Journal de Théorie des Nombres
de Bordeaux **13** (2001), 1–25

Iwasawa theory for elliptic curves over imaginary quadratic fields

par Massimo BERTOLINI

Résumé. Soit E une courbe elliptique sur $\mathbb{Q}$, soit K un corps quadratique imaginaire, et soit K_∞ une $\mathbb{Z}_p$-extension de K. Étant donné un ensemble Σ de places de K contenant les places au-dessus de p et les places de mauvaise réduction de E, nous notons K_Σ l'extension maximale de K non ramifiée en-dehors de Σ. Cet article est consacré à l'étude de la structure des groupes de cohomologie $H^i(K_\Sigma/K_\infty, E_{p^\infty})$ pour $i = 1, 2$, et de la composante p-primaire du groupe de Selmer $\mathrm{Sel}_{p^\infty}(E/K_\infty)$, considérés comme modules discrets sur l'algèbre d'Iwasawa de K_∞/K.

Abstract. Let E be an elliptic curve over $\mathbb{Q}$, let K be an imaginary quadratic field, and let K_∞ be a $\mathbb{Z}_p$-extension of K. Given a set Σ of primes of K, containing the primes above p, and the primes of bad reduction for E, write K_Σ for the maximal algebraic extension of K which is unramified outside Σ. This paper is devoted to the study of the structure of the cohomology groups $H^i(K_\Sigma/K_\infty, E_{p^\infty})$ for $i = 1, 2$, and of the p-primary Selmer group $\mathrm{Sel}_{p^\infty}(E/K_\infty)$, viewed as discrete modules over the Iwasawa algebra of K_∞/K.

Contents

Manuscrit reçu le 28 octobre 1999.
Partially supported by GNSAGA (C.N.R.), M.U.R.S.T., and European Community.

Introduction

Let E be an elliptic curve defined over a number field K, and let K_∞ be a $\mathbb{Z}_p$-extension of K, where p is a rational prime. Given a set Σ of primes of K, containing the primes above p, the primes of bad reduction for E and the Archimedean primes, write K_Σ for the maximal algebraic extension of K which is unramified outside Σ.

The diophantine properties of E with values in the layers of K_∞ can be encoded in the Galois cohomology groups $H^i(K_\Sigma/K_\infty, E_{p^\infty})$, $i = 1, 2$ and in the p-primary Selmer group $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ of E over K_∞. Denote by Λ the Iwasawa algebra attached to the extension K_∞/K, i.e., the completed group ring $\mathbb{Z}_p[\![\Gamma]\!]$, with $\Gamma := \mathrm{Gal}(K_\infty/K)$. The above groups are equipped with a natural structure of discrete Λ-modules.

This paper is devoted to the study of the Λ-module structure of the above groups, when E is an elliptic curve defined over the rationals and K is an imaginary quadratic field. This setting is particularly rich, as elliptic curves over $\mathbb{Q}$ carry a modular structure, and moreover, when K_∞ is the anticyclotomic $\mathbb{Z}_p$-extension of an imaginary field K, the points of E over the finite subextensions of K_∞ have interesting growth properties, due in certain cases to the presence of systematic families of points.

Let K_n denote the subfield of K_∞ having degree over K equal to p^n. After reviewing in section 1 the definition of Selmer group, we state in section 2 two natural conjectures on the ranks of the Mordell-Weil groups $E(K_n)$. These conjectures are compatible with the Birch and Swinnerton-Dyer conjectures, and with the expected behaviour of the special values of the complex L-series of E/K twisted by finite order complex characters of $\mathrm{Gal}(K_\infty/K)$. Assuming the above conjectures, and using general theorems of Greenberg [8], we show in section 3 a result on the structure of the Λ-module $H^i(K_\Sigma/K_\infty, E_{p^\infty})$, $i = 1, 2$. In section 5, we assume that K_∞ is the anticyclotomic $\mathbb{Z}_p$-extension of K, p is a good ordinary prime for E and there are Heegner points defined over K_∞, satisfying a mild non-vanishing condition [1]. In this setting the Pontryagin dual $\mathcal{X}_\infty$ of the Selmer group $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ has positive Λ-rank, and we can prove the above conjectures. The proof uses results of [1], which provide a partial proof of a Main Conjecture of Iwasawa theory formulated by Perrin-Riou in [14]. We also consider the problem of the existence of non-trivial finite Λ-submodules of $\mathcal{X}_\infty$. If $\mathcal{X}_\infty$ is a torsion Λ-module, this problem is studied by Greenberg in [8]; we review some of his results in section 4. If the Λ-rank of $\mathcal{X}_\infty$ is positive, we study this problem in section 7, working in the setting of section 5, and making use of a duality theorem proved in section 6.

