

COMPOSITIO MATHEMATICA

MASSIMO BERTOLINI

**Selmer groups and Heegner points in
anticyclotomic \mathbb{Z}_p -extensions**

Compositio Mathematica, tome 99, n° 2 (1995), p. 153-182

http://www.numdam.org/item?id=CM_1995__99_2_153_0

© Foundation Compositio Mathematica, 1995, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://http://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

Selmer groups and Heegner points in anticyclotomic \mathbb{Z}_p -extensions *

MASSIMO BERTOLINI

Dipartimento di Matematica, Università di Pavia, Via Abbiategrasso 209, 27100 Pavia, Italy

Received 21 October 1993; accepted in final form 30 October, 1994

Abstract. Let E/\mathbb{Q} be a modular elliptic curve, and let p be a prime of good ordinary reduction for E . Write K_∞ for the anticyclotomic \mathbb{Z}_p -extension of an imaginary quadratic field K which satisfies the Heegner hypothesis. Assuming that some Heegner point on E defined over K_∞ has infinite order, we show that the p^∞ -Selmer group $\text{Sel}_{p^\infty}(E/K_\infty)$ of E over K_∞ has corank equal to 1 over the Iwasawa algebra Λ relative to K_∞/K . Moreover, we construct a pseudo-annihilator in Λ of the Λ -cotorsion quotient of $\text{Sel}_{p^\infty}(E/K_\infty)$, which encodes the way the Heegner points “sit inside” the Selmer group.

Introduction

Let E be an elliptic curve over \mathbb{Q} of conductor N . Assume that E is modular, i.e., there exists a non-constant morphism defined over \mathbb{Q}

$$\phi : X_0(N) \rightarrow E,$$

where $X_0(N)$ is the modular curve which classifies pairs of elliptic curves related by a cyclic N -isogeny.

Given an imaginary quadratic field K and an integer $n \geq 1$, let $K[n]$ stand for the ring class field of conductor n . If \mathcal{O}_n denotes the order of K of conductor n and the modular function j is viewed as a function of lattices, then $K[n] = K(j(\mathcal{O}_n))$. By class field theory, the extension $K[n]$ is Abelian over K and dihedral over \mathbb{Q} . The primes of K ramified in $K[n]$ are those dividing n .

Assume that every rational prime which divides N is split in K . Factor N as $p_1^{e_1} \cdots p_k^{e_k}$, and fix a choice of a prime ideal of K , say \mathcal{P}_i , above each p_i . Define the ideal $\mathcal{N} = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_k^{e_k}$. If $n \geq 1$ is prime to N , the natural projection of complex tori

$$\mathbb{C}/\mathcal{O}_n \rightarrow \mathbb{C}/(\mathcal{O}_n \cap \mathcal{N})^{-1}$$

is a cyclic N -isogeny, which corresponds to a point of $X_0(N)$ defined over $K[n]$. Let $\alpha[n] \in E(K[n])$ be its image under the modular parametrization ϕ . We call $\alpha[n]$ the *Heegner point of conductor n* .

In the spirit of Iwasawa theory, we focus on \mathbb{Z}_p -extensions of K constructed from ring class fields, p being an odd rational prime. Since the ramification is concentrated above p , we need only consider ring class fields of p -power conductor. Let \tilde{K}_∞ be $\bigcup_{n \geq 1} K[p^n]$. The Galois group $\text{Gal}(\tilde{K}_\infty/K)$ is isomorphic to $\mathbb{Z}_p \times \Delta$, where Δ is a finite Abelian

* Partially supported by M.U.R.S.T. of Italy and Consiglio Nazionale delle Ricerche.

group. Thus, \tilde{K}_∞ contains a unique \mathbb{Z}_p -extension K_∞ of K , called the *anticyclotomic \mathbb{Z}_p -extension*. Among all \mathbb{Z}_p -extensions of K , K_∞ is characterized as the one which is dihedral over \mathbb{Q} .

Write K_n for the subextension of K_∞ of degree p^n over K , and $K[p^{k(n)}]$ for the ring class field of minimal conductor containing K_n . (Under the assumptions of the subsequent sections, we will have $k(n) = n + 1$.) Let $\alpha_n \in E(K_n)$ denote the trace from $K[p^{k(n)}]$ to K_n of the Heegner point $\alpha[p^{k(n)}]$.

The theme of this paper is the study of the structure of the p -Selmer group of E over K_∞ , under the assumption that p is a prime of good ordinary reduction for E and some Heegner point α_n has infinite order. Roughly stated, our results show that the structure of the above Selmer group is accounted for by the family of all Heegner points defined over K_∞ . The method of proof blends ideas of Kolyvagin with techniques of Iwasawa theory.

More precisely, we define the *p -Selmer group of E over K_∞* to be the p -torsion module

$$\text{Sel}_{p^\infty}(E/K_\infty) := \varinjlim_n \text{Sel}_{p^\infty}(E/K_n),$$

where $\text{Sel}_{p^\infty}(E/K_n)$ denotes the p -Selmer group of E over K_n , and the direct limit is taken with respect to the natural restriction maps. Write Γ for the Galois group $\text{Gal}(K_\infty/K)$, and Λ for the Iwasawa algebra $\mathbb{Z}_p[[\Gamma]]$. Then, the Pontryagin dual

$$\mathcal{X}_\infty := \text{Hom}_{\mathbb{Z}_p}(\text{Sel}_{p^\infty}(E/K_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$$

of $\text{Sel}_{p^\infty}(E/K_\infty)$ is a finitely generated Λ -module.

We state our main results, which are obtained under the additional hypotheses listed in Subsection 2.2.

THEOREM A. *Assume that the Heegner point α_n has infinite order for some $n \geq 1$. Then \mathcal{X}_∞ is a Λ -module of rank one.*

(Theorem A corresponds in the text to Theorem 3.1.1) Assuming that some α_n has infinite order, we define in Subsection 3.2 a non-zero element ρ_∞ of Λ , which encodes the way the family of all Heegner points over K_∞ “sits inside” the Selmer group.

THEOREM B. *Assume that α_n has infinite order for some $n \geq 1$. Then $\rho_\infty^2 \cdot (\mathcal{X}_\infty)_{\text{tors}}$ is finite, $(\mathcal{X}_\infty)_{\text{tors}}$ being the Λ -torsion submodule of \mathcal{X}_∞ .*

(In fact, we prove a more precise and stronger statement: cf. Theorem 3.2.1)

In our setting, Theorems A and B may be viewed as an analogue of the results of Kolyvagin ([10]) for the Selmer group of E over K . Kolyvagin’s results hold under the assumption that the Heegner point over K has infinite order, i.e., by a theorem of Gross–Zagier, the analytic rank of E over K is one. In our case, the analogue assumption is the non-triviality of some Heegner point over the anticyclotomic \mathbb{Z}_p -extension. Mazur conjectures that this is always verified. See the Remark 4 of Subsection 3.1 for more comments.

Our results provide evidence for a conjecture of Perrin-Riou, which is the analogue in the present situation of the Main Conjecture of Iwasawa theory for cyclotomic fields (cf. Remark 11 of Subsection 3.2).

1. Preliminary results

1.1. NOTATIONS AND CONVENTIONS

We keep throughout the paper the notations and definitions of the introduction. In particular, p will denote an odd rational prime.

We fix an algebraic closure $\overline{\mathbb{Q}}$ of \mathbb{Q} and, by choosing an embedding of $\overline{\mathbb{Q}}$ in \mathbb{C} , a complex conjugation τ on $\overline{\mathbb{Q}}$.

Given a $\mathbb{Z}[\frac{1}{2}][\tau]$ -module M , we have a decomposition $M = M^+ \oplus M^-$, where M^+ , respectively M^- denotes the submodule on which τ acts as $+1$, respectively -1 . Given an Abelian group A and an integer $m \geq 1$, we adopt the convention of writing A/p^m as a shorthand for $A/p^m A$.

Let l be a rational prime, m a positive integer, and F a number field. Define

$$E(F_l)/p^m := \bigoplus_{\lambda|l} E(F_\lambda)/p^m,$$

$$H^1(F_l, E)_{p^m} := \bigoplus_{\lambda|l} H^1(F_\lambda, E)_{p^m},$$

$$H^1(F_l, E_{p^m}) := \bigoplus_{\lambda|l} H^1(F_\lambda, E_{p^m}),$$

where the sum is taken over the primes of F dividing l .

In the rest of Section 1 we work with a fixed finite layer K_n of K_∞ , which we denote for short by H . We also write G , respectively D for the Galois group $\text{Gal}(H/K)$, respectively, $\text{Gal}(H/\mathbb{Q})$. Given an integer $m \geq 1$, we let R stand for the group ring $\mathbb{Z}/p^m\mathbb{Z}[G]$.

The numbering of the results within the same subsection is progressive. In referring to a result from a different subsection of the same section, we shall write the number of the subsection in front of the number of the result. Similarly, a result from a different section will be indicated by the number of the section followed by the number of the subsection followed by the number of the result.

1.2. DUALITY

(References: [15], Section 1; [23], [24].)

Let m, l and H be as in Subsection 1.1.

The cup product composed with the Weil pairing gives rise to a non-degenerate pairing

$$H^1(H_l, E_{p^m}) \times H^1(H_l, E_{p^m}) \rightarrow \mathbb{Z}/p^m\mathbb{Z}$$

([15], Corollary 2.3, p. 34). (In view of our conventions, the above pairing is a sum of local pairings corresponding to the primes of H dividing l .) Identify $E(H_l)/p^m$ with a submodule of $H^1(H_l, E_{p^m})$ via the local descent exact sequence

$$0 \rightarrow E(H_l)/p^m \rightarrow H^1(H_l, E_{p^m}) \rightarrow H^1(H_l, E)_{p^m} \rightarrow 0.$$

Then, $E(H_l)/p^m$ is the orthogonal complement of itself under the above pairing ([15], Corollary 3.4, p. 53). We obtain the following

PROPOSITION 1 (Local Tate duality). *The cup product induces a non-degenerate pairing*

$$\langle \ , \ \rangle_l : E(H_l)/p^m \times H^1(H_l, E)_{p^m} \rightarrow \mathbb{Z}/p^m\mathbb{Z}.$$

Let $\text{Sel}_{p^m}(E/H)$ denote the p^m -Selmer group of E over H . Thus

$$\text{Sel}_{p^m}(E/H) := \text{Ker}(H^1(H, E_{p^m}) \rightarrow \prod_v H^1(H_v, E)_{p^m}),$$

where v runs over all places of H and we consider the kernel of the obvious map. Let

$$\text{res}_l : \text{Sel}_{p^m}(E/H) \rightarrow E(H_l)/p^m$$

be the restriction map. By taking Pontryagin duals and using Proposition 1, we get a map

$$\delta_l : H^1(H_l, E)_{p^m} \rightarrow \text{Sel}_{p^m}(E/H)^{\text{dual}}.$$

We shall denote the module $\text{Im}(\delta_l)$ by $V(l)$. Write

$$\delta = \oplus_l \delta_l : \oplus_l H^1(H_l, E)_{p^m} \rightarrow \text{Sel}_{p^m}(E/H)^{\text{dual}}$$

for the sum of the δ_l .

PROPOSITION 2 (Global duality). *Let $c \in H^1(H, E)_{p^m}$ be a global class and let $\text{res}(c)$ be its image in $\oplus_l H^1(H_l, E)_{p^m}$. Then $\delta(\text{res}(c)) = 0$, i.e., c pairs to zero with all the elements of the Selmer group $\text{Sel}_{p^m}(E/H)$.*

Proposition 2 follows from the global reciprocity law for the elements of the Brauer group of H : see [15], Lemma 6.15, p. 105 and [7], Theorem B, p. 188.

Recall from Subsection 1.1 that R denotes $\mathbb{Z}/p^m\mathbb{Z}[G]$ with $G = \text{Gal}(H/K)$. The group ring R may naturally be viewed as a module $R^{(\sigma)}$, $\sigma = \pm$ over the dihedral group $D = \text{Gal}(H/\mathbb{Q})$, by making τ act on it via the involution τ_σ defined on group-like elements by

$$g^{\tau_\sigma} := \sigma g^{-1}, \quad g \in G.$$

Hence $R^{(+)}$ corresponds to extending to R by linearity the natural action of τ on G .

DEFINITION 3. Given E of conductor N , p and $m \geq 1$ as above, a *Kolyvagin prime* for p^m is a rational prime number l which satisfies:

1. l does not divide $p \cdot N \cdot \text{disc}(K)$;
2. $\text{Frob}_l(K(E_{p^m})/\mathbb{Q}) = [\tau]$.

If the reference to p and m is clear from the context, l will simply be called a *Kolyvagin prime*. Note that l as above is inert in K . Let ℓ be the prime of K above l . Then ℓ is totally split in $H(E_{p^m})$ since, by class field theory, ℓ is totally split in H .

Let l be a Kolyvagin prime. Let λ be the prime of H above l such that $\text{Frob}_\lambda(H/\mathbb{Q}) = \tau$. Then $E(H_\lambda)/p^m$ and $H^1(H_\lambda, E)_{p^m}$ are τ -invariant. Define the D -modules

$$\begin{aligned} (E(H_l)/p^m)^{(\pm)} &:= R(E(H_\lambda)/p^m)^\pm, \\ (H^1(H_l, E)_{p^m})^{(\pm)} &:= R(H^1(H_\lambda, E)_{p^m})^\pm. \end{aligned}$$

They give direct sum decompositions of $E(H_l)/p^m$ and $H^1(H_l, E)_{p^m}$.

