nr}, E[p])$, where K_v^{nr} is the maximal unramified extension of K_v (the set of "unramified classes").*

Proof. – Note that E/K_v has good reduction. Let $c \in H^1_f(K_v, E[p])$. So c is represented by the cocycle $z : \sigma \longmapsto \sigma(P) - P$, for some point $P \in E(\overline{K_v})$ such that $pP \in E(K_v)$. When σ lies in the inertia group of K_v, $\sigma(P)$ and P have the same image in $E(k)$, where k is the residue field of $\overline{K_v}$. In particular, $z(\sigma)$ is a p-torsion point with trivial reduction in $E(k)$, so is zero by [10, Proposition VII.3.1]. Thus z vanishes when restricted to the inertia group.

We showed that the geometric classes were unramified. Now note that the set of unramified classes has the same cardinality as $|E[p](K_v)|$ (see [11, Lemma 1]). On the other hand, the set of geometric classes has cardinality $|E(K_v)/pE(K_v)| = |E(K_v)[p]|$ by [7, Lemma I.3.3]. $\square$

Proposition 2.2 *$H^1_f(K_v, E[p])$ is a maximal isotropic subspace under $(-,-)_v$.*

Proof. – By [7, Corollary I.3.4] and the following discussion, there is a pairing

$$H^0(K_v, E) \times H^1(K_v, E) \to \mathbb{Q}/\mathbb{Z}$$

compatible with $(-,-)_v$ (since elliptic curves are self-dual). It is then straightforward from the definitions that $H^1_f(K_v, E[p])$ is orthogonal to itself. All we need to show is thus that $|H^1_f(K_v, E[p])|^2 = |H^1(K_v, E[p])|$. By local Tate duality (eg [8, Proposition 7.2.10]), the local Euler-Poincaré characteristic formula ([8, Theorem 7.3.1]) and [7, Lemma I.3.3],

$$\begin{aligned} |H^1_f(K_v, E[p])|^2 &= |E(K_v)/pE(K_v)|^2 = |E[p](K_v)|^2 |\mathcal{O}_{K_v}/p\mathcal{O}_{K_v}|^2 \\ &= |H^0(K_v, E[p])||H^2(K_v, E[p])||\mathcal{O}_{K_v}/(p^2)| = |H^1(K_v, E[p])|. \end{aligned}$$

$\square$

Now, suppose, until the end of the section, that v is the place associated to a Kolyvagin prime ℓ – we will abusively write $v = \ell$. Then we naturally have $\mathrm{Gal}(K_\ell/\mathbb{Q}_\ell) \cong \{1, \tau\}$. In particular, τ

acts as an involution on $H^1(K_\ell, E[p])$, $H^1_f(K_\ell, E[p])$, and $H^1_s(K_\ell, E[p]) = H^1(K_\ell, E[p])/H^1_f(K_\ell, E[p])$. We will denote its eigenspaces (with eigenvalues ± 1) with the superscripts $\pm$.

Proposition 2.3 *$H^1(K_v, E[p])^+$ and $H^1(K_v, E[p])^-$ are orthogonal.*

Proof. – τ acts equivariantly on $(-,-)_\ell$, and trivially on $H^2(K_\ell, \mu_p)$. So if $x_\pm \in H^1(K_v, E[p])^\pm$, then $(x_+, x_-)_\ell \in H^2(K_v, E[p])^- = \{0\}$. □

Proposition 2.4 $\dim H^1(K_\ell, E[p]) = 4$. *For any sign ϵ, $H^1_f(K_\ell, E[p])^\epsilon$, $H^1_s(K_\ell, E[p])^\epsilon$ are lines, and $(-,-)_\ell$ is a perfect duality between them.*

Proof. – For the first part, we use the local Euler-Poincaré characteristic formula and local Tate duality as above:

$$\dim H^1(K_\ell, E[p]) = \dim H^0(K_\ell, E[p]) + \dim H^2(K_\ell, E[p]) = 2 \dim H^0(K_\ell, E[p]) = 2 \cdot 2 = 4,$$

since $E[p]$ is unramified at ℓ and the Frobenius at ℓ acts by an involution.