[1] Note Added in Proof: This condition has recently been proved in many cases by Christophe Cornut, *Réduction de Familles de points CM,* PhD thesis, Strasbourg, 2000.

Acknowledgements. We thank Ralph Greenberg for interesting conversations on the topics of this paper.

1. Selmer groups

In this section, let E be an elliptic curve defined over a number field K and let p be a rational prime. Define Σ and K_Σ as in the introduction. The group E_{p^∞} of p-power torsion points of E is naturally a $\mathrm{Gal}(K_\Sigma/K)$-module. Given an extension L of K contained in K_Σ and a prime w of L, write L_w for the compositum of the completions of the finite subextensions L' of L/K at the prime of L' below w. If v is a prime of K, let $L_v := \prod_{w|v} L_w$, the product being taken over the primes of L above v.

For $1 \le m \le \infty$, the p^m*-Selmer group* of E over L is defined by the exactness of the natural sequence

$$0 \to \mathrm{Sel}_{p^m}(E/L) \to H^1(K_\Sigma/L, E_{p^m}) \to \oplus_{v\in\Sigma} H^1(L_v, E)_{p^m},$$

where we extend multiplicatively our functors on local fields with values in the category of Abelian groups. We find directly from the definitions that

$$\mathrm{Sel}_{p^\infty}(E/L) = \varinjlim_{n} \mathrm{Sel}_{p^n}(E/L),$$

the limit being compiled by means of the maps induced by the natural inclusions $E_{p^n} \hookrightarrow E_{p^{n+1}}$.

If L/K is a finite extension, define the *pro-p Selmer group* of E over L to be

$$S_p(E/L) := \varprojlim_{n} \mathrm{Sel}_{p^n}(E/L),$$

where the inverse limit is with respect to the maps induced by $E_{p^{n+1}} \xrightarrow{p} E_{p^n}$. When the p-torsion points $E_p(L)$ of E over L are trivial, then $S_p(E/L)$ is equal to the Tate module $\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \mathrm{Sel}_{p^\infty}(E/L))$ of $\mathrm{Sel}_{p^\infty}(E/L)$; in particular, it is a free $\mathbb{Z}_p$-module. Letting $E(L)_p := E(L) \otimes \mathbb{Z}_p$ denote the p-adic completion of $E(L)$, there is a natural inclusion $E(L)_p \hookrightarrow S_p(E/L)$.

Define K_∞, K_n, Γ and Λ as in the introduction; let $\Gamma_n := \mathrm{Gal}(K_\infty/K_n) = \Gamma^{p^n}$ and $G_n := \mathrm{Gal}(K_n/K) = \Gamma/\Gamma_n$. Given a discrete Λ-module M, we say that M is cofinitely generated, resp. cotorsion, or cofree over Λ if its Pontryagin dual $M^{\mathrm{dual}} = \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ is finitely generated, resp. torsion, or free as a Λ-module.

The inflation-restriction exact sequence gives

$$\mathrm{Sel}_{p^m}(E/K_\infty) = \varinjlim_{n} \mathrm{Sel}_{p^m}(E/K_n),$$

where the direct limit is taken with respect to the natural restriction mappings. One can show that the Pontryagin dual $\mathcal{X}_\infty$ of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ is finitely generated.

Define the Λ-module

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

the limit being taken with respect to the corestriction maps.

Lemma 1.1. *Assume that E has good ordinary reduction at the primes of K (above p) which are ramified in K_∞. Then there is a canonical identification*

$$\hat{S}_p(E/K_\infty) = \mathrm{Hom}_\Lambda(\mathcal{X}_\infty, \Lambda).$$

Proof. See [14, lemme 5, p. 417]. $\square$

It follows that $\hat{S}_p(E/K_\infty)$ is a torsion free Λ-module, having the same rank over Λ as $\mathcal{X}_\infty$.