LEMMA 4. *Let l be a Kolyvagin prime for p^m . Then $(E(H_l)/p^m)^{(\pm)}$ is isomorphic to $R^{(\pm)}$ as a D -module. Thus $E(H_l)/p^m$ is isomorphic to $R^{(+)} \oplus R^{(-)}$.*

Proof. Let λ be the prime of H above l such that $\text{Frob}_\lambda(H/\mathbb{Q}) = \tau$. By definition of λ , $E_{p^m}(H_\lambda)$ is isomorphic to the direct sum of two copies of $\mathbb{Z}/p^m\mathbb{Z}$. Moreover, the reduction map induces isomorphisms of $\mathbb{Z}[\tau]$ -modules $E(H_\lambda)/p^m \simeq E(\mathbb{F}_\lambda)/p^m$, $E_{p^m}(H_\lambda) \simeq E_{p^m}(\mathbb{F}_\lambda)$. This implies that $E(H_\lambda)/p^m$ is isomorphic to $E_{p^m}(H_\lambda)$ as a $\mathbb{Z}[\tau]$ -module (see [2], remark after Corollary 3.5). By the existence of the Weil pairing, we deduce that $(E(H_\lambda)/p^m)^\pm$ is isomorphic to $\mathbb{Z}/p^m\mathbb{Z}$. The lemma follows.

LEMMA 5. *Let l be a Kolyvagin prime for p^m . Then $(E(H_l)/p^m)^{(\pm)}$ is the orthogonal complement of $(H^1(H_l, E)_{p^m})^{(\mp)}$ with respect to the local pairing $\langle \cdot, \cdot \rangle_l$.*

Proof. Let λ be the prime of H above l such that $\text{Frob}_\lambda(H/\mathbb{Q}) = \tau$. We make use of the Galois equivariance properties of the local Tate pairing, which follow directly from the definition ([15]). By the τ -equivariance of the non-degenerate pairing

$$\langle \cdot, \cdot \rangle_\lambda : E(H_\lambda)/p^m \times H^1(H_\lambda, E)_{p^m} \rightarrow \mathbb{Z}/p^m\mathbb{Z},$$

we get

$$((E(H_\lambda)/p^m)^\pm)^\perp = (H^1(H_\lambda, E)_{p^m})^\mp.$$

The claim follows from the G -equivariance of $\langle \cdot, \cdot \rangle_l$.

COROLLARY 6. *Let l be a Kolyvagin prime for p^m . Then $(H^1(H_l, E)_{p^m})^{(\pm)}$ is isomorphic to $R^{(\pm)}$ as a D -module. Thus $H^1(H_l, E)_{p^m}$ is isomorphic to $R^{(+)} \oplus R^{(-)}$.*

Proof. It follows from Lemma 4 and 5.

We conclude with a module-theoretic result which will be useful later.

LEMMA 7. *Let $(\alpha) = R\alpha$ and $(\beta) = R\beta$ be principal ideals of R . Assume that there is a surjection of R -modules*

$$R\alpha \twoheadrightarrow R\beta.$$

Then α divides β in R .

Proof.

Step 1. Let \mathcal{I} be the set of ideals of R . Given $I \in \mathcal{I}$, we denote by $\text{Ann}_R(I) \in \mathcal{I}$ the annihilator of I in R . Then the map

$$I \mapsto \text{Ann}_R(I)$$

is an inclusion-reversing injection. For, if I is an ideal of R , i.e., there is an inclusion of R -modules $I \subset R$, then its Pontryagin dual is a cyclic R -module, i.e., there is a projection of R -modules $R \twoheadrightarrow I^{\text{dual}}$. It is easy to see that $I^{\text{dual}} \simeq R/\text{Ann}_R(I^{\text{dual}})$ and $\text{Ann}_R(I^{\text{dual}}) = \text{Ann}_R(I)^{\tau+}$. Now assume that there are two distinct ideals I and J , with $J \not\subset I$, such that $\text{Ann}_R(I) = \text{Ann}_R(J)$. Hence $\text{Ann}_R(I + J) = \text{Ann}_R(I)$. But then

$$(I + J)^{\text{dual}} \simeq R/\text{Ann}_R(I^{\text{dual}}) \simeq I^{\text{dual}}.$$

This is a contradiction, because the cardinality of $(I + J)^{\text{dual}}$ is strictly greater than the cardinality of I^{dual} .

Step 2. The dual of the surjections $R \rightarrow (\alpha) \rightarrow (\beta)$, where the first map sends 1_G to α , gives the injections

$$(\beta)^{\text{dual}} \hookrightarrow (\alpha)^{\text{dual}} \hookrightarrow R.$$

Thus we may view the cyclic R -modules $(\alpha)^{\text{dual}}$ and $(\beta)^{\text{dual}}$ as principal ideals of R . Step 1 implies that they are equal to $(\alpha^{\tau+})$ and $(\beta^{\tau+})$, respectively. We deduce that $\alpha^{\tau+}$ divides $\beta^{\tau+}$ in R . Hence α divides β in R .

1.3. LOCAL CONTROL OF THE SELMER GROUP

Let

$$\rho_p : \text{Gal}(\overline{K}/K) \rightarrow \text{Aut}(E_{p^\infty}) \simeq \text{GL}_2(\mathbb{Z}_p)$$

denote the Galois representation arising from the p -torsion points of E . By a theorem of Serre [21], ρ_p is surjective for almost all p if E is a curve with no complex multiplications.

LEMMA 1. *Assume that ρ_p is surjective. Then the restriction map*

$$H^1(H, E_{p^m}) \rightarrow H^1(H(E_{p^m}), E_{p^m})^{\text{Gal}(H(E_{p^m})/H)}$$

is injective.

Proof. The kernel of the above map is equal to $H^1(\text{Gal}(H(E_{p^m})/H), E_{p^m})$. Identify $\text{Gal}(H(E_{p^m})/H)$ with a subgroup of $\text{GL}_2(\mathbb{Z}/p^m\mathbb{Z})$. Then the scalar matrix -1 belongs to $\text{Gal}(H(E_{p^m})/H)$, since p is odd. Let $\Sigma = \{\pm 1\}$ denote the normal subgroup generated by this element. The inflation-restriction sequence gives the exact sequence

$$\begin{aligned} 0 &\rightarrow H^1(\text{Gal}(H(E_{p^m})/H)/\Sigma, E_{p^m}^\Sigma) \\ &\rightarrow H^1(\text{Gal}(H(E_{p^m})/H), E_{p^m}) \rightarrow H^1(\Sigma, E_{p^m}). \end{aligned}$$

But $E_{p^m}^\Sigma = 0$ and $H^1(\Sigma, E_{p^m}) = 0$, since p is odd. This proves Lemma 1.

LEMMA 2. Assume that ρ_p is surjective and $p \geq 5$. Then the extensions K_∞/K and $K(E_{p^\infty})/K$ are linearly disjoint. In particular, $\text{Gal}(K_n(E_{p^m})/K_n)$ is isomorphic to $\text{GL}_2(\mathbb{Z}/p^m\mathbb{Z})$ for all m and n .

Proof. Since $\text{SL}_2(\mathbb{F}_p)$ is simple for $p \geq 5$ and the index of $\text{SL}_2(\mathbb{F}_p)$ in $\text{GL}_2(\mathbb{F}_p)$ is $p - 1$, $\text{Gal}(K_\infty(E_p)/K_\infty)$ is isomorphic to $\text{GL}_2(\mathbb{F}_p)$. By [22], Lemma 3, IV-23 we deduce that $\text{Gal}(K_\infty(E_{p^\infty})/K_\infty)$, viewed as a subgroup of $\text{GL}_2(\mathbb{Z}_p)$, contains $\text{SL}_2(\mathbb{Z}_p)$. Finally, note that the quotient group $\text{GL}_2(\mathbb{Z}_p)/\text{SL}_2(\mathbb{Z}_p)$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$, and the corresponding \mathbb{Z}_p -extension of K is the cyclotomic \mathbb{Z}_p -extension.

Under the assumptions of Lemma 2, it follows that

$$\begin{aligned} \text{Gal}(H(E_{p^m})/\mathbb{Q}) &= \text{Gal}(H(E_{p^m})/\mathbb{Q}(E_{p^m})) \times \text{Gal}(H(E_{p^m})/H) \\ &\simeq D \times \text{GL}_2(\mathbb{Z}/p^m\mathbb{Z}). \end{aligned}$$

Let $\mathcal{G} := \text{Gal}(H(E_{p^m})/H)$ and $\tilde{\mathcal{G}} := \text{Gal}(H(E_{p^m})/\mathbb{Q})$. Lemma 1 allows us to identify the elements of $\text{Sel}_{p^m}(E/H)$ with \mathcal{G} -homomorphisms of $\text{Gal}(\bar{H}/H(E_{p^m}))$ taking values in E_{p^m} . Given a D -submodule S of $\text{Sel}_{p^m}(E/H)$, let M_S denote the extension of $H(E_{p^m})$ cut out by S . Thus, if for $s \in S$ we let M_s denote the fixed field of $\text{Ker}(s)$, M_S is the compositum of the M_s with s varying in S .

LEMMA 3. Assume that ρ_p is surjective and $p \geq 5$. Then there is a canonical isomorphism of $\tilde{\mathcal{G}}$ -modules

$$\text{Gal}(M_S/H(E_{p^m})) \xrightarrow{\sim} \text{Hom}(S, E_{p^m}).$$

Proof.

Step 1. Let $s \in S$ be an element of order p^k . Since E_p is an irreducible \mathcal{G} -module, Lemma 1 implies that $\text{Gal}(M_s/H(E_{p^m}))$ is isomorphic to E_{p^k} .

Step 2. If S is isomorphic to $\bigoplus_{i=1}^s \mathbb{Z}/p^{k_i}\mathbb{Z}$, then $\text{Gal}(M_S/H(E_{p^m}))$ is isomorphic to $\bigoplus_{i=1}^s E_{p^{k_i}}$. This follows again from Lemma 1 and the irreducibility of E_p .

Step 3. Step 2 and Lemma 1 show that restriction induces a canonical identification

$$S = \text{Hom}_{\mathcal{G}}(\text{Gal}(M_S/H(E_{p^m})), E_{p^m}).$$

Then, the canonical map

$$\begin{cases} \text{Gal}(M_S/H(E_{p^m})) & \rightarrow \text{Hom}(S, E_{p^m}) \\ h & \mapsto (\phi_h : s \rightarrow s(h)) \end{cases}$$

is an isomorphism.

The next theorem and its corollaries will be crucial in the study of the Galois-module structure of the Selmer group that we undertake in Section 3. Recall the definition of the D -modules $R^{(+)}$ and $R^{(-)}$ given in Subsection 1.2.

THEOREM 4. Assume that ρ_p is surjective and $p \geq 5$. Let \bar{S} be a subquotient of $\text{Sel}_{p^m}(E/H)$, i.e., $\bar{S} = S/S'$, where $S' \subset S$ are D -submodules of $\text{Sel}_{p^m}(E/H)$. Assume

we are given a D -module decomposition $\bar{S} = \bar{S}^{(+)} \oplus \bar{S}^{(-)}$ of \bar{S} , and an injective map of D -modules

$$j : \bar{S} \hookrightarrow R^{(+)} \oplus R^{(-)}$$

such that $j(\bar{S}^{(+)} \oplus (0)) \subset R^{(+)} \oplus (0)$ and $j((0) \oplus \bar{S}^{(-)}) \subset (0) \oplus R^{(-)}$.

Then, for infinitely many Kolyvagin primes l for p^m the restriction map

$$\text{res}_l : \text{Sel}_{p^m}(E/H) \rightarrow E(H_l)/p^m$$

induces an embedding

$$\overline{\text{res}}_l : \bar{S} \hookrightarrow E(H_l)/p^m.$$

Proof. Let $\bar{S} = S/S'$ be as in the statement of the theorem. Define the D -submodules $S^{(\pm)}$ of S by the equalities

$$S^{(\pm)}/S' = \bar{S}^{(\pm)}.$$

The heart of the proof consists in an application of the Chebotarev density theorem to the extension cut out by the G -invariants of \bar{S} .

Step 1. We compute the G -invariants of \bar{S} . We have

$$\bar{S}^G = (\bar{S}^{(+)})^G \oplus (\bar{S}^{(-)})^G.$$

By our assumptions, $(\bar{S}^{(\pm)})^G$ injects into $(R^{(\pm)})^G$. By definition of $R^{(\pm)}$, $(R^{(\pm)})^G$ is isomorphic to $\mathbb{Z}/p^m\mathbb{Z}$, and τ acts on it by \pm . Thus,

$$(\bar{S}^{(\pm)})^G \simeq \mathbb{Z}/p^{m_{\pm}}\mathbb{Z},$$

with $m_{\pm} \leq m$. Moreover, τ acts on $(\bar{S}^{(\pm)})^G$ by \pm .