For the second part, we first note that by Proposition 2.2, $\dim H^1_f(K_\ell, E[p]) = \dim H^1_s(K_\ell, E[p] = 2$. Moroever, by the inflation-restriction exact sequence [11, Proposition 2] (since $K_\ell/\mathbb{Q}_\ell$ has degree two, coprime to p), and [11, Lemma 1]

$$\dim H^1_f(K_\ell, E[p])^+ = \dim H^1(K_\ell^{nr}/K_\ell, E[p])^{\mathrm{Gal}(K_\ell/\mathbb{Q}_\ell)} = \dim H^1(\mathbb{Q}_\ell^{nr}/\mathbb{Q}_\ell, E[p]) = \dim E[p](\mathbb{Q}_\ell) = 1.$$

Hence $\dim H^1_f(K_\ell, E[p])^- = 1$. Now, for any sign ϵ, $H^1_f(K_\ell, E[p]) + H^1(K_\ell, E[p])^{-\epsilon}$ is orthogonal to $H^1_f(K_\ell, E[p])^+$, so $H^1_s(K_\ell, E[p])^\epsilon$ has dimension $d_\epsilon > 0$. Since $d_+ + d_- = 2$, it follows $d_+ = d_- = 1$. The final statement follows from this argument and the fact that $(-,-)_\ell$ is perfect (as a bilinear pairing on $H^1(K_\ell, E[p])$). □

3 Local properties of Kolyvagin's derived classes

Let H_∞ be the field generated by all the H_n; it is an abelian extension of K and is Galois over $\mathbb{Q}$.

For every Kolyvagin prime ℓ, we choose an element $\sigma_\ell \in \mathrm{Gal}(H_\infty/H_1)$ satisfying the following properties: it restricts to a generator of $\mathrm{Gal}(H_\ell/H_1)$ (which is cyclic of order $\ell+1$), and, for any integer n prime to ℓ, σ_ℓ is the identity on H_n. Such a choice is possible because, for any coprime integers $n, m \geq 1$, $H_n \cap H_m = H_1$.

We then denote $D_\ell = \sum_{i=1}^{\ell} i\sigma_\ell^i$. For every $n \in \mathscr{N}$, we denote $D_n = \prod_{\ell | n} D_\ell$.

Let finally $T \subset \mathrm{Gal}(H_\infty/K)$ be a set of representatives for the quotient $\mathrm{Gal}(H_1/K)$. We then denote, for every n coprime to N, $P_n = \sum_{s \in T} sD_n y_n \in E(H_n)$. Note that the definition of P_n depends on the choice of T, but $P_n \pmod{pE(H_n)}$ does not.

Definition: As we saw in a previous talk, the derived class $c_n \in H^1(K, E[p])$ is the unique $c \in H^1(K, E[p])$ whose restriction to H_n is $\delta(P_n)$.

It is known that the completed L-function $\Lambda(E, s)$ satisfies a functional equation

$$\Lambda(E, s) = -\epsilon\Lambda(E, 2-s)$$

for some sign ϵ. This follows from the existence of a special involution on $X_0(N)$, the *Fricke involution w_N*. Formally, it maps a pair (E, C) (where E is an elliptic curve and C a cyclic subgroup of order N) to $(E/C, E[N]/C)$. An explicit computation yields that $\varphi(w_N(x)) = \epsilon(\varphi(x) - \varphi(0))$ for every $x \in X_0(N)$, where $\varphi(0) \in E(\mathbb{Q})_{tors}$ by Manin-Drinfeld's theorem [6, 3].

Proposition 3.1 *For every $n \in \mathscr{N}$, $c_n^\tau = \epsilon\mu(n)c_n$, where μ is the Möbius function.*

Sketch of proof. – We saw in a previous talk that the restriction $H^1(K, E[p]) \to H^1(H_n, E[p])$ was injective, so it is enough to show that their restrictions as classes in $H^1(H_n, E[p])$ agree, that is, that $\tau(P_n)$ and $\epsilon\mu(n)P_n$ are congruent modulo $pE(H_n)$.

Because $\overline{\rho_E}$ is onto, the order of $\varphi(0)$ is prime to p, so $\varphi(0) \in pE(\mathbb{Q})$.
Let now $n \in \mathscr{N}$. Applying the definitions of w_N and τ, we see that $w_N(x_n) = \tau(x_n)$. It follows from the above that $\tau(y_n) = \epsilon y_n - \epsilon\varphi(0)$. By construction, τ acts on $\mathrm{Gal}(H_\infty/K)$ by inversion, so that $D_\ell^\tau + D_\ell = (\ell+1)\sum_{i=1}^{\ell} \sigma_\ell^i$. Therefore, $\tau(P_n) \equiv \sum_{s\in T} s^{-1} \prod_{\ell | n}(-D_\ell)(\epsilon y_n - \epsilon\varphi(0)) \equiv \epsilon\mu(n)P_n$ (mod $pE(H_n)$). $\square$

Proposition 3.2 *Let v be a finite place of K not dividing some $n \in \mathscr{N}$. Then c_n is geometric at v.*