2. Special values of L-series and Selmer groups

In this section and in the sequel of the paper, let E be an elliptic curve defined over $\mathbb{Q}$ and let K be an imaginary quadratic field. Write Σ for a finite set of *rational* primes including p and the primes of bad reduction for E. (Note that in the definition of the Selmer group for extensions of K no reference to the Archimedean primes is needed.) Let K_∞ stand for a $\mathbb{Z}_p$-extension of K, and retain the notations of the previous section.

Given a finite order character $\chi : \Gamma \to \mathbb{C}^\times$, write $L(E/K, \chi, s)$ for the L-series of E/K twisted by χ. By the fundamental work initiated by Wiles and Taylor, E is known to be modular. Hence, $L(E/K, \chi, s)$ can be continued analytically to the whole complex plane, so that it is defined at $s = 1$.

We review some conjectures on the behaviour of $L(E/K, \chi, 1)$, which, combined with the Birch and Swinnerton-Dyer conjectures, lead to predictions on the rank of the Mordell-Weil groups $E(K_n)$ and on the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/K_n)$. Our purpose is that of motivating certain assumptions that will be made later in the paper.

Recall that the $\mathbb{Z}_p$-extensions of K which are Galois over $\mathbb{Q}$ are the cyclotomic $\mathbb{Z}_p$-extension, which is Abelian over $\mathbb{Q}$, and the anticyclotomic $\mathbb{Z}_p$-extension, whose Galois group over $\mathbb{Q}$ is pro-dihedral. Their composite is the $\mathbb{Z}_p^2$-extension of K, which contains all $\mathbb{Z}_p$-extensions of K.

If K_∞ is different from the anticyclotomic $\mathbb{Z}_p$-extension of K, it is expected that $L(E/K, \chi, 1)$ is non-zero for almost all χ as above. For the cyclotomic $\mathbb{Z}_p$-extension of K, this is proved in Rohlrich's paper [17].

Suppose now that K_∞ is the anticyclotomic $\mathbb{Z}_p$-extension of K. It is convenient to distinguish two cases. We say, following Mazur's terminology, that E is in the *generic case* if either E does not have complex multiplications or the field of complex multiplication of E is different from K. Otherwise, we say that E is in the *exceptional case*.

Let E be in the generic case. For χ an anticyclotomic character, then $L(E/K,\chi,s)$ and $L(E/K,\chi,2-s)$ are related by a functional equation, whose sign is the same for all ramified χ. We call this common sign the *sign of* $(E, K_\infty/K)$. (It can be different from the sign corresponding to unramified characters when p divides the conductor of E.) If the sign of $(E, K_\infty/K)$ is $+1$, resp. -1, it is expected (cf. [11] and [12]) that $L(E/K,\chi,1)$, resp. the first derivative $L'(E/K,\chi,1)$ is non-zero for almost all χ.

We now turn our attention to elliptic curves in the exceptional case. There is a factorization

$$L(E/K,\chi,s) = L(\psi_E,\chi,s) \cdot L(\psi_E\epsilon,\chi,s),$$

where ψ_E is the Grossencharacter attached to $E/\mathbb{Q}$ and ϵ is the quadratic character associated with K. The Hecke L-series appearing in the above factorization satisfy a functional equation relating their values at s and $2-s$. Here, we define the sign of $(E, K_\infty/K)$ to be the common sign of the functional equations of the L-series $L(\psi_E,\chi,s)$, so that the sign of $(E, K_\infty/K)$ determines the parity of one half the order of vanishing of $L(E/K,\chi,s)$. When the sign of $(E, K_\infty/K)$ is $+1$, it is again expected that $L(E/K,\chi,1)$ is non-zero for almost all χ; when the sign of $(E, K_\infty/K)$ is -1, then $L(E/K,\chi,s)$ should vanish to exact order 2 for almost all χ.

By combining the above expectations with the Birch and Swinnerton-Dyer conjectures, one is lead to formulate the following conjecture. See [11, sec. 18] and [12].) Given two functions $f, g : \mathbb{N} \to \mathbb{C}$, we write $f(n) = g(n) + O(1)$ if $|f(n) - g(n)|$ is bounded by a constant independent of n.

Conjecture 2.1. *If K_∞ is a $\mathbb{Z}_p$-extension of the imaginary quadratic field K, there exists an integer $r = r(E, K_\infty/K) \in \{0,1,2\}$ depending on E and K_∞/K such that*

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/K_n) = r \cdot p^n + O(1).$$

Conjecture 2.1 is equivalent to the statement that $\mathrm{rank}_{\mathbb{Z}_p} S_p(E/K_n)$ is equal to $r \cdot p^n + O(1)$. If the p-primary part $\text{Ш}(E/K)_{p^\infty}$ of the Shafarevich-Tate group of E/K is finite for all n, it is also equivalent to the equality of $\mathrm{rank}_{\mathbb{Z}} E(K_n)$ and $r \cdot p^n + O(1)$.