Step 2. Let L' , respectively, $L^{(\pm)}$ denote the extensions of $H(E_{p^m})$ cut out by S' , respectively, $S^{(\pm)}$. Lemma 3 identifies their Galois groups as follows:

$$\begin{aligned} \text{Gal}(L'/H(E_{p^m})) &= \text{Hom}(S', E_{p^m}), \\ \text{Gal}(L^{(\pm)}/H(E_{p^m})) &= \text{Hom}(S^{(\pm)}, E_{p^m}). \end{aligned}$$

Then, the extensions $L^{(+)} / L'$ and $L^{(-)} / L'$ are linearly disjoint and

$$\begin{aligned} \text{Gal}(L^{(+)}L^{(-)}/L') &= \text{Hom}(\bar{S}, E_{p^m}) \\ &= \text{Hom}(\bar{S}^{(+)}, E_{p^m}) \oplus \text{Hom}(\bar{S}^{(-)}, E_{p^m}). \end{aligned}$$

Finally, denote by $\tilde{L}^{(\pm)}$ the subfield of $L^{(\pm)}$ corresponding to $(\bar{S}^{(\pm)})^G$. In other words,

$$\begin{aligned} \text{Gal}(\tilde{L}^{(\pm)}/L') &= \text{Hom}((\bar{S}^{(\pm)})^G, E_{p^m}) \\ &\simeq \text{Hom}(\mathbb{Z}/p^{m_{\pm}}\mathbb{Z}, E_{p^m}). \end{aligned}$$

Step 3. We can choose elements $h_{\pm} \in \text{Gal}(\tilde{L}^{(\pm)}/L')$ such that

$$\#((h_{\pm})^{\tau} h_{\pm}) = p^{m_{\pm}}.$$

For, if h_{\pm} corresponds to a homomorphism ϕ in $\text{Hom}((\overline{S}^{(\pm)})^G, E_{p^m})$ under the identification of step 2, then $(h_{\pm})^{\tau} h_{\pm}$ corresponds to the homomorphism

$$s \mapsto \pm \tau \phi(s) + \phi(s).$$

Hence, it will suffice to choose a ϕ which sends a generator of $\mathbb{Z}/p^{m_{\pm}}\mathbb{Z}$ to an element of order $p^{m_{\pm}}$ in $(E_{p^m})^{\pm}$. The Chebotarev density theorem ensures the existence of infinitely many primes $\tilde{\lambda}$ of $\tilde{L}^{(+)}\tilde{L}^{(-)}$ such that

$$\text{Frob}_{\tilde{\lambda}}(\tilde{L}^{(+)}\tilde{L}^{(-)}/\mathbb{Q}) = \tau(h_+, h_-).$$

Then

$$\begin{aligned} \text{Frob}_{\tilde{\lambda}}(\tilde{L}^{(+)}\tilde{L}^{(-)}/K) &= (\tau(h_+, h_-))^2 \\ &= ((h_+)^{\tau} h_+, (h_-)^{\tau} h_-). \end{aligned}$$

Let λ , respectively l denote the prime of H , respectively the rational prime below $\tilde{\lambda}$. The number l is a Kolyvagin prime. Our choice of $\tilde{\lambda}$ implies that $(\overline{S}^{(\pm)})^G$ embeds into $(E(H_{\lambda})/p^m)^{\pm}$ (where, as usual, $(E(H_{\lambda})/p^m)^{\pm}$ denotes the submodule of $E(H_{\lambda})/p^m$ on which τ acts by \pm). Thus, the restriction map induces an embedding

$$\overline{S}^G \hookrightarrow E(H_{\lambda})/p^m.$$

Step 4. With l as in step 3, we claim that the restriction map induces an embedding

$$\overline{S} \hookrightarrow E(H_l)/p^m.$$

For, if there is a non-zero element s of \overline{S} which restricts to zero, then the non-trivial submodule $(Rs)^G$ of \overline{S}^G is mapped to zero. By step 3, this is impossible. This proves the claim, and concludes the proof of Theorem 4.

Next corollary is essentially a restatement of Theorem 4 in a form apt to be applied in the arguments of Section 3. Recall the definition of the module $V(l)$ given in Subsection 1.2.

COROLLARY 5. *Assume that ρ_p is surjective and $p \geq 5$. Let S be a D -submodule of $\text{Sel}_{p^m}(E/H)$ and let S^{dual} be its Pontryagin dual. Let*

$$f : R^{(+)} \oplus R^{(-)} \rightarrow S^{\text{dual}}$$

denote a D -equivariant map such that $f(R^{(+)} \oplus (0)) \cap f((0) \oplus R^{(-)}) = (0)$. Then, for infinitely many Kolyvagin primes l for p^m there exists a natural D -equivariant projection

$$\pi_f : V(l) \rightarrow \text{Im}(f).$$

Proof. We may reduce to Theorem 4 by taking Pontryagin duals. Observe that the dual of the D -module $R^{(\pm)}$ may be identified, non-canonically, with $R^{(\pm)}$. Hence, the dual of the map f gives a map of D -modules

$$\tilde{j} : S \rightarrow R^{(+)} \oplus R^{(-)}.$$

Let S' be the kernel of \tilde{j} , and let \bar{S} denote S/S' . Thus, \tilde{j} induces an injection

$$j : \bar{S} \hookrightarrow R^{(+)} \oplus R^{(-)}.$$

Let $\bar{S}^{(+)} := j^{-1}(R^{(+)} \oplus (0))$ and $\bar{S}^{(-)} := j^{-1}((0) \oplus R^{(-)})$. By our assumptions on f , \bar{S} decomposes as $\bar{S}^{(+)} \oplus \bar{S}^{(-)}$ and j satisfies the hypothesis of Theorem 4. Then there exist infinitely many Kolyvagin primes l for p^m such that the restriction map induces an injection

$$\text{res}_l : \bar{S} \hookrightarrow E(H_l)/p^m.$$

By passing to the duals and identifying $(E(H_l)/p^m)^{\text{dual}}$ with $H^1(H_l, E)_{p^m}$ via the local Tate duality, we get a surjective map

$$H^1(H_l, E)_{p^m} \rightarrow \bar{S}^{\text{dual}}.$$

But \bar{S}^{dual} is equal to $\text{Im}(f)$ and, by definition of $V(l)$, the above map factors through $V(l)$.

In Section 3, we shall also need the following immediate consequence of Theorem 4. The notations and assumptions are the same as in Corollary 5, and $R^{(\sigma)}$, $\sigma = \pm$ is identified in the obvious way with a submodule of $R^{(+)} \oplus R^{(-)}$.

COROLLARY 6. *Let \mathcal{E} be a D -submodule of S , and let $\pi : S^{\text{dual}} \rightarrow \mathcal{E}^{\text{dual}}$ be the dual of the inclusion $\mathcal{E} \subset S$. Assume that $\pi f(R^{(-\sigma)}) = 0$, with $\sigma = +$ or $-$, so that the dual of πf factors through a map*

$$\psi : \mathcal{E} \rightarrow R^{(\sigma)}.$$

Then, for infinitely many Kolyvagin primes l satisfying the conclusion of Corollary 5 the D -module $\psi(\mathcal{E})$ is isomorphic to the image $\text{res}_l \mathcal{E} \subset E(H_l)/p^m$ of \mathcal{E} under the restriction map.

Proof. Let l be a Kolyvagin prime chosen as in the proof of Corollary 5. Then the restriction map induces an injection

$$\mathcal{E}/\mathcal{E} \cap S' \hookrightarrow E(H_l)/p^m.$$

On the other hand, $\text{Im}(\pi f) = (\mathcal{E}/\mathcal{E} \cap S')^{\text{dual}}$. Hence, by definition of ψ , $\psi(\mathcal{E}) \simeq \mathcal{E}/\mathcal{E} \cap S'$.

1.4. HEEGNER POINTS AND KOLYVAGIN COHOMOLOGY CLASSES

(References: [2], [8].)

Assume that E is endowed with a modular parametrization $\phi : X_0(N) \rightarrow E$, and that every rational prime dividing the conductor N of E splits in K . In the Introduction we have defined the Heegner point $\alpha[n] \in E(K[n])$, $n \geq 1$ being prime to N .

Let p be an odd prime not dividing N . In order to simplify things, we assume that p does not divide $\text{disc}(K) \cdot \#\text{Pic}(\mathcal{O}_K)$. Recalling that H stands for the extension K_n , $K[p^{n+1}]$ is the ring class field of minimal conductor which contains H . Let r be a squarefree product of Kolyvagin primes for p^m . Let $H[r]$ denote the maximal subextension of $HK[r]$ having degree over H a power of p . Write $\alpha(r) \in E(H[r])$ for the trace from $K[rp^{n+1}]$ to $H[r]$ of the Heegner point $\alpha[rp^{n+1}]$. In particular, we get a Heegner point $\alpha = \alpha(1)$ defined over H .

Let $\mathcal{G}_r = \text{Gal}(H[r]/H)$, $\mathcal{G}_l = \text{Gal}(H[l]/H)$. Then $\mathcal{G}_r = \prod_{l|r} \mathcal{G}_l$. By class field theory, $\mathcal{G}_l \simeq \mathbb{Z}/n_l\mathbb{Z}$ with $n_l = p^{ord_p(l+1)}$. Since l is a Kolyvagin prime for p^m , $p^m \mid n_l$. Choose for each l a generator σ_l of \mathcal{G}_l , and let

$$D_l := \sum_{i=1}^{n_l-1} i\sigma_l^i \in (\mathbb{Z}/p^m\mathbb{Z})[\mathcal{G}_l], \quad D_r := \prod_{l|r} D_l \in (\mathbb{Z}/p^m\mathbb{Z})[\mathcal{G}_r].$$

In $\mathbb{Z}/p^m\mathbb{Z}[\mathcal{G}_l]$, we have the equality $(\sigma_l - 1)D_l = -\text{Norm}_l$. This gives the following

PROPOSITION 1 ([2], Lemma 3.3). $D_r\alpha(r) \in (E(H[r])/p^m)^{\mathcal{G}_r}$.

Assume that $E_p(H[r]) = 0$. (This follows, for instance, from the surjectivity of ρ_p , which we have assumed in the previous section.) Then, the long exact sequence associated to

$$0 \rightarrow E(H[r]) \xrightarrow{p^m} E(H[r]) \rightarrow E(H[r])/p^m \rightarrow 0$$

gives

$$0 \rightarrow E(H)/p^m \rightarrow (E(H[r])/p^m)^{\mathcal{G}_r} \rightarrow H^1(\mathcal{G}_r, E(H[r]))_{p^m} \rightarrow 0.$$

Thus, $D_r\alpha(r)$ gives rise to a cohomology class in $H^1(\mathcal{G}_r, E(H[r]))_{p^m}$. We call its image $d(r) \in H^1(H, E)_{p^m}$ under inflation a *Kolyvagin cohomology class*.

PROPOSITION 2 (Local behaviour. [2], Corollary 3.5; [8], Proposition 6.20).

1. If v does not divide r , then $\text{res}_v d(r) = 0$.
2. For $l \mid r$, there is a G -equivariant and τ -antiequivariant isomorphism

$$\phi_l : H^1(H_l, E)_{p^m} \rightarrow E(H_l)/p^m$$

such that

$$\phi_l(\text{res}_l d(r)) = \text{res}_l(D_{r/l}\alpha(r/l)).$$

2. Iwasawa theory

2.1. REVIEW OF IWASAWA THEORY

(References: [12], [13], [14], [16].)

As in the Introduction, K_∞ will denote the anticyclotomic \mathbb{Z}_p -extension of an imaginary quadratic field K , K_n the subextension of K_∞ having degree p^n over K , and Λ the Iwasawa algebra $\mathbb{Z}_p[[\Gamma]]$, with $\Gamma = \text{Gal}(K_\infty/K)$. We write Γ_n , respectively G_n for the Galois group $\text{Gal}(K_\infty/K_n) = \Gamma^{p^n}$, respectively, $\text{Gal}(K_n/K) = \Gamma/\Gamma_n$. Recall that $\text{Sel}_{p^\infty}(E/K_\infty)$ indicates the p -Selmer group of E over K_∞ , defined before. Let E/E^0 denote the group of connected components of the Néron model of E over $\text{Spec}(\mathcal{O}_K)$.

PROPOSITION 1. Assume that p is a prime of good ordinary reduction for E .

1. The kernel and the cokernel of the restriction maps

$$\text{Sel}_{p^\infty}(E/K_n) \rightarrow \text{Sel}_{p^\infty}(E/K_\infty)^{\Gamma_n}$$

are finite and bounded independently of n .

2. Assume that $E_p(K) = 0$ and $p \nmid \#\text{Pic}(\mathcal{O}_K) \cdot \#(E/E^0) \cdot \prod_{\mathcal{P}|p} \#E(\mathbb{F}_{\mathcal{P}})$, where the product is over the primes of K above p . Then the above maps are isomorphisms.

Proof. See [14] Chapter 1, or [13] Section 4.

Let

$$S_p(E/K_n) := \text{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \text{Sel}_{p^\infty}(E/K_n)),$$

$$E(K_n)_p := \text{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$

be the Tate modules of $\text{Sel}_{p^\infty}(E/K_n)$ and $E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$, respectively. We call $S_p(E/K_n)$ the *pro- p Selmer group of E over K_n* . Note that $E(K_n)_p$ is equal to $E(K_n)/(\text{torsion}) \otimes \mathbb{Z}_p$, and there is a natural injection of $E(K_n)_p$ into $S_p(E/K_n)$. If $E_p(K) = 0$, then $E(K_n)_p$ coincides with the p -adic completion of $E(K_n)$, and $S_p(E/K_n)$ is equal to the inverse limit of the p^m -Selmer groups $\text{Sel}_{p^m}(E/K_n)$ with respect to the maps induced by $E_{p^{m+1}} \xrightarrow{p} E_{p^m}$.

DEFINITION 2. The *pro- p Selmer group of E over K_∞* is defined to be

$$\hat{S}_p(E/K_\infty) := \varprojlim_n S_p(E/K_n),$$

the inverse limit being taken with respect to the natural corestriction maps.

We write, as before, \mathcal{X}_∞ for the Pontryagin dual of $\text{Sel}_{p^\infty}(E/K_\infty)$.

PROPOSITION 3. Let p be a prime of good ordinary reduction for E .

1. The $\mathbb{Z}_p[\text{Gal}(K_\infty/\mathbb{Q})]$ -modules $\hat{S}_p(E/K_\infty)$ and $\text{Hom}_\Lambda(\mathcal{X}_\infty, \Lambda)$ are canonically isomorphic.

2. The *pro- p Selmer group $\hat{S}_p(E/K_\infty)$ is a free Λ -module of finite rank.*

Proof.

1. [16], Lemme 5, p. 417.

2. Cf. [12], p. 201. In the sequel of the paper we shall need 2. only when the Λ -rank of \mathcal{X}_∞ is equal to 1. An alternate proof in this case goes as follows. By [16], Lemma 4 and 5, p. 415-7, $\hat{S}_p(E/K_\infty)_\Gamma$ injects into the free \mathbb{Z}_p -module $\text{Hom}_{\mathbb{Z}_p}((\mathcal{X}_\infty)_\Gamma, \mathbb{Z}_p)$. Moreover, its \mathbb{Z}_p -rank is equal to the Λ -rank of $\hat{S}_p(E/K_\infty)$, which is one by part 1. Thus $\hat{S}_p(E/K_\infty)_\Gamma$ is isomorphic to \mathbb{Z}_p . Since $\hat{S}_p(E/K_\infty)$ is not Λ -torsion, we conclude that it is isomorphic to Λ by [14], Lemma 6.8, p. 50.