Proof. – Let w be any place of H_n above v. Let $c = \mathrm{loc}_v(c_n) \in H^1(K_v, E[p])$, and c' be its image in $H^1(K_v, E(\overline{K_v}))$. We know that c' restricts trivially to $(H_n)_w$, because the restriction of c_n to H_n is $\delta(P_n)$ (where $P_n \in E(H_n)$). So c' comes from $H^1((H_n)_w/K_v, E((H_n)_w))$, has order dividing p, and we want to show that it is zero. But this cohomology group injects into $H^1(K_v^{nr}/K_v, E(K_v^{nr}))[p]$, which is isomorphic[1] by [7, Proposition I.3.8] to $H^1(K_v^{nr}/K_v, \pi_0(\mathscr{E}_{\overline{\mathbb{F}_v}}))[p]$. By our assumption on p, this cohomology group is trivial, which concludes.

$\square$

Proposition 3.3 *Let $m \in \mathscr{N}$ and $\ell \in \mathscr{L}$ be coprime, let $n = \ell m$. Then c_n is geometric at ℓ iff* $\mathrm{loc}_\ell(c_m) = 0$.

Sketch of proof. – For any $\sigma \in G_K$, we know that there is a unique point $\frac{(\sigma-1)(P_n)}{p} \in E(H_n)$ whose p-th power is $\sigma(P_n) - P_n$ (its existence follows from the existence of the Kolyvagin class c_n, its uniqueness from the fact that $E[p](H_n) = 0$, which we saw in a previous talk). Choose now some finite extension L of H_n and some $R_n \in E(L)$ such that $pR_n = P_n$. We can then check that the cocycle $z_n : \sigma \in G_K \longmapsto \sigma(R_n) - R_n - \frac{(\sigma-1)(P_n)}{p} \in E[p]$ represents c_n (it is a cocycle, and has the correct restriction to H_n).

As above, c_n is geometric at ℓ iff the image of z_n in $H^1(K, E(\overline{K}))[p]$ (which actually lies in $H^1(H_n/K, E(H_n))[p]$) vanishes when restricted to $\mathrm{Gal}((H_n)_\lambda/K_\ell)$, where Λ is a prime of H_n above ℓ; it can be easily shown that $(H_n)_\Lambda/K_\ell$ is totally ramified, cyclic of order $\ell+1$, with Galois group generated by σ_ℓ.

This implies, by [10, Propositions IV.3.2, IV.6.4, Chapter VII.2], that the reduction mod Λ map $H^1((H_n)_\Lambda/K_\ell) \to H^1(\langle\sigma_\ell\rangle, E(\mathbb{F}_{\ell^2}))$ is an isomorphism (since the kernel of the reduction is a pro-ℓ-group).

Clearly, the image of z_n in $H^1(K, E(\overline{K}))[p]$ is given by the cocycle $z_n' : \sigma \longmapsto -\frac{(\sigma-1)(P_n)}{p}$, so that c_n is geometric at ℓ iff the reduction mod Λ of $\frac{(\sigma_\ell-1)(P_n)}{p}$ is zero.

Now, we can compute thanks to the norm relation that

$$\frac{(\sigma_\ell - 1)(P_n)}{p} = \sum_{s\in T} sD_m\left(\frac{\ell+1}{p}y_n - \frac{a_\ell}{p}y_m\right) = -\frac{a_\ell}{p}P_m + \frac{\ell+1}{p}\sum_{s\in T} sD_m y_n.$$

On the other hand, because H_m/K is totally split above ℓ, $\mathrm{loc}_\ell(c_m) = 0$ iff for some (thus for all) prime $\lambda \subset \mathcal{O}_{H_m}$ above ℓ, $P_m \in pE((H_m)_\lambda)$; by Hensel's lemma, this is equivalent to the reduction mod λ of P_m being in $pE(\mathbb{F}_\ell^2)$; we saw that this condition was independent from the choice of λ'.

Then it's apparently a simple computation using the congruence relation[2]. $\square$

[1] Briefly, it is a combination of Hensel's lemma and "Lang's lemma" for connected algebraic groups over finite fields (roughly, $\mathrm{Frob}\cdot\mathrm{id}^{-1}$ is surjective)

[2] it features in Castella's lecture notes that I encourage you to read. I personally do not understand it, because it seemingly claims that the sD_m meaningfully exist as operators on the geometric fibre of $E(\mathbb{F}_{\ell^2})$ (insofar as they map a global point with trivial reduction modulo a fixed prime above ℓ to another such point) – which I do not think can be true. I will hopefully edit these notes when I find an explanation.

4 Proof of the theorem

Define $L = K(E[p])$.