We formulate conjecture 2.1 in the weakest form apt to be assumed as a working hypothesis in the next sections. Following Mazur, we call r the *growth number of* $(E, K_\infty/K)$. The above discussion indicates that r should be 0 or 1 if E is in the generic case, and 0 or 2 if E is in the exceptional case.

Given a rational prime l, let $K_{n,l} := \oplus_{\lambda|l}(K_n)_\lambda$, the sum being extended over the primes of K_n above l. By our conventions, $E(K_{n,l}) =$

$\oplus_{\lambda|l} E((K_n)_\lambda)$ denotes the group of the local points of E at l. Write

$$E(K_{n,l})_p := \lim_{\substack{\leftarrow \\ m}} E(K_{n,l})/p^m E(K_{n,l})$$

for the p-adic completion of $E(K_{n,l})$.

By definition of Selmer group, there are natural maps

$$\rho_{n,l} : S_p(E/K_n) \to E(K_{n,l})_p,$$
$$\tilde{\rho}_{n,l} : \mathrm{Sel}_{p^\infty}(E/K_n) \to \lim_{\substack{\rightarrow \\ m}} E(K_{n,l})/p^m E(K_{n,l}),$$

the direct limit being with respect to the natural maps.
Note that $\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Im}(\rho_{n,l})$ is always equal to $\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Im}(\tilde{\rho}_{n,l})$.

Conjecture 2.2. *We have* $\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Im}(\rho_{n,p}) = r(E, K_\infty/K) \cdot p^n + O(1)$.

Assume that the "weak Leopoldt conjecture"

$$\mathrm{rank}_{\mathbb{Z}_p}\ker(\rho_{n,l}) = O(1)$$

is satisfied. Then conjecture 2.1 and conjecture 2.2 are equivalent. In particular, this is the case when the growth number r is equal to 0.

In section 5 we provide evidence for these conjectures, when K_∞ is the anticyclotomic $\mathbb{Z}_p$-extension and there are Heegner points defined over K_∞. We can show that they follow from a mild non-vanishing assumption on the Heegner points.

3. Descent Iwasawa modules

Using results of Greenberg [8], and assuming the validity of the conjectures 2.1 and 2.2, in this section we prove a result on the structure of the descent Λ-modules $H^i(K_\Sigma/K_\infty, E_{p^\infty})$, $i = 1, 2$. This result holds for all odd primes p, irrespective of whether they are ordinary or supersingular primes for E, or primes of bad reduction. It is an analogue in the current context of the theorems 1 and 2 of [7], which study the case of a modular elliptic curve over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ having analytic rank over $\mathbb{Q}$ at most 1.

Theorem 3.1. *Assume that the conjectures 2.1 and 2.2 hold, and that p is an odd prime. Then:*

1. the discrete Λ-module $H^1(K_\Sigma/K_\infty, E_{p^\infty})$ has corank over Λ equal to 2. Moreover, its Pontryagin dual has no non-zero finite submodule;

2. $H^2(K_\Sigma/K_\infty, E_{p^\infty}) = 0$.

Proof. Greenberg ([8, prop. 3, 4 and 5]) has shown the following:

a. $H^2(K_\Sigma/K_\infty, E_{p^\infty})$ is a cofree Λ-module;

b. if $H^2(K_\Sigma/K_\infty, E_{p^\infty}) = 0$, then the Pontryagin dual of $H^1(K_\Sigma/K_\infty, E_{p^\infty})$ has no non-zero finite submodule;

c. $\mathrm{corank}_\Lambda H^1(K_\Sigma/K_\infty, E_{p^\infty}) - \mathrm{corank}_\Lambda H^2(K_\Sigma/K_\infty, E_{p^\infty}) = 2$.

It follows that part 1 and part 2 of theorem 3.1 are equivalent. Moreover, if $s = s(E, K_\infty/K)$ denotes the Λ-corank of $H^1(K_\Sigma/K_\infty, E_{p^\infty})$, then we have $s \geq 2$.