We now work under the hypotheses of Subsection 1.4. Recall the Heegner point $\alpha_n \in E(K_n)$ defined in the Introduction: α_n is the trace from $K[p^{n+1}]$ to K_n of $\alpha[p^{n+1}]$. Denote by $\mathcal{E}(E/K_n)_p$ the submodule $\mathbb{Z}_p[G_n]\alpha_n$ of $E(K_n)_p$, spanned by the group ring $\mathbb{Z}_p[G_n]$ acting on α_n . Let a_p be the integer $1 + p - \#E(\mathbb{F}_p)$.

PROPOSITION 4. Choose K such that $\mathcal{O}_K^\times = \{\pm 1\}$. Let p be a prime of good ordinary reduction for E such that $p \nmid \#E(\mathbb{F}_p)\text{disc}(K)$. Moreover, assume that $a_p \not\equiv 2 \pmod{p}$

if p splits in K and $a_p \not\equiv -1 \pmod{p}$ if p is inert in K . Then, for all n , corestriction induces surjective maps

$$N_{K_{n+1}/K_n} : \mathcal{E}(E/K_{n+1})_p \rightarrow \mathcal{E}(E/K_n)_p.$$

In particular, we have natural inclusions $\mathcal{E}(E/K_n)_p \subset \mathcal{E}(E/K_{n+1})_p$.

Proof. The formulae for the action of the Hecke operators on the Heegner points ([16], Lemme 2, p. 432) imply

$$\begin{cases} N_{K_1/K}(\alpha_1) = (a_p - a_p^{-1}(p+1))\alpha_0, & \text{for } p \text{ inert in } K, \\ N_{K_1/K}(\alpha_1) = (a_p - (a_p - 2)^{-1}(p-1))\alpha_0, & \text{for } p \text{ split in } K. \end{cases} \quad (1)$$

$$N_{K_{n+1}/K_n}(\alpha_{n+1}) = a_p\alpha_n - \alpha_{n-1}, \quad \text{for } n \geq 1. \quad (2)$$

We reason by induction on n . By our assumptions, the number $a_p - a_p^{-1}(p+1)$, respectively $a_p - (a_p - 2)^{-1}(p-1)$ is a p -adic unit when p is inert in K , respectively p splits in K . This proves the proposition for $n = 0$. Assume the claim for $n - 1$. Then $\alpha_{n-1} = uN_{K_n/K_{n-1}}(\alpha_n)$ for some unit u of $\mathbb{Z}_p[G_{n-1}]$. Combining this equality with (2) we get

$$N_{K_{n+1}/K_n}(\alpha_{n+1}) = (a_p - uN_{K_n/K_{n-1}})\alpha_n.$$

Since a_p is a p -adic unit, $a_p - uN_{K_n/K_{n-1}}$ is a unit in $\mathbb{Z}_p[G_n]$. The claim for n follows.

In the sequel, we assume the hypotheses of Proposition 4.

DEFINITION 5. The Iwasawa module of the Heegner points is defined to be

$$\hat{\mathcal{E}}(E/K_\infty)_p := \varprojlim_n \mathcal{E}(E/K_n)_p,$$

where the inverse limit is taken with respect to the corestriction maps.

PROPOSITION 6. The Λ -module $\hat{\mathcal{E}}(E/K_\infty)_p$ is free of rank 0 or 1.

Proof. The Λ -module $\hat{\mathcal{E}}(E/K_\infty)_p$ is cyclic, and embeds naturally into $\hat{S}_p(E/K_\infty)$. But $\hat{S}_p(E/K_\infty)$ is torsion free by Proposition 3. Hence $\hat{\mathcal{E}}(E/K_\infty)_p$ is either equal to zero or isomorphic to Λ .

Note that $\hat{\mathcal{E}}(E/K_\infty)_p$ has rank 1 if and only if for some n the Heegner point α_n has infinite order.

2.2. ASSUMPTIONS

We recall the assumptions on (E, K, p) imposed in order to obtain the results of the previous sections. From now on we shall work under these assumptions.

- (1) E/\mathbb{Q} is a modular elliptic curve of conductor N .
- (2) K is an imaginary quadratic field such that all primes dividing N split in K and $\mathcal{O}_K^\times = \{\pm 1\}$.
- (3) $p \nmid 6N \text{disc}(K) \# \text{Pic}(\mathcal{O}_K) \# (E/E^0)$.

- (4) The Galois representation $\rho_p : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Aut}(E_{p^\infty})$ is surjective.
- (5) p is ordinary for E , i.e., $a_p \not\equiv 0 \pmod{p}$.
- (6) $p \nmid \#E(\mathbb{F}_{\mathcal{P}})$ for all primes \mathcal{P} of K above p .
- (7) $a_p \not\equiv 2 \pmod{p}$ if p splits in K .

Remarks.

1. According to the conjecture of Shimura–Taniyama–Weil, proved recently by Wiles and Taylor for semistable elliptic curves, all elliptic curves over \mathbb{Q} are modular. Given E and K satisfying (1) and (2), condition (3) excludes only a finite number of primes. The same is true for condition (4) if E has no complex multiplications, by a theorem of Serre [21]. Consider conditions (5), (6) and (7). Assume that p splits in K . If $p > 7$, then (5), (6) and (7) are equivalent to $a_p \neq 0, 1, 2$ in \mathbb{Z} , by the Hasse bound on a_p . Now fix a rational prime $l \neq p$ where E has good reduction. The integer a_p is equal to the trace of Frob_p acting on the Tate module $T_l(E)$. By [21], we may assume that $\text{Gal}(K(E_{l^n})/K)$ is isomorphic to $\text{GL}_2(\mathbb{Z}/l^n\mathbb{Z})$ for all $n \geq 1$. The Chebotarev density theorem, applied to the extensions $K(E_{l^n})/K$ for $n \rightarrow \infty$, implies that the set of p such that $a_p \neq 0, 1, 2$ has density 1. One deals similarly with the case of p inert in K , where (6) is equivalent to $a_p \not\equiv \pm 1 \pmod{p}$. In conclusion, given E and K satisfying (1) and (2), with E without complex multiplications, the other assumptions are satisfied by a set of primes of density 1.

2. By conditions (6) and (7), the corestriction maps on the Heegner points are surjective. This simplifies the construction and the study of the Iwasawa module of Heegner points. In the general situation one can still prove the analogue of Proposition 1.6 ([16], Proposition 10, p. 441) and the arguments in the sequel of the paper can be adapted, at the cost of more technical complications.

2.3. REMARKS ON THE SELMER GROUP

LEMMA 1.

- 1. The natural maps $\text{Sel}_{p^m}(E/K_n) \rightarrow \text{Sel}_{p^\infty}(E/K_n)[p^m]$ are isomorphisms.
- 2. The natural maps $\text{Sel}_{p^m}(E/K_n) \rightarrow \text{Sel}_{p^m}(E/K_{n'})^{\text{Gal}(K_{n'}/K_n)}$, $n \leq n' \leq \infty$, are isomorphisms.

Proof.

1. We have $E_p(K_n) = 0$ by our assumptions. The cohomology sequence associated to

$$0 \rightarrow E_{p^m} \rightarrow E_{p^{m'}} \xrightarrow{p^m} E_{p^{m'-m}} \rightarrow 0, \quad m' \geq m$$

identifies $H^1(K_n, E_{p^m})$ with $H^1(K_n, E_{p^{m'}})[p^m]$. Hence $\text{Sel}_{p^m}(E/K_n)$ is equal to $\text{Sel}_{p^{m'}}(E/K_n)[p^m]$. This implies the claim.

2. It is a consequence of part 1 and Proposition 1.1.

COROLLARY 2. We may identify

$$\text{Sel}_{p^\infty}(E/K_\infty) \quad \text{with} \quad \bigcup_n \text{Sel}_{p^\infty}(E/K_n) = \bigcup_{n,m} \text{Sel}_{p^m}(E/K_n),$$

where the inclusions are induced by the natural maps.

Let M_n denote the extension of $K_n(E_{p^n})$ cut out by $\text{Sel}_{p^n}(E/K_n)$. By Lemma 1.3.3 we have a natural identification

$$\text{Gal}(M_n/K_n(E_{p^n})) = \text{Hom}(\text{Sel}_{p^n}(E/K_n), E_{p^n}).$$

Let $M_\infty = \bigcup_n M_n$. Then

$$\begin{aligned} \text{Gal}(M_\infty/K_\infty(E_{p^\infty})) &= \varprojlim_n \text{Gal}(M_n/K_n(E_{p^n})) \\ &= \text{Hom}(\text{Sel}_{p^\infty}(E/K_\infty), E_{p^\infty}) \end{aligned}$$

is the Galois group of the extension of $K_\infty(E_{p^\infty})$ cut out by $\text{Sel}_{p^\infty}(E/K_\infty)$.

LEMMA 3. *We have canonical isomorphisms*

$$\begin{aligned} \text{Gal}(M_{n'}/K_{n'}(E_{p^{n'}})) \text{Gal}(K_{n'}/K_n)/p^n &\xrightarrow{\sim} \text{Gal}(M_n/K_n(E_{p^n})), \quad n' \geq n, \\ \text{Gal}(M_\infty/K_\infty(E_{p^\infty})) \Gamma_n/p^n &\xrightarrow{\sim} \text{Gal}(M_n/K_n(E_{p^n})). \end{aligned}$$

Proof. Apply Lemma 1.

LEMMA 4. *Let $g_\infty = (g_n)_{n \in \mathbb{N}}$, $g_n \in \text{Gal}(M_n/K_n(E_{p^n}))$ be an element of $\text{Gal}(M_\infty/K_\infty(E_{p^\infty}))$. For each n choose a Kolyvagin prime l_n such that $\text{Frob}_{l_n}(M_n/\mathbb{Q}) = [\tau g_n]$.*

1. *The module $V(l_n) \subset \text{Sel}_{p^n}(E/K_n)^{\text{dual}}$ depends only on the conjugacy class of $\text{Frob}_{l_n}(M_n/K)$.*
2. *There are natural projections $V(l_{n+1}) \rightarrow V(l_n)$, which give rise to a submodule $\varprojlim_n V(l_n)$ of \mathcal{X}_∞ .*

Proof. Thanks to Lemma 1.3.1 we may view the elements of $\text{Sel}_{p^n}(E/K_n)$ as homomorphisms of $\text{Gal}(M_n/K_n(E_{p^n}))$ with values in E_{p^n} . By definition of $V(l_n)$,

$$\begin{aligned} V(l_n)^{\text{dual}} &= \text{Sel}_{p^n}(E/K_n)/\{s \in \text{Sel}_{p^n}(E/K_n): \text{res}_{l_n}(s) = 0\} \\ &= \text{Sel}_{p^n}(E/K_n)/\{s \in \text{Sel}_{p^n}(E/K_n): s(\text{Frob}_{\tilde{\lambda}_n}(M_n/K)) \\ &= 0 \forall \tilde{\lambda}_n \mid l_n\}. \end{aligned}$$

This proves 1. Moreover, the natural injections

$$\text{Sel}_{p^n}(E/K_n) \hookrightarrow \text{Sel}_{p^{n+1}}(E/K_{n+1})$$

give rise to injections $V(l_n)^{\text{dual}} \hookrightarrow V(l_{n+1})^{\text{dual}}$. Part 2 follows.

We shall use the notation $V((\text{Frob}_{l_n})_{n \in \mathbb{N}})$ for the module defined in part 2 of Lemma 4, and sometimes write $V(\text{Frob}_{l_n})$ instead of $V(l_n)$ to emphasize the dependence of $V(l_n)$ only on the conjugacy class of Frob_{l_n} .

Finally, we introduce some notations concerning the Heegner points. Let \mathcal{E}_n denote the image of the module $\mathcal{E}(E/K_n)_p$ in $\text{Sel}_{p^n}(E/K_n)$. We have $\mathcal{E}_n \subset \mathcal{E}_{n+1}$. Let $\mathcal{E}_\infty := \bigcup_n \mathcal{E}_n$. Then \mathcal{E}_∞ is a Λ -submodule of $\text{Sel}_{p^\infty}(E/K_\infty)$.

3. On the structure of the Selmer group

3.1. THE RANK OF \mathcal{X}_∞

The goal of this section is to prove the following

THEOREM 1. *Assume that the Iwasawa module of the Heegner points $\hat{\mathcal{E}}(E/K_\infty)_p$ is non-zero. Then the rank over Λ of \mathcal{X}_∞ is equal to 1.*

Let $\text{III}(E/K_n)$ be the Shafarevich–Tate group of E over K_n . Define the Shafarevich–Tate group of E over K_∞ to be

$$\text{III}(E/K_\infty) := \varinjlim_n \text{III}(E/K_n),$$

the limit being taken with respect to the restriction mappings. The p -torsion of $\text{III}(E/K_\infty)$ fits in the descent exact sequence

$$0 \rightarrow E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \rightarrow \text{Sel}_{p^\infty}(E/K_\infty) \rightarrow \text{III}(E/K_\infty)_{p^\infty} \rightarrow 0.$$

COROLLARY 2. *Assume that $\hat{\mathcal{E}}(E/K_\infty)_p$ is non-zero. Then $(\text{III}(E/K_\infty)_{p^\infty})^{\text{dual}}$ is a torsion Λ -module.*

Proof. Let \mathcal{E}_∞ be the module defined in Subsection 2.3. The inclusions

$$\mathcal{E}_\infty \hookrightarrow E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \text{Sel}_{p^\infty}(E/K_\infty)$$

give rise to the projections

$$\mathcal{X}_\infty \twoheadrightarrow (E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\text{dual}} \twoheadrightarrow \mathcal{E}_\infty^{\text{dual}}.$$

We obtain $\text{rank}_\Lambda(E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\text{dual}} = 1$, since $\text{rank}_\Lambda(\mathcal{X}_\infty) = 1$ by Theorem 1 and $\text{rank}_\Lambda(\mathcal{E}_\infty^{\text{dual}}) = 1$ by our assumption on $\hat{\mathcal{E}}(E/K_\infty)_p$. Then, the Pontryagin dual of the above descent sequence shows that $(\text{III}(E/K_\infty)_{p^\infty})^{\text{dual}}$ is a torsion Λ -module, which embeds in $(\mathcal{X}_\infty)_{\text{tors}}$.