Recall that we chose a complex conjugation τ. It is clear that τ acts on $E[p]$ and on $H^1(K, E[p])$; it preserves $\mathrm{Sel}_p(E/K)$.

Lemma 4.1 *The restriction map $H^1(K, E[p]) \to \mathrm{Hom}_{G_K}(G_L, E[p])$ is an isomorphism.*

Proof. – Its kernel (resp. cokernel) is (resp. is contained in) $H^1(\mathrm{Gal}(L/K), E[p](L)) \cong H^1(\overline{\rho_E}(G_K), E[p])$ (resp the H^2). Since $\overline{\rho_E}(G_K)$ is a subgroup of index at most 2 of $\mathrm{Aut}(E[p])$, so it contains the central element $-\mathrm{id}$ with order 2. Thus, $-\mathrm{id}$ must act on $H^*(\overline{\rho_E}, -)$ by the identity; yet it acts on $E[p]$ by -1, so that $H^*(\overline{\rho_E}(G_K), E[p])$ vanishes. □

Proposition 4.2 *(see [5, Lemma 1.6.2][3]) Let $c_\pm \in H^1(K, E[p])^\pm$ be two nonzero classes, one lying in the $+$ eigenspace for τ and one lying in the $-$ eigenspace. There are infinitely many $\ell \in \mathscr{L}$ such that both localizations at ℓ of c_+ and c_- do not vanish.*

Proof. – Choose cocycles representing $c_\pm$ (denoted in the same way). Consider the restriction map $J : H^1(G_K, E[p]) \to \mathrm{Hom}_{G_K}(G_L, E[p])$ where $L = K(E[p])$, which is an isomorphism. We denote $f_\pm = J(c_\pm)$.

Define the finite extension M/K by $G_M = \ker c_+ \cap \ker c_- \cap G_L$. It is a Galois extension of K: indeed, the right-hand side is clearly a closed subgroup of finite index, and if $\tau \in G_M$ and $\sigma \in G_K$, then $c_\pm(\sigma\tau\sigma^{-1}) = (1 - \sigma\tau\sigma^{-1}) \cdot c_\pm(\sigma) + \sigma \cdot c_\pm(\tau) = (1 - \mathrm{id})c_\pm(\sigma) + \sigma \cdot 0 = 0$. Moreover, M is clearly stable under τ, so that $M/\mathbb{Q}$ is Galois. The same computation also shows that $f_\pm : \mathrm{Gal}(M/L) \to E[p]^{\oplus 2}$ is an injective group homomorphism, so that $H = \mathrm{Gal}(M/L)$ is a $\mathbb{F}_p$-vector space with action of τ, so there are eigenspaces H^+ and H^-.

Note that the image of $f_\pm$ is nonzero and stable under G_K. Since $\overline{\rho_E}(G_K) \supset \mathrm{Aut}(E[p])' = SL(E[p])$, the image of $f_\pm$ it is all of $E[p]$. Let now $g_\pm$ be the projection of $f_\pm$ to $E[p]^\pm$. They are *not* G_K-homomorphisms any more; however, they are still surjective group homomorphisms $\mathrm{Gal}(M/L) \to E[p]^\pm$.

A formal computation shows that, for any $z \in H^-$, $f_+(z) \in E[p]^-$, so that $g_+(H^-) = 0$. Similarly, $g^-(H^-) = 0$, so that $\ker g_\pm \cap H^+$ are two proper subspaces of H^+. In particular, there is some $\eta \in H^+$ outside $\ker g_+ \cup \ker g_-$. Let now $\sigma = \tau \cdot z \in \mathrm{Gal}(M/\mathbb{Q})$, so that $\sigma^2 = z^2$.

Now let $\ell \nmid 6p$ be a rational prime such that E has good reduction at ℓ, $c_\pm, L$ are unramified at ℓ (these conditions are true for all but finitely many ℓ), and such that the image of $\mathrm{Frob}_{\ell\mathbb{Z}}$ in $\mathrm{Gal}(M/\mathbb{Q})$ is σ. By Cebotarev, there are infinitely many such primes. In particular, $\mathrm{Frob}_{\ell\mathbb{Z}}$ acts as τ on $E[p]$ so $\ell \in \mathscr{L}$.

Moreover, $c_\pm(\mathrm{Frob}_{\ell O_K}) = c_\pm(\mathrm{Frob}_{\ell\mathbb{Z}}^2) = c_\pm(z^2) = 2f_\pm(z) \neq 0$. □

Proof of the main theorem. – By the assumptions, $c_1 \in (\mathrm{Sel}_p(E/K))^\epsilon$ is a nonzero class.