Recall that $\mathrm{Sel}_{p^\infty}(E/K_n)$ is defined by the exact sequence

$$(1) \quad 0 \to \mathrm{Sel}_{p^\infty}(E/K_n) \to H^1(K_\Sigma/K_n, E_{p^\infty}) \xrightarrow{\delta_n} \oplus_{l\in\Sigma} H^1(K_{n,l}, E)_{p^\infty}.$$

For every rational prime l, the local Tate duality gives a perfect pairing

$$\langle\ ,\ \rangle_l : E(K_{n,l})_p \times H^1(K_{n,l}, E)_{p^\infty} \to \mathbb{Q}_p/\mathbb{Z}_p.$$

By the theory of the formal groups attached to elliptic curves, we find that

$$(2) \quad \mathrm{rank}_{\mathbb{Z}_p} E(K_{n,p})_p = \mathrm{corank}_{\mathbb{Z}_p} H^1(K_{n,p}, E)_{p^\infty} = 2 \cdot p^n,$$

and, for $l \neq p$, $E(K_{n,l})_p$ and $H^1(K_{n,l}, E)_{p^\infty}$ are finite. It follows that

$$(3) \quad \mathrm{rank}_{\mathbb{Z}_p}(\oplus_{l\in\Sigma} E(K_{n,l})_p) = \mathrm{corank}_{\mathbb{Z}_p}(\oplus_{l\in\Sigma} H^1((K_{n,l}, E)_{p^\infty}) = 2 \cdot p^n.$$

The inflation-restriction sequence gives readily

$$0 \to H^1(\Gamma_n, E_{p^\infty}(K_\infty)) \to H^1(K_\Sigma/K_n, E_{p^\infty}) \to H^1(K_\Sigma/K_\infty, E_{p^\infty})^{\Gamma_n} \to 0.$$

From the theory of Λ-modules and the fact that $H^1(\Gamma_n, E_{p^\infty}(K_\infty))$ is finite, we deduce

$$(4) \quad \mathrm{corank}_{\mathbb{Z}_p} H^1(K_\Sigma/K_n, E_{p^\infty}) = s \cdot p^n + O(1).$$

By combining conjecture 2.1 with (1) and (4), we obtain

$$(5) \quad \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Im}(\delta_n) = (s - r) \cdot p^n + O(1).$$

Together with (3), this shows that $s - r \leq 2$. When $r = 0$, this concludes the proof. In general, consider the natural map

$$\rho_n = \oplus_{l\in\Sigma} \rho_{n,l} : S_p(E/K_n) \to \oplus_{l\in\Sigma} E(K_{n,l})_p.$$

By conjecture 2.2 and the above remarks

$$(6) \quad \mathrm{rank}_{\mathbb{Z}_p} \mathrm{Im}(\rho_n) = r \cdot p^n + O(1).$$

The global reciprocity law of class field theory implies that $\mathrm{Im}(\rho_n)$ and $\mathrm{Im}(\delta_n)$ are isotropic under the local Tate pairing

$$\langle\ ,\ \rangle = \oplus_{l\in\Sigma} \langle\ ,\ \rangle_l : \oplus_{l\in\Sigma} E(K_{n,l})_p \times \oplus_{l\in\Sigma} H^1(K_{n,l}, E)_{p^\infty} \to \mathbb{Q}_p/\mathbb{Z}_p.$$

Hence, by (3), (5) and (6), we get

$$r \cdot p^n + (s - r) \cdot p^n + O(1) \leq 2 \cdot p^n.$$

This implies that $s \leq 2$, which, together with the inequality $s \geq 2$ observed before, gives $s = 2$, as was to be shown. □

4. Finite submodules of $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$

It is of interest to formulate conditions under which the quotient

$$\mathcal{X}_\infty = \mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$$

of $H^1(K_\Sigma/K_\infty, E_{p^\infty})^{\mathrm{dual}}$ has no non-trivial finite Λ-submodule. See in particular the applications to the structure of $\mathcal{X}_\infty$ of section 8.

Let $\mathcal{T}$ be the order of the torsion subgroup of $\oplus_{l\in\Sigma-\{p\}}E(K_l)$.