COROLLARY 3. *Assume that $\hat{\mathcal{E}}(E/K_\infty)_p$ is non-zero. Then there exists a non-decreasing bounded sequence of non-negative integers $\{e_n\}_{n \geq 1}$ such that $\text{rank}_{\mathbb{Z}_p}(S_p(E/K_n)) = p^n + e_n$.*

Proof. We have $\text{rank}_{\mathbb{Z}_p}(S_p(E/K_n)) = \text{rank}_{\mathbb{Z}_p}(\text{Sel}_{p^\infty}(E/K_n)^{\text{dual}})$. The claim follows from Proposition 2.1.1 and the theory of Λ -modules.

Remark 4. 1. Assuming the “standard” conjecture that $\text{III}(E, K_n)_{p^\infty}$ is finite for all n , Corollary 3 may be reformulated as a statement about the growth of the rank of the Mordell–Weil groups $E(K_n)$, since in this case $\text{rank}_{\mathbb{Z}}(E(K_n)) = \text{rank}_{\mathbb{Z}_p}(S_p(E/K_n))$.

2. The non-vanishing of the module $\hat{\mathcal{E}}(E/K_\infty)_p$ is conjectured by Mazur [12], Section 19. It is a natural expectation, in view of likely generalizations to ring class fields of the theorem of Gross and Zagier [9]. More specifically, given a finite order character $\chi : \Gamma \rightarrow \mathbb{C}^\times$ factoring through G_n , let $L(E/K, \chi, s)$ denote the L -function of E over K twisted by χ , and let $\alpha_n(\chi) \in E(K_n) \otimes \mathbb{C}$ be the χ -component of the Heegner point

$\alpha_n \in E(K_n)$. The analogue of Gross–Zagier’s limit formula in this setting (yet to be proven) is

$$L'(E/K, \chi, 1) = ah(\alpha_n(\chi)),$$

where h is the Néron–Tate height extended to $E(K_n) \otimes \mathbb{C}$ and a is a non-zero constant. Assuming this formula, the non-vanishing of $\hat{\mathcal{E}}(E/K_\infty)_p$ is reduced to the non-vanishing of $L'(E/K, \chi, 1)$ for some χ as above. It is expected that $L'(E/K, \chi, s)$ be non-zero for almost all χ , and results in this direction are obtained by Rohrlich [18] in the case of Hecke L -series attached to elliptic curves with complex multiplications.

3. The conclusion of Theorem 1 is predicted by Mazur’s “growth number conjecture” [12], Section 18. Assume that $L'(E/K, \chi, 1)$ is non-zero for almost all finite order characters $\chi : \Gamma \rightarrow \mathbb{C}^\times$. Then Theorem 1 follows from the Birch Swinnerton–Dyer Conjecture. In effect, by writing the L -function $L(E/K_n, s)$ as a product of the $L(E/K, \chi, s)$ corresponding to the characters which factor through G_n , one sees that the Birch Swinnerton–Dyer Conjecture implies, when n is sufficiently large,

$$\text{rank}_{\mathbb{Z}}(E(K_n)) = p^n + k \tag{*}$$

for some integer k independent of n . By the conjectural finiteness of $\text{III}(E/K_n)_{p^\infty}$ we have $\text{rank}_{\mathbb{Z}}(E(K_n)) = \text{rank}_{\mathbb{Z}_p}(\text{Sel}_{p^\infty}(E/K_n)^{\text{dual}})$. Theorem 1 now follows from Proposition 2.1.1 and the theory of Λ -modules.

4. Assume, in addition to the hypothesis of Theorem 1, that $\text{III}(E/K_n)_{p^\infty}$ is finite for all n . As we observed in the remark above, Theorem 1 follows in this case from the equalities (*). We sketch how to obtain these equalities from the main result of [2], whose methods, however, cannot be applied to study the p -Selmer group in p -extensions. Propositions 2.1.3 and 2.1.4, and the theory of Λ -modules show that for n sufficiently large

$$\text{rank}_{\mathbb{Z}_p} \mathcal{E}(E/K_n)_p = p^n - e,$$

where e is a non-negative constant independent of n . For such n let Σ_n^1 , respectively, Σ_n^2 be the set of characters $\chi : G_n \rightarrow \mathbb{C}_p^\times$ such that $\mathcal{E}(E/K_n)_p^{(\chi)}$ is isomorphic to \mathbb{C}_p , respectively, is zero, where (χ) indicates the χ -component. Then $\text{Card}(\Sigma_n^1) = p^n - e$. The Σ_n^2 have the same cardinality e and can be identified in the obvious way. Let

$$f = \dim_{\mathbb{C}_p}(\oplus_{\chi \in \Sigma_n^2} E(K_n)^{(\chi)}).$$

The integer f does not depend on n . The theorem of [2] (in a slightly modified form) implies that for $\chi \in \Sigma_n^1$

$$E(K_n)^{(\chi)} \simeq \mathbb{C}_p.$$

Then, $\text{rank}_{\mathbb{Z}}(E(K_n)) = p^n - e + f$, as claimed.

Proof of Theorem 1. Let r denote the Λ -rank of \mathcal{X}_∞ and let $R_n := \mathbb{Z}/p^n\mathbb{Z}[G_n]$. Recall the modules of Heegner points \mathcal{E}_n defined in Subsection 2.3. Since the \mathcal{E}_n are cyclic R_n -modules,

$$\mathcal{E}_\infty^{\text{dual}} = \varprojlim_n \mathcal{E}_n^{\text{dual}}$$

is a rank-one torsion-free Λ -module. The natural inclusion $\mathcal{E}_\infty \subset \text{Sel}_{p^\infty}(E/K_\infty)$ induces a $\mathbb{Z}_p[[\text{Gal}(K_\infty/\mathbb{Q})]]$ -equivariant projection

$$\mathcal{X}_\infty \xrightarrow{\pi} \mathcal{E}_\infty^{\text{dual}}.$$

The Λ -rank of $\ker \pi$ is equal to $r - 1$. Choose an element $x \in \mathcal{X}_\infty$ such that

$$\begin{cases} \tau x = \sigma x, & \sigma = \pm, \\ \pi x \neq 0. \end{cases}$$

Since $\mathcal{E}_\infty^{\text{dual}}$ is torsion-free, $\Lambda x \cap \ker \pi = 0$. We shall prove the theorem by showing that for all elements $y \in \ker \pi$ on which τ acts as ± 1 the module Λy is torsion. This suffices because if $y \in \text{Ker } \pi$ generates a free Λ -module, then either $y + \tau y$ or $y - \tau y$ generates a free Λ -module. We may also assume that

$$\tau y = -\sigma y,$$

σ as above. For, there exists a generator ω of the ideal $(\gamma - 1)\Lambda$, where γ is a topological generator of Γ , such that

$$\omega^\tau = -\omega.$$

If $\tau y = \sigma y$, we then replace y by ωy , since $\tau(\omega y) = -\sigma(\omega y)$ and Λy is torsion if and only if $\Lambda(\omega y)$ is torsion. In analogy with the definitions of Subsection 1.2, we may view the Iwasawa algebra Λ as a module $\Lambda^{(\pm)}$ over the pro-dihedral group $\text{Gal}(K_\infty/\mathbb{Q})$, by letting τ act via the involution τ_\pm defined on group-like elements by

$$\delta^{\tau_\pm} = \pm \delta^{-1}, \quad \delta \in \Gamma.$$

Let

$$f : \Lambda^{(\sigma)} \oplus \Lambda^{(-\sigma)} \rightarrow \mathcal{X}_\infty$$

be the composite of the $\mathbb{Z}_p[[\text{Gal}(K_\infty/\mathbb{Q})]]$ -equivariant maps

$$\begin{cases} \Lambda^{(\sigma)} \oplus \Lambda^{(-\sigma)} \rightarrow \Lambda x \oplus \Lambda y \\ (\xi, \eta) \mapsto \xi x + \eta y \end{cases}$$

and

$$\Lambda x \oplus \Lambda y \hookrightarrow \mathcal{X}_\infty.$$

In view of Lemma 2.3.1, we write

$$p_n : \mathcal{X}_\infty \rightarrow (\mathcal{X}_\infty)_{\Gamma_n}/p^n = \text{Sel}_{p^n}(E/K_n)^{\text{dual}}$$

for the natural projection. Let

$$Z_n := p_n f(\Lambda^{(\sigma)} \oplus (0)) \cap p_n f((0) \oplus \Lambda^{(-\sigma)}),$$

$$W_n^{(\sigma)} := p_n f(\Lambda^{(\sigma)} \oplus (0))/Z_n,$$

$$W_n^{(-\sigma)} := p_n f((0) \oplus \Lambda^{(-\sigma)})/Z_n.$$

Let S_n denote the D_n -submodule of $\text{Sel}_{p^n}(E/K_n)$, $D_n := \text{Gal}(K_n/\mathbb{Q})$, such that

$$S_n^{\text{dual}} = \text{Sel}_{p^n}(E/K_n)^{\text{dual}}/Z_n.$$

Define D_n -modules $R_n^{(+)}$ and $R_n^{(-)}$ as in Subsection 1.2. We have obvious maps

$$\Lambda^{(\sigma)} \oplus \Lambda^{(-\sigma)} \twoheadrightarrow R_n^{(\sigma)} \oplus R_n^{(-\sigma)} \twoheadrightarrow W_n^{(\sigma)} \oplus W_n^{(-\sigma)} \subset S_n^{\text{dual}}.$$

Let

$$f_n : R_n^{(\sigma)} \oplus R_n^{(-\sigma)} \rightarrow S_n^{\text{dual}}$$

be the composition of the second and the third map. Recall from Subsection 2.3 the definition of the modules $V(\text{Frob}_{l_n})$ and $V((\text{Frob}_{l_n})_{n \in \mathbb{N}})$. As in Subsection 2.3, let $M_n/K_n(E_{p^n})$, $n \leq \infty$, denote the extension cut out by the Selmer group $\text{Sel}_{p^n}(E/K_n)$.

LEMMA 5. *There exists a sequence of Kolyvagin primes $\{l_n\}_{n \in \mathbb{N}}$ such that:*

1. $\text{Frob}_{l_n}(M_n/\mathbb{Q}) = [\tau g_n]$, where the $g_n \in \text{Gal}(M_n/K_n(E_{p^n}))$ give rise to an element $(g_n)_{n \in \mathbb{N}}$ of $\text{Gal}(M_\infty/K_\infty(E_{p^\infty})) = \varinjlim_n \text{Gal}(M_n/K_n(E_{p^n}))$;
2. for all n there is a surjective map $V(\text{Frob}_{l_n}) \rightarrow W_n^{(\sigma)} \oplus W_n^{(-\sigma)}$.

Proof. The D_n -maps f_n satisfy the assumptions of Corollary 1.3.5, since, by construction,

$$f_n(R_n^{(\sigma)} \oplus (0)) \cap f_n((0) \oplus R_n^{(-\sigma)}) = (0).$$

Then, by the proof of Corollary 1.3.5 and Theorem 1.3.4, for any n there exists a natural D_n -equivariant projection

$$V(\text{Frob}_{l_n}) \twoheadrightarrow \text{Im}(f_n) = W_n^{(\sigma)} \oplus W_n^{(-\sigma)},$$

where l_n is a Kolyvagin prime such that $\text{Frob}_{l_n}(M_n/\mathbb{Q}) = [\tau g_n]$ for an element g_n of $\text{Gal}(M_n/K_n(E_{p^n}))$. We have to prove that the l_n can be so chosen that the elements g_n are compatible under the natural projections

$$\text{Gal}(M_{n+1}/K_{n+1}(E_{p^{n+1}})) \twoheadrightarrow \text{Gal}(M_n/K_n(E_{p^n})).$$

The construction of the elements g_n is explained in the proofs of Theorem 1.3.4 and Corollary 1.3.5, and the reader is urged to consult them at this point. As in the proof of Corollary 1.3.5, let

$$\tilde{j}_n : S_n \rightarrow R_n^{(\sigma)} \oplus R_n^{(-\sigma)}$$

denote the Pontryagin dual of f_n . Write S'_n for the kernel of \tilde{j}_n , and \bar{S}_n for S_n/S'_n . The injection

$$j_n : \bar{S}_n \hookrightarrow R_n^{(\sigma)} \oplus R_n^{(-\sigma)},$$

induced by \tilde{j}_n , gives rise to a decomposition

$$\bar{S}_n = \bar{S}_n^{(\sigma)} \oplus \bar{S}_n^{(-\sigma)},$$

where $\bar{S}_n^{(\sigma)} = j_n^{-1}(R_n^{(\sigma)} \oplus (0))$ and $\bar{S}_n^{(-\sigma)} = j_n^{-1}((0) \oplus R_n^{(-\sigma)})$. Let $S_n^{(\pm\sigma)}$ be defined by the equality

$$S_n^{(\pm\sigma)}/S'_n = \bar{S}_n^{(\pm\sigma)}.$$

Write L'_n for the extension of $K_n(E_{p^n})$ cut out by S'_n , and $\tilde{L}_n^{(\pm\sigma)}$ for the extension of L'_n cut out by the G_n -invariants $(\bar{S}_n^{(\pm\sigma)})^{G_n}$ of $\bar{S}_n^{(\pm\sigma)}$. Then $\tilde{L}_n^{(\sigma)}/L'_n$ and $\tilde{L}_n^{(-\sigma)}/L'_n$ are linearly disjoint, and their compositum \tilde{L}_n is equal to the extension of L'_n cut out by $(\bar{S}_n)^{G_n}$. We have canonical identifications

$$\text{Gal}(L'_n/K_n(E_{p^n})) = \text{Hom}(S'_n, E_{p^n})$$

and

$$\begin{aligned} \text{Gal}(\tilde{L}_n/L'_n) &= \text{Hom}((\bar{S}_n)^{G_n}, E_{p^n}) \\ &= \text{Hom}((\bar{S}_n^{(\sigma)})^{G_n}, E_{p^n}) \oplus \text{Hom}((\bar{S}_n^{(-\sigma)})^{G_n}, E_{p^n}). \end{aligned}$$