First, let $c \in (\mathrm{Sel}_p(E/K))^{-\epsilon}$ be nonzero. By Proposition 4.2, there is a Kolyvagin prime ℓ at which c_1 and c do not vanish. Therefore, by Proposition 3.3, c_ℓ is not geometric at ℓ. By Proposition 3.1, $c_\ell \in (\mathrm{Sel}_p(E/K))^\epsilon$.

By global duality, we know that

$$(\mathrm{loc}_\ell(c), \mathrm{loc}_\ell(c_\ell))_\ell = -\sum_{v \neq \ell} (\mathrm{loc}_v(c), \mathrm{loc}_v(c_\ell))_v.$$

At any place $v \neq \ell$, both c and c_ℓ are geometric (by Proposition 3.2), so by Proposition 2.2 the right-hand side is a sum of zeros. Therefore $(\mathrm{loc}_\ell(c), \mathrm{loc}_\ell(c_\ell))_\ell = 0$. But the two local classes are nonzero in $H^1_f(K_\ell, E[p])^{-\epsilon}$ and $H^1_s(K_\ell, E[p])^{-\epsilon}$, which contradicts Proposition 2.4.

Hence $\mathrm{Sel}_p(E/K)^{-\epsilon} = 0$.

[3] I learnt of this lemma through G. Grossi's MSRI talk in January 2023. The proof of the main theorem also follows the argument she then described.

Suppose that $\mathrm{Sel}_p(E/K) \neq \mathbb{F}_p \cdot c_1$: then $(\mathrm{Sel}_p(E/K))^\epsilon$ has dimension at least two, so there is a nonzero element d in the kernel of the localization $(\mathrm{Sel}_p(E/K))^\epsilon \to H^1_f(K_\ell, E[p])^\epsilon$. Now d and c_ℓ are nonzero cohomology classes with opposite signs, so by Proposition 4.2 there is a Kolyvagin prime m at which both localizations do not vanish. As above, this means that $c_{m\ell}$ is not geometric at m, and that $c_{m\ell}, d \in H^1(K, E[p])^\epsilon$.

By global duality, we know that

$$(\mathrm{loc}_\ell(d), \mathrm{loc}_\ell(c_{m\ell}))_\ell + (\mathrm{loc}_m(d), \mathrm{loc}_m(c_{m\ell}))_m = -\sum_{v \neq m,\ell} (\mathrm{loc}_v(d), \mathrm{loc}_v(c_{m\ell}))_v.$$

As above, the right-hand side is zero, since both d and $c_{m\ell}$ are geometric at all places $v \neq m, \ell$. Moreover, since $\mathrm{loc}_\ell(d) = 0$, we find that $(\mathrm{loc}_m(d), \mathrm{loc}_m(c_{m\ell}))_m = 0$. But both elements are nonzero in the lines $H^1_f(K_m, E[p])^\epsilon$ and $H^1_s(K_m, E[p])^\epsilon$, so this contradicts again the Proposition 2.4.

Thus $\mathrm{Sel}_p(E/K) = \mathbb{F}_p \cdot c_1$. $\square$

References

[1] F. Castella, G. Grossi, J. Lee, and C. Skinner, *On the anticyclotomic Iwasawa theory of rational elliptic curves at eisenstein primes*, Invent. math. **227** (2022), no. 2, 517–580.

[2] F. Castella, G. Grossi, and C. Skinner, *Mazur's main conjecture at Eisenstein primes*, 2023.

[3] V. G. Drinfel'd, *Two theorems on modular curves*, Functional Analysis and Its Applications **7** (1973), no. 2, 155–156.

[4] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[5] B. Howard, *The Heegner point kolyvagin system*, Compos. Math. **140** (2004), no. 6, 1439–1472.

[6] Y. I. Manin, *Parabolic pointsand zeta-functions of modular curves*, Mathematics of the USSR-Izvestiya **6** (1972), no. 1, 19–64.

[7] J. S. Milne, *Arithmetic duality theorems*, 2nd edition ed., BookSurge, 2006.

[8] J. Neukirch, A Schmidt, and K. Wingberg, *Cohomology of number fields*, second edition ed., Grundlehren Math. Wiss., no. 323, Springer Berlin Heidelberg, 2008.

[9] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1971), no. 4, 259–331.

[10] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed. 2009. ed., Grad. Texts in Math., 106, Springer New York, 2009.

[11] L. C. Washington, *Galois Cohomology*, Modular Forms and Fermat's Last Theorem (G. Cornell, J. H. Silverman, and G. Stevens, eds.), Springer New York, 1997, pp. 101–120.