Lemma 4.1. *If $p \nmid \mathcal{T}$, then $\oplus_{l\in\Sigma-\{p\}}H^1(K_{\infty,l}, E)_{p^\infty} = 0$.*

Proof. It is enough to show that $H^1((K_\infty)_\lambda, E_{p^\infty}) = 0$ for all the primes λ of K_∞ above $l \in \Sigma - \{p\}$. By proposition 2 of [8], this holds if $E_{p^\infty}((K_\infty)_\lambda)$ is finite. But $E_{p^\infty}((K_\infty)_\lambda)$ is zero under our assumption on p. $\square$

To simplify the arguments, we assume from now on that p is a prime of good reduction for E. The case where p is an ordinary prime is radically different from the case where p is supersingular. We first consider the latter case.

Lemma 4.2. *If p is a supersingular prime for E, then $H^1(K_{\infty,p}, E)_{p^\infty}$ is equal to zero.*

Proof. By local Tate duality, $H^1(K_{\infty,p}, E)_{p^\infty}$ is the dual of $\lim_{\leftarrow n} E(K_{n,p})_p$, the inverse limit being taken with respect to the corestriction maps. The claim follows from well-known results on the norm mapping for Lubin-Tate formal groups of height 2. See [20]. $\square$

Proposition 4.3. *Let p be a prime of supersingular reduction for E such that $p \nmid 2\mathcal{T}$. Assume that the conjectures 2.1 and 2.2 hold.*
Then, $\mathcal{X}_\infty$ is a Λ-module of rank 2 with no non-trivial finite Λ-submodule.

Proof. By combining lemma 4.1 with lemma 4.2, we see that

$$\oplus_{l\in\Sigma}H^1(K_{\infty,l}, E)_{p^\infty}$$

is zero. By definition, $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ is equal to $H^1(K_\Sigma/K_\infty, E_{p^\infty})$. The result follows from theorem 3.1. $\square$

Remark. Lemma 4.2 shows that if p is supersingular, the Λ-coranks of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ and $H^1(K_\Sigma/K_\infty, E_{p^\infty})$ are equal. Thus, the results of Greenberg recalled in the proof of theorem 3.1 imply that for supersingular primes the Λ-rank of $\mathcal{X}_\infty$ is always at least 2.

We now turn to consider primes p of good ordinary reduction for E. In the remainder of this section, we review an argument of Greenberg ([8, sec. 7]) which shows that if $\mathcal{X}_\infty$ is Λ-torsion, it has no non-trivial finite Λ-submodule for almost all ordinary p (see theorem 4.5 below). This argument does not seem to generalize to the case where the Λ-rank of $\mathcal{X}_\infty$ is positive. This case will be treated in the sections 5, 6 and 7, from a different viewpoint. For a strengthening of theorem 4.5, see Greenberg's forthcoming publications.

The following lemma clarifies the relation between the growth number defined in section 2 and the Λ-rank of $\mathcal{X}_\infty$.

Lemma 4.4. *Let p be a prime of good ordinary reduction for E, and let $r = \mathrm{rank}_\Lambda \mathcal{X}_\infty$. Then we have*

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/K_n) = r \cdot p^n + O(1).$$

Proof. Mazur's "control theorem" ([10, ch. 4]) shows that the natural restriction maps

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

have finite kernel and cokernel, of order bounded independently of n. The lemma follows from the theory of Λ-modules. $\square$

Theorem 4.5 (Greenberg)**.** *Assume that:*

(i) p is a prime of good ordinary reduction for E;

(ii) $p \nmid 6\mathcal{T}$;

(iii) $\mathcal{X}_\infty$ is a torsion Λ-module.

Then $\mathcal{X}_\infty$ has no non-trivial finite Λ-submodule.

Proof. ([8, sec. 7])

Step 1. Since p is ordinary for E, reduction mod p gives rise to an exact sequence

$$0 \to F^1E_{p^\infty} \to E_{p^\infty} \to E_{p^\infty}/F^1E_{p^\infty} \to 0 \tag{7}$$

of modules over $G_{K_p} := \mathrm{Gal}(\bar{K}_p/K_p)$, such that the inertia group $I_p \subset G_{K_p}$ at p acts trivially on $E_{p^\infty}/F^1E_{p^\infty}$ and via the cyclotomic character χ_p on $F^1E_{p^\infty}$. By [8, sec. 2] and by lemma 4.1, the Selmer group of E over K_∞ can be defined by the exact sequence

(8)

$$0 \to \mathrm{Sel}_{p^\infty}(E/K_\infty) \to H^1(K_\Sigma/K_\infty, E_{p^\infty}) \to H^1(K_{\infty,p}, E_{p^\infty}