Moreover, $(\bar{S}_n^{(\pm\sigma)})^{G_n}$ is isomorphic to $\mathbb{Z}/p^{m_n, \pm\sigma}\mathbb{Z}$, $m_n, \pm\sigma \leq n$, equipped with a τ -action via multiplication by $\pm\sigma$. Let $\phi_n^{(\pm\sigma)} \in \text{Hom}((\bar{S}_n^{(\pm\sigma)})^{G_n}, E_{p^n})$ be a homomorphism which sends a generator of $(\bar{S}_n^{(\pm\sigma)})^{G_n}$ to an element of order $p^{m_n, \pm\sigma}$ in $(E_{p^n})^{\pm\sigma}$. Let h_n denote the element of $\text{Gal}(\tilde{L}_n/L'_n)$ corresponding to $(\phi_n^{(\sigma)}, \phi_n^{(-\sigma)})$ under the above identification. The proofs of Theorem 1.3.4 and Corollary 1.3.5 show that any Kolyvagin prime l_n such that $\text{Frob}_{l_n}(\tilde{L}_n/\mathbb{Q}) = [\tau h_n]$ satisfies part 2 of this lemma. Moreover, the natural inclusion $\text{Sel}_{p^n}(E/K_n) \hookrightarrow \text{Sel}_{p^{n+1}}(E/K_{n+1})$ induces a τ -equivariant injection

$$(\bar{S}_n^{(\pm\sigma)})^{G_n} \hookrightarrow (\bar{S}_{n+1}^{(\pm\sigma)})^{G_{n+1}}.$$

Thus we may choose the homomorphisms above so that h_{n+1} maps to h_n under the natural projection

$$\text{Gal}(\tilde{L}_{n+1}/L'_{n+1}) \twoheadrightarrow \text{Gal}(\tilde{L}_n/L'_n).$$

Finally, let T_n be the D_n -submodule of $\text{Sel}_{p^n}(E/K_n)$ such that

$$\text{Im}(p_n f) = (\text{Sel}_{p^n}(E/K_n)/T_n)^{\text{dual}}.$$

Write M'_n for the subextension of M_n cut out by T_n . We have a natural commutative diagram of surjective maps

$$\begin{array}{ccc} \text{Gal}(M_{n+1}/M'_{n+1}) & \longrightarrow & \text{Gal}(\tilde{L}_{n+1}/L'_{n+1}) \\ \downarrow & & \downarrow \\ \text{Gal}(M_n/M'_n) & \longrightarrow & \text{Gal}(\tilde{L}_n/L'_n). \end{array}$$

Then we may lift h_n to $g_n \in \text{Gal}(M_n/M'_n)$ so that for all n g_{n+1} maps to g_n . This completes the construction of the g_n , and the proof of Lemma 5.

Choose a set of l_n as in Lemma 5. By Lemma 2.3.4 there are natural projections $V(\text{Frob}_{l_{n+1}}) \rightarrow V(\text{Frob}_{l_n})$, giving rise to a commutative diagram of surjective maps

$$\begin{array}{ccc}
 V(\text{Frob}_{l_{n+1}}) & \longrightarrow & W_{n+1}^{(\sigma)} \oplus W_{n+1}^{(-\sigma)} \\
 \downarrow & & \downarrow \\
 V(\text{Frob}_{l_n}) & \longrightarrow & W_n^{(\sigma)} \oplus W_n^{(-\sigma)},
 \end{array} \tag{+}$$

where the horizontal arrows are the maps defined in Lemma 5 and the right vertical arrow is the dual of the injection $\overline{S}_n \hookrightarrow \overline{S}_{n+1}$.

LEMMA 6. *The limit of the projective system (+) is a surjective map*

$$V((\text{Frob}_{l_n})_{n \in \mathbb{N}}) \rightarrow \Lambda x \oplus \Lambda y.$$

Proof. By definition $V((\text{Frob}_{l_n})_{n \in \mathbb{N}}) = \varprojlim_n V(\text{Frob}_{l_n})$ (cf. Lemma 2.3.4). The limit of (+) is a surjective map by [11], Proposition 9.3, p. 109 (we are working with finite modules, hence they satisfy the Mittag-Leffler condition). Thus we are reduced to prove that

$$\varprojlim_n (W_n^{(\sigma)} \oplus W_n^{(-\sigma)}) = \Lambda x \oplus \Lambda y.$$

Consider the exact sequence of finite modules

$$0 \rightarrow Z_n \rightarrow \text{Im}(p_n f) \rightarrow W_n^{(\sigma)} \oplus W_n^{(-\sigma)} \rightarrow 0.$$

By passing to the limit we get

$$0 \rightarrow \varprojlim_n Z_n \rightarrow \Lambda x \oplus \Lambda y \rightarrow \varprojlim_n (W_n^{(\sigma)} \oplus W_n^{(-\sigma)}) \rightarrow 0.$$

But $\varprojlim_n Z_n$ is zero because it is contained in $\Lambda x \cap \Lambda y$.

LEMMA 7. *We can choose the $\{l_n\}_{n \in \mathbb{N}}$ of Lemma 5 so that $\text{rank}_\Lambda V((\text{Frob}_{l_n})_{n \in \mathbb{N}}) \leq 1$.*

Proof. Recall the maps

$$f_n : R_n^{(\sigma)} \oplus R_n^{(-\sigma)} \rightarrow S_n^{\text{dual}} = \text{Sel}_{p^n}(E/K_n)^{\text{dual}}/Z_n.$$

Let

$$\pi_n : \text{Sel}_{p^n}(E/K_n)^{\text{dual}} \rightarrow \mathcal{E}_n^{\text{dual}}$$

be the dual of the natural inclusion $\mathcal{E}_n \subset \text{Sel}_{p^n}(E/K_n)$. Since y maps to zero under the projection $\pi : \mathcal{X}_\infty \rightarrow \mathcal{E}_\infty^{\text{dual}}$, we have $\pi_n(Z_n) = 0$. Hence π_n induces a projection

$$\overline{\pi}_n : S_n^{\text{dual}} \rightarrow \mathcal{E}_n^{\text{dual}}.$$

In other words, \mathcal{E}_n is a submodule of S_n and not just of $\text{Sel}_{p^n}(E/K_n)$. Moreover, $\bar{\pi}_n f_n((0) \oplus R^{(-\sigma)}) = 0$. Thus, the dual of $\bar{\pi}_n f_n$ factors through a map

$$\psi_n : \mathcal{E}_n \rightarrow R_n^{(\sigma)},$$

where we have identified $R_n^{(\sigma)}$ with its dual. Let $\theta_n R_n^{(\sigma)}$ denote the image of the cyclic R_n -module \mathcal{E}_n under ψ_n . We may choose the θ_n so that they give rise to an element $\theta_\infty = (\theta_n)_{n \in \mathbb{N}} \in \Lambda$ of the Iwasawa algebra. This follows from the next commutative diagram expressing the compatibility properties of the maps ψ_n as n varies.

$$\begin{array}{ccc} \mathcal{E}_{n+1} & \xrightarrow{\psi_{n+1}} & R_{n+1}^{(\sigma)} \\ \uparrow & & \uparrow \\ \mathcal{E}_n & \xrightarrow{\psi_n} & R_n^{(\sigma)} \end{array}$$

The left vertical map is the natural inclusion $\mathcal{E}_n \subset \mathcal{E}_{n+1}$. Let α_n denote, by abuse of notation, the image of the Heegner point α_n in \mathcal{E}_n . Then

$$\alpha_n = u_n p N_{K_{n+1}/K_n}(\alpha_{n+1}),$$

where u_n is a unit in $\mathbb{Z}/p^n \mathbb{Z}[G_n]$. The right vertical map is an injection, and we may choose the identification of $R_n^{(\sigma)}$ with its dual for all n so that the element 1_{G_n} of $R_n^{(\sigma)}$ corresponds to $u_n p N_{K_{n+1}/K_n}$ in $R_{n+1}^{(\sigma)}$. The existence of the above diagram follows from the compatibility properties of the maps $\bar{\pi}_n f_n$. Choose a set of Kolyvagin primes $\{l_n\}_{n \in \mathbb{N}}$ as in the proof of Lemma 5. Then, Corollary 1.3.6 implies that

$$\text{res}_{l_n}(\mathcal{E}_n) \simeq \theta_n R_n^{(\sigma)}$$

as D_n -modules. Let $d(l_n) \in H^1(K_n, E)_{p^n}$ denote the Kolyvagin cohomology class $d(l_n)$ constructed in Subsection 1.4. By part 2 of Proposition 1.4.2

$$\text{res}_{l_n}(R_n d(l_n)) \simeq \theta_n R_n^{(-\sigma)}.$$

Recall the decomposition of Corollary 1.2.6

$$\begin{aligned} H^1((K_n)_{l_n}, E)_{p^n} &= H^1((K_n)_{l_n}, E)_{p^n}^{(\sigma)} \oplus H^1((K_n)_{l_n}, E)_{p^n}^{(-\sigma)} \\ &\simeq R_n^{(\sigma)} \oplus R_n^{(-\sigma)}. \end{aligned}$$

Let $\xi_{\pm\sigma}$ denote a generator of $H^1((K_n)_{l_n}, E)_{p^n}^{(\pm\sigma)}$ as a $R_n^{(\pm\sigma)}$ -module. Since

$$\text{res}_{l_n}(R_n d(l_n)) \cap H^1((K_n)_{l_n}, E)_{p^n}^{(\sigma)} = 0,$$

Lemma 1.2.7 implies that

$$\text{res}_{l_n} d(l_n) = (\rho_n \theta_n \xi_\sigma, v_n \theta_n \xi_{-\sigma}),$$

with $\rho_n \in R_n$ and $v_n \in R_n^\times$. Let $U_n := R_n(\rho_n \xi_\sigma, v_n \xi_{-\sigma})$. Then we have a decomposition

$$H^1((K_n)_{l_n}, E)_{p^n} = H^1((K_n)_{l_n}, E)_{p^n}^{(\sigma)} \oplus U_n.$$

We deduce

$$\theta_n H^1((K_n)_{l_n}, E)_{p^n} = \theta_n H^1((K_n)_{l_n}, E)_{p^n}^{(\sigma)} \oplus \text{res}_{l_n}(R_n d(l_n)).$$

By part 1 of Proposition 1.4.2 $d(l_n)$ restricts to 0 at all primes not above l_n . Hence, by Proposition 1.2.2 (global duality)

$$\delta_{l_n} \text{res}_{l_n}(R_n d(l_n)) = 0,$$

where $\delta_{l_n} : H^1((K_n)_{l_n}, E)_{p^n} \rightarrow \text{Sel}_{p^n}(E/K_n)^{\text{dual}}$ is the map induced by the local Tate duality defined in Subsection 1.2. By combining the above equalities we get

$$\begin{aligned} \theta_n V(\text{Frob}_{l_n}) &= \delta_{l_n}(\theta_n H^1((K_n)_{l_n}, E)_{p^n}) \\ &= \delta_{l_n}(\theta_n H^1((K_n)_{l_n}, E)_{p^n}^{(\sigma)}). \end{aligned}$$

We conclude that $\theta_n V(\text{Frob}_{l_n})$ is a cyclic R_n -module for all n . By taking the inverse limit of the projections of finite modules

$$V(\text{Frob}_{l_n}) \xrightarrow{\theta_n} \theta_n V(\text{Frob}_{l_n})$$

we find that $\theta_\infty V((\text{Frob}_{l_n})_{n \in \mathbb{N}})$ is a cyclic Λ -module. This proves Lemma 7.

Since Λx is a free Λ -module of rank 1, Lemma 6 and 7 imply that Λy is torsion (and also that the rank of $V((\text{Frob}_{l_n})_{n \in \mathbb{N}})$ is equal to 1). As we observed before, this suffices to prove Theorem 1.

3.2. THE ANNIHILATOR OF $(\mathcal{X}_\infty)_{\text{tors}}$

Let γ be a topological generator of $\text{Gal}(K_\infty/K)$, and let $\Lambda_n := \mathbb{Z}_p[G_n]$. Let $(\mathcal{X}_\infty)_{\text{tors}}$ denote the Λ -torsion submodule of \mathcal{X}_∞ . Assume, as in the previous section, that $\hat{\mathcal{E}}(E/K_\infty)_p$ is non-zero. Then, Proposition 1.1.3 and Theorem 1.1 imply

$$\hat{S}_p(E/K_\infty) \simeq \Lambda.$$

Write

$$\rho_\infty \Lambda := \text{char}(\hat{S}_p(E/K_\infty)/\hat{\mathcal{E}}(E/K_\infty)_p)$$

for the characteristic ideal of the torsion cyclic Λ -module $\hat{S}_p(E/K_\infty)/\hat{\mathcal{E}}(E/K_\infty)_p$.

THEOREM 1. *Assume that $\hat{\mathcal{E}}(E/K_\infty)_p$ is non-zero. Then:*

1. $(\gamma - 1)\rho_\infty(\mathcal{X}_\infty)_{\text{tors}}$ is finite.
 2. If $\gamma - 1 \nmid \rho_\infty$, then $\rho_\infty(\mathcal{X}_\infty)_{\text{tors}}$ is finite.
- In particular, we always have that $\rho_\infty^2(\mathcal{X}_\infty)_{\text{tors}}$ is finite.*

COROLLARY 2. *Assume that $\hat{\mathcal{E}}(E/K_\infty)_p$ is non-zero.*

Then $(\gamma - 1)\rho_\infty(\text{III}(E/K_\infty)_{p^\infty})^{\text{dual}}$ is finite and, when $\gamma - 1 \nmid \rho_\infty$, also $\rho_\infty(\text{III}(E/K_\infty)_{p^\infty})^{\text{dual}}$ is finite.

Proof. By the proof of Corollary 1.2, $(\text{III}(E/K_\infty)_{p^\infty})^{\text{dual}}$ embeds into $(\mathcal{X}_\infty)_{\text{tors}}$.

Proof of Theorem 1. We begin with a lemma on the structure of the Selmer group as a $\mathbb{Z}_p[[\text{Gal}(K_\infty/\mathbb{Q})]]$ -module.

LEMMA 3.

1. There exists a $\mathbb{Z}_p[[\text{Gal}(K_\infty/\mathbb{Q})]]$ -equivariant exact sequence

$$0 \rightarrow \mathcal{K} \rightarrow \mathcal{X}_\infty \rightarrow \Lambda \oplus (\mathcal{X}_\infty)_{\text{tors}} \rightarrow \mathcal{C} \rightarrow 0, \quad (*)$$

where \mathcal{C} and \mathcal{K} are finite and the action of τ on Λ is induced by one of the involutions τ_\pm .

2. The Γ_n -coinvariants of $(*)$ give rise to a $\mathbb{Z}_p[[\text{Gal}(K_n/\mathbb{Q})]]$ -equivariant exact sequence

$$0 \rightarrow \mathcal{K}(n) \rightarrow \text{Sel}_{p^\infty}(E/K_n)^{\text{dual}} \rightarrow \Lambda_n \oplus ((\mathcal{X}_\infty)_{\text{tors}})_{\Gamma_n} \rightarrow \mathcal{C}_{\Gamma_n} \rightarrow 0, \quad (**)$$

where $\mathcal{K}(n)$ is an extension of a quotient of \mathcal{C}^{Γ_n} by \mathcal{K}_{Γ_n} .

Proof of 1. (Reference: [5], p. 57)

Step 1. It is known the existence of a morphism $\mathcal{X}_\infty \rightarrow (\mathcal{X}_\infty)_{\text{tors}}$ whose restriction to $(\mathcal{X}_\infty)_{\text{tors}}$ is a quasi-isomorphism and a homotety by a factor λ . One checks that the same proof can be carried out by replacing λ by $\lambda\lambda^{\tau+}$. This gives a $\mathbb{Z}_p[[\text{Gal}(K_\infty/\mathbb{Q})]]$ -equivariant map

$$f : \mathcal{X}_\infty \rightarrow (\mathcal{X}_\infty)_{\text{tors}}$$

whose restriction to $(\mathcal{X}_\infty)_{\text{tors}}$ is a quasi-isomorphism.

Step 2. Let $\pi : \mathcal{X}_\infty \rightarrow \mathcal{X}_\infty/(\mathcal{X}_\infty)_{\text{tors}}$ denote the canonical projection. The map

$$\pi \oplus f : \mathcal{X}_\infty \rightarrow \mathcal{X}_\infty/(\mathcal{X}_\infty)_{\text{tors}} \oplus (\mathcal{X}_\infty)_{\text{tors}}$$

is a quasi-isomorphism, by the snake lemma.

Step 3. Since $\mathcal{X}_\infty/(\mathcal{X}_\infty)_{\text{tors}}$ is torsion free, the natural map to its Λ -bidual is injective and has finite cokernel. Being the bi-dual reflexive, it is free (of the same rank as \mathcal{X}_∞). Recall the canonical isomorphism $\text{Hom}_\Lambda(\mathcal{X}_\infty, \Lambda) \simeq \hat{S}_p(E/K_\infty)$ of Proposition 2.1.3. We obtain a $\mathbb{Z}_p[[\text{Gal}(K_\infty/\mathbb{Q})]]$ -equivariant quasi-isomorphism

$$\mathcal{X}_\infty/(\mathcal{X}_\infty)_{\text{tors}} \rightarrow \text{Hom}_\Lambda(\hat{S}_p(E/K_\infty), \Lambda) \simeq \Lambda,$$

where, if s is a generator of $\text{Hom}_\Lambda(\hat{S}_p(E/K_\infty), \Lambda)$ such that $\tau s = \delta s$, $\delta = \pm$, we choose an identification

$$\text{Hom}_\Lambda(\hat{S}_p(E/K_\infty), \Lambda) \simeq \Lambda$$

sending s to 1_Γ , and we assume that τ acts on Λ via τ_δ . By combining this with step 2, we prove the claim.

Proof of 2. By [19], Lemma 6.2, p. 407, we have an exact sequence

$$0 \rightarrow \mathcal{C}(n) \rightarrow (\text{Sel}_{p^\infty}(E/K_n)^{\text{dual}})_{\Gamma_n}/\mathcal{K}_{\Gamma_n} \rightarrow \Lambda_n \oplus ((\mathcal{X}_\infty)_{\text{tors}})_{\Gamma_n} \rightarrow \mathcal{C}_{\Gamma_n} \rightarrow 0,$$

where $\mathcal{C}(n)$ is a quotient of \mathcal{C}^{Γ_n} . The claim follows.

We continue with a lemma on universal norms. Let

$$US_p(E/K_n) := \bigcap_{m \geq n} \text{cores}_{K_m/K_n} S_p(E/K_m)$$

be the universal norms submodule of $S_p(E/K_n)$. We fix from now on a sequence (*) as in Lemma 3. Let $\beta \in \Lambda$ be any annihilator of \mathcal{C} . The sequence (*) determines in the obvious way an inclusion

$$\mu : \beta\Lambda \hookrightarrow \mathcal{X}_\infty/\mathcal{K}.$$

Moreover, by composing the middle map of (*) with the projection onto the first summand we get

$$\nu : \mathcal{X}_\infty/\mathcal{K} \rightarrow \Lambda.$$

The composite map $\nu\mu$ is the natural inclusion $\beta\Lambda \subset \Lambda$.

LEMMA 4. *By taking the Γ_n -coinvariants of the maps ν and μ and then applying the functor $\text{Hom}_{\mathbb{Z}_p}(\cdot, \mathbb{Z}_p)$ we find maps*

$$\begin{aligned} \text{Hom}_{\mathbb{Z}_p}(\Lambda_n, \mathbb{Z}_p) &\xrightarrow{\hat{\nu}} S_p(E/K_n), \\ S_p(E/K_n) &\xrightarrow{\hat{\mu}} \text{Hom}_{\mathbb{Z}_p}((\beta\Lambda)_{\Gamma_n}, \mathbb{Z}_p) \end{aligned}$$

such that:

1. $\hat{\mu}\hat{\nu}$ is the \mathbb{Z}_p -dual of the natural map $(\beta\Lambda)_{\Gamma_n} \rightarrow \Lambda_n$;
2. the image of $\hat{\nu}$ is contained in the universal norms submodule $US_p(E/K_n)$ of $S_p(E/K_n)$.

Proof.

Step 1. Note that there is a canonical identification

$$S_p(E/K_n) = \text{Hom}_{\mathbb{Z}_p}(\text{Sel}_{p^\infty}(E/K_n)^{\text{dual}}, \mathbb{Z}_p).$$

Since \mathcal{C} is finite, by applying $\text{Hom}_{\mathbb{Z}_p}(\cdot, \mathbb{Z}_p)$ to the sequence (**) we obtain

$$0 \rightarrow \text{Hom}_{\mathbb{Z}_p}(\Lambda_n, \mathbb{Z}_p) \oplus \text{Hom}_{\mathbb{Z}_p}(((\mathcal{X}_\infty)_{\text{tors}})_{\Gamma_n}, \mathbb{Z}_p) \rightarrow S_p(E/K_n).$$

This is canonically equal to

$$0 \rightarrow \text{Hom}_\Lambda(\Lambda, \Lambda_n) \oplus \text{Hom}_\Lambda((\mathcal{X}_\infty)_{\text{tors}}, \Lambda_n) \rightarrow \text{Hom}_\Lambda(\mathcal{X}_\infty, \Lambda_n),$$

where the norm mappings N_{K_{n+1}/K_n} are induced by the canonical projections

$\Lambda_{n+1} \rightarrow \Lambda_n$ (cf. [16], Lemme 4, p. 415). Hence we find an inclusion

$$\hat{\nu} : \text{Hom}_{\mathbb{Z}_p}(\Lambda_n, \mathbb{Z}_p) \hookrightarrow US_p(E/K_n).$$

Step 2. By definition of β , $(*)$ determines in the obvious way the exact sequence

$$0 \rightarrow \beta\Lambda \oplus \beta(\mathcal{X}_\infty)_{\text{tors}} \rightarrow \mathcal{X}_\infty/\mathcal{K} \rightarrow M_\beta \rightarrow 0,$$

where M_β is annihilated by β . By an argument similar to the one in step 1 we get an exact sequence

$$\begin{aligned} 0 &\rightarrow \text{Hom}_{\mathbb{Z}_p}((M_\beta)_{\Gamma_n}, \mathbb{Z}_p) \rightarrow S_p(E/K_n) \\ &\rightarrow \text{Hom}_{\mathbb{Z}_p}((\beta\Lambda)_{\Gamma_n}, \mathbb{Z}_p) \oplus \text{Hom}_{\mathbb{Z}_p}((\beta(\mathcal{X}_\infty)_{\text{tors}})_{\Gamma_n}, \mathbb{Z}_p). \end{aligned}$$

The composition of the last map with the projection onto the first factor gives the sought for map

$$\hat{\mu} : S_p(E/K_n) \rightarrow \text{Hom}_{\mathbb{Z}_p}((\beta\Lambda)_{\Gamma_n}, \mathbb{Z}_p).$$

Since $(\mathcal{X}_\infty)_{\text{tors}}$ is compact, in order to prove Theorem 1 it suffices to show that for all y in $(\mathcal{X}_\infty)_{\text{tors}}$ the module $(\gamma - 1)^t \rho_\infty \Lambda y \subset (\mathcal{X}_\infty)_{\text{tors}}$, $t = 0$ or 1 depending on the case considered, is finite. We may also assume that τ acts on y as ± 1 . Fix any such y and let

$$\tau y = \epsilon y,$$

with $\epsilon = \pm 1$. Let $\tilde{\tau}$ be the involution defining the action of τ on Λ in the sequence $(*)$. Let $\beta \in \Lambda$ denote any non-zero annihilator of \mathcal{C} such that

$$\beta^{\tilde{\tau}} = \sigma \beta,$$

with $\sigma = \pm 1$. Let x be an element of \mathcal{X}_∞ which maps to $(\beta, 0) \in \Lambda \oplus (\mathcal{X}_\infty)_{\text{tors}}$ under the map $\mathcal{X}_\infty \rightarrow \Lambda \oplus (\mathcal{X}_\infty)_{\text{tors}}$ of $(*)$, and such that

$$\tau x = \sigma x,$$

σ as above. Note that

$$\Lambda x \cap \Lambda y = (0),$$

since Λx is torsion-free. Thus we have a $\mathbb{Z}_p[[\text{Gal}(K_\infty/\mathbb{Q})]]$ -equivariant map

$$\begin{cases} f : \Lambda^{(\sigma)} \oplus \Lambda^{(\epsilon)} \rightarrow \Lambda x \oplus \Lambda y \subset \mathcal{X}_\infty \\ (\xi, \eta) \mapsto \xi x + \eta y \end{cases}$$

where τ acts via τ_σ , respectively, τ_δ on the first, respectively, second copy of Λ . With notations as in the previous section, we let

$$\begin{aligned} Z_n &:= p_n f(\Lambda^{(\sigma)} \oplus (0)) \cap p_n f((0) \oplus \Lambda^{(\epsilon)}), \\ W_n^{(\sigma)} &:= p_n f(\Lambda^{(\sigma)} \oplus (0))/Z_n, \\ W_n^{(\epsilon)} &:= p_n f((0) \oplus \Lambda^{(\epsilon)})/Z_n, \\ S_n^{\text{dual}} &:= \text{Sel}_{p^n}(E/K_n)^{\text{dual}}/Z_n, \end{aligned}$$

where

$$p_n : \mathcal{X}_\infty \rightarrow (\mathcal{X}_\infty)_{\Gamma_n}/p^n = \text{Sel}_{p^n}(E/K_n)^{\text{dual}}$$

is the natural projection and S_n is viewed as a submodule of $\text{Sel}_{p^n}(E/K_n)$. We obtain D_n -maps

$$f_n : R_n^{(\sigma)} \oplus R_n^{(\epsilon)} \rightarrow W_n^{(\sigma)} \oplus W_n^{(\epsilon)} \subset S_n^{\text{dual}}.$$

Note that if $\epsilon = -\sigma$ then the maps f_n satisfy the assumptions of Corollary 1.3.5. Finally, let π , respectively, π_n denote the dual of the natural inclusion $\mathcal{E}_\infty \subset \text{Sel}_{p^\infty}(E/K_\infty)$, respectively, $\mathcal{E}_n \subset \text{Sel}_{p^n}(E/K_n)$. Since $\mathcal{E}_\infty^{\text{dual}}$ is torsion-free, then $\pi((\mathcal{X}_\infty)_{\text{tors}}) = 0$. In particular, $\pi f((0) \oplus \Lambda^{(\epsilon)}) = 0$. As in the proof of Lemma 1.7, this implies that \mathcal{E}_n is contained in S_n . Let $\bar{\pi}_n$ be the dual of this inclusion. Since $\bar{\pi}_n f_n((0) \oplus R_n^{(\epsilon)}) = 0$, the dual of $\bar{\pi}_n f_n$ induces a map

$$\psi_n : \mathcal{E}_n \rightarrow R_n^{(\sigma)},$$

where we have identified $R_n^{(\sigma)}$ with its dual.

LEMMA 5. $\beta \rho_\infty R_n^{(\sigma)} \subset \text{Im}(\psi_n) \subset \rho_\infty R_n^{(\sigma)}$.

Proof. Let $\theta_n \text{Hom}_{\mathbb{Z}_p}((\beta\Lambda)_{\Gamma_n}, \mathbb{Z}_p)$, $\theta_n \in \mathbb{Z}_p[G_n]$ denote the image of the composite map

$$\mathcal{E}(E/K_n)_p \hookrightarrow S_p(E/K_n) \xrightarrow{\hat{\mu}} \text{Hom}_{\mathbb{Z}_p}((\beta\Lambda)_{\Gamma_n}, \mathbb{Z}_p) \simeq \mathbb{Z}_p[G_n]. \tag{+}$$

The universal norms submodule $US_p(E/K_n)$ is isomorphic to $\mathbb{Z}_p[G_n]$. For, we have a projection

$$\hat{S}_p(E/K_\infty)_{\Gamma_n} \rightarrow US_p(E/K_n),$$

where $\hat{S}_p(E/K_\infty)_{\Gamma_n} \simeq \Lambda_n$. Moreover, $\text{rank}_{\mathbb{Z}_p}(US_p(E/K_n)) = p^n$, since $\text{Im}(\hat{\nu})$ is contained in $US_p(E/K_n)$. Then, by Lemma 4

$$\beta \rho_\infty \text{Hom}_{\mathbb{Z}_p}((\beta\Lambda)_{\Gamma_n}, \mathbb{Z}_p) \subset \theta_n \text{Hom}_{\mathbb{Z}_p}((\beta\Lambda)_{\Gamma_n}, \mathbb{Z}_p) \subset \rho_\infty \text{Hom}_{\mathbb{Z}_p}((\beta\Lambda)_{\Gamma_n}, \mathbb{Z}_p).$$

By tensoring (+) with $\mathbb{Z}/p^n\mathbb{Z}$ we get

$$\mathcal{E}(E/K_n)_p/p^n \rightarrow S_p(E/K_n)/p^n \rightarrow \text{Hom}_{\mathbb{Z}_p}((\beta\Lambda)_{\Gamma_n}, \mathbb{Z}_p)/p^n \simeq R_n^{(\sigma)}. \tag{++}$$

Since $S_p(E/K_n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ is canonically isomorphic to the divisible subgroup of $\text{Sel}_{p^\infty}(E/K_n)$, we can view $S_p(E/K_n)/p^n$ as a submodule of $\text{Sel}_{p^n}(E/K_n)$. Thus (++) induces in the obvious way a map

$$\mathcal{E}_n \rightarrow R_n^{(\sigma)}.$$

One checks, by unfolding the various definitions, that this coincides with ψ_n , provided that it is chosen a suitable identification of $\text{Hom}_{\mathbb{Z}_p}((\beta\Lambda)_{\Gamma_n}, \mathbb{Z}_p)/p^n$ with $R_n^{(\sigma)}$.

Case 1. $\epsilon = -\sigma$. We use the same notations as in Lemma 1.5.

LEMMA 6. Assume $\epsilon = -\sigma$. We can find a sequence of Kolyvagin primes $\{l_n\}_{n \in \mathbb{N}}$ such that:

1. $\text{Frob}_{l_n}(M_n/\mathbb{Q}) = [\tau g_n]$, where $(g_n)_{n \in \mathbb{N}}$ belongs to $\text{Gal}(M_\infty/K_\infty(E_{p^\infty}))$;
2. there exists a natural surjective map $V((\text{Frob}_{l_n})_{n \in \mathbb{N}}) \rightarrow \Lambda x \oplus \Lambda y$;
3. $\beta \rho_\infty V((\text{Frob}_{l_n})_{n \in \mathbb{N}})$ is a cyclic Λ -module.

Proof. We may repeat the arguments of the proof of the Lemmas 1.5–1.7. In particular, if we let $\text{Im}(\psi_n) = \theta_n R_n^{(\sigma)}$, where the θ_n give rise to $\theta_\infty \in \Lambda$, the proof of 1.7 shows that $\theta_\infty V((\text{Frob}_{l_n})_{n \in \mathbb{N}})$ is a cyclic Λ -module. By Lemma 5, θ_n divides $\beta \rho_\infty$ in R_n for all n . Hence θ_∞ divides $\beta \rho_\infty$ in Λ . It follows that $\beta \rho_\infty V((\text{Frob}_{l_n})_{n \in \mathbb{N}})$ is a cyclic Λ -module.

COROLLARY 7. $(\beta \rho_\infty) \Lambda y = 0$.

Proof. By Lemma 6 we have a surjection

$$\beta \rho_\infty V((\text{Frob}_{l_n})_{n \in \mathbb{N}}) \rightarrow (\beta \rho_\infty) \Lambda x \oplus (\beta \rho_\infty) \Lambda y.$$

Since Λx is non-zero and torsion-free, then $(\beta \rho_\infty) \Lambda x$ is also non-zero and torsion-free. Hence $(\beta \rho_\infty) \Lambda y$ is equal to zero.

Case 2. $\epsilon = \sigma$.

LEMMA 8. Assume that $\epsilon = \sigma$. We can find a sequence of Kolyvagin primes $\{l_n\}_{n \in \mathbb{N}}$ such that:

1. $\text{Frob}_{l_n}(M_n/\mathbb{Q}) = [\tau g_n]$, where $(g_n)_{n \in \mathbb{N}}$ belongs to $\text{Gal}(M_\infty/K_\infty(E_{p^\infty}))$;
2. there exists a natural surjective map $V((\text{Frob}_{l_n})_{n \in \mathbb{N}}) \rightarrow \Lambda x \oplus \Lambda(\gamma - 1)y$;
3. $\beta \rho_\infty V((\text{Frob}_{l_n})_{n \in \mathbb{N}})$ is a cyclic Λ -module.

Proof. The module $\Lambda(\gamma - 1)y$ has a generator on which τ acts as $-\sigma$. Then apply Lemma 6 to the modules Λx and $\Lambda(\gamma - 1)y$.

COROLLARY 9. $\beta(\gamma - 1) \rho_\infty \Lambda y = 0$.

Since the β generate a finite-index ideal of Λ , we conclude that

$$\#((\gamma - 1) \rho_\infty (\mathcal{X}_\infty)_{\text{tors}}) < \infty.$$

When $\gamma - 1 \nmid \rho_\infty$, Theorem 1 follows from the next lemma.

LEMMA 10. Assume that $\gamma - 1 \nmid \rho_\infty$. Then $\rho_\infty (\mathcal{X}_\infty)_{\text{tors}}$ is finite.

Proof. By the definition of ρ_∞ and the assumption, we have $\mathcal{E}(E, K)_p \simeq \mathbb{Z}_p$, i.e., the Heegner point over K has infinite order. Then, by a theorem of Kolyvagin [10],

$$\text{rank}_{\mathbb{Z}_p} \text{Sel}_{p^\infty}(E, K)^{\text{dual}} = 1.$$

We claim that $\gamma - 1$ does not divide the characteristic power series of $(\mathcal{X}_\infty)_{\text{tors}}$. Otherwise, $(\mathcal{X}_\infty)_{\text{tors}}$ would be quasi-isomorphic to a module containing a direct summand of the

type $\Lambda/(\gamma - 1)^k$, $k \geq 1$, by the theory of Λ -modules. Then $\text{rank}_{\mathbb{Z}_p}((\mathcal{X}_\infty)_{\text{tors}})_\Gamma \geq 1$, and, by the sequence (*),

$$\text{rank}_{\mathbb{Z}_p} \text{Sel}_{p^\infty}(E, K)^{\text{dual}} \geq 2,$$

a contradiction. Since $(\gamma - 1)\rho_\infty(\mathcal{X}_\infty)_{\text{tors}}$ is finite, the lemma follows.

Remark 11. 1. B. Perrin-Riou [16] formulates a conjecture relating ρ_∞ to the characteristic ideal $\text{char}((\mathcal{X}_\infty)_{\text{tors}})$ of $(\mathcal{X}_\infty)_{\text{tors}}$. We assume for simplicity that the Manin constant of the modular parametrization of E is a p -adic unit.

Conjecture (Perrin-Riou). Assume that $\hat{S}_p(E/K_\infty)$ and $\hat{\mathcal{E}}(E/K_\infty)_p$ are Λ -modules of rank 1. Then $\rho_\infty^2 \Lambda = \text{char}((\mathcal{X}_\infty)_{\text{tors}})$.

Note that Theorem 1.1 shows that it is enough to assume that $\hat{\mathcal{E}}(E/K_\infty)_p$ has rank 1. The conjecture implies that $\rho_\infty^2(\mathcal{X}_\infty)_{\text{tors}}$ is finite. Let C_∞ , respectively, L_∞ denote the cyclotomic \mathbb{Z}_p -extension of K , respectively, the unique \mathbb{Z}_p^2 -extension of K . Assume that the Pontryagin dual of $\text{Sel}_{p^\infty}(E, L_\infty)$ is a $\mathbb{Z}_p[[\text{Gal}(L_\infty/K)]]$ -torsion module, and write \mathcal{L}_∞ for its characteristic power series (defined up to a unit). Perrin-Riou’s conjecture may be reformulated by stating the equality between the first derivative in the direction of C_∞ of \mathcal{L}_∞ restricted to K_∞ and the discriminant of a certain p -adic height pairing defined on the module $\hat{\mathcal{E}}(E/K_\infty)_p$ of the Heegner points. In view of the relation between the Heegner points and the analytic p -adic L -function interpolating special values of complex L -functions attached to E , proved for characters of the Hilbert class field of K in [17] and likely to extend to arbitrary ring class field characters, this conjecture states the equality between the first derivatives of an analytic p -adic L -function and an algebraic p -adic L -function. Thus, it may be viewed as an analogue in the present situation of the Main Conjecture of Iwasawa theory for cyclotomic fields.

2. Let $\sigma = \pm$ be such that we have an isomorphism of $\mathbb{Z}_p[[\text{Gal}(K_\infty/\mathbb{Q})]]$ -modules

$$\hat{S}_p(E/K_\infty) \simeq \Lambda^{(\sigma)}.$$

Let $((\mathcal{X}_\infty)_{\text{tors}})^{(-\sigma)}$ denote the Λ -submodule of $(\mathcal{X}_\infty)_{\text{tors}}$ generated by all the elements y such that $\tau y = -\sigma y$. Then the methods of the proof of Theorem 1 give

$$\#(\rho_\infty((\mathcal{X}_\infty)_{\text{tors}})^{(-\sigma)}) < \infty.$$

In fact, one checks that it is possible to find x and β as in the proof of Theorem 1 so that β varies among the generators of a finite index ideal of Λ and $\tau x = \sigma x$, σ as above. Then the claim follows from Lemma 6.

3. By comparing Theorem 1 with the results of Kolyvagin over K , one is lead to ask whether it should be expected that $\rho_\infty(\mathcal{X}_\infty)_{\text{tors}}$ be always finite. The results of [3] and [4], where in some cases alternating “derived” height pairings are constructed on the Selmer groups $\text{Sel}_{p^n}(E/K_n)$, might shed some light on this question.

4. In view of the results of this chapter, it would be desirable to know whether there can be finite submodules of \mathcal{X}_∞ . We plan to discuss the problem in a future paper.

Acknowledgements

It is a pleasure to thank my advisor Karl Rubin for suggesting the problem and providing valuable comments, and Henri Darmon for many stimulating conversations on the topics of this paper.

References

1. Bertolini, M.: Iwasawa Theory, L -functions and Heegner Points, PhD Thesis, Columbia University, 1992.
2. Bertolini, M. and Darmon, H.: Kolyvagin's descent and Mordell–Weil groups over ring class fields, *J. für die Reine und Angewandte Mathematik* **412** (1990), 63–74.
3. Bertolini, M. and Darmon, H.: Derived heights and generalized Mazur–Tate regulators, *Duke Math. J.* **76** (1994), 75–111.
4. Bertolini, M. and Darmon, H.: Derived p -adic heights, submitted.
5. Bourbaki, N.: *Algèbre Commutative*, Ch.7, Diviseurs, Hermann et Co., Paris, 1965.
6. Darmon, H.: Refined Class Number Formulas and Derivatives of L -functions, PhD Thesis, Harvard University, 1991.
7. Cassels, J. W. S. and Fröhlich, A.: *Algebraic Number Theory*, Academic Press, New York, 1969.
8. Gross, B. H.: Kolyvagin's work on modular elliptic curves, in *L-functions and Arithmetic*, Cambridge University Press, Cambridge, 1991, pp. 235–256.
9. Gross, B. H. and Zagier, D.: Heegner points and derivatives of L -series, *Inventiones Math.* **84** (1986), 225–320.
10. Kolyvagin, V. A.: *Euler Systems*, The Grothendieck Festschrift, vol. 2, Progr. in Math. **87**, Birkhäuser, 1990, pp. 435–483.
11. Lang, S.: *Algebra*, 2nd edn, Addison Wesley, 1984.
12. Mazur, B.: *Modular Curves and Arithmetic*, Proc. Int. Congress of Math., Warszawa, 1983.
13. Mazur, B.: Rational points of Abelian Varieties with values in towers of number fields, *Inventiones Math.* **18** (1972), 183–266.
14. Manin, Ju.: Cyclotomic fields and modular curves. Engl. transl.: *Russian Math. Surveys* **26** (1971), 7–78.
15. Milne, J. S.: Arithmetic duality theorems, in *Perspective in Math.*, Academic Press, New York, 1986.
16. Perrin-Riou, B.: Fonctions L p -adiques, Théorie d'Iwasawa et points de Heegner, *Bull. Soc. Math. de France* **115** (1987), 399–456.
17. Perrin-Riou, B.: Points de Heegner et dérivées de fonctions L p -adiques, *Inventiones Math.* **89** (1987), 455–510.
18. Rohrlich, D.: On L -functions of elliptic curves and anti-cyclotomic towers, *Inventiones Math.* **64** (1984), 383–408.
19. Rubin, K. C.: The Main Conjecture, Appendix in S. Lang, *Cyclotomic fields*, I and II, GTM 121, Springer-Verlag, 1990.
20. Rubin, K. C.: The “main conjectures” of Iwasawa theory for imaginary quadratic fields, *Inventiones Math.* **103** (1991), 25–68.
21. Serre, J. P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Inventiones Math.* **15** (1972), 259–331.
22. Serre, J. P.: *Abelian l -adic Representations and Elliptic Curves*, Advanced Book Classics, Addison Wesley, 1989.
23. Tate, J.: *WC-groups over p -adic Fields*, Séminaire Bourbaki no. 156, 1957.
24. Tate, L.: Duality theorems in Galois cohomology over number fields, in *Proc. Int. Congress of Math.*, Stockholm, 1962, pp. 288–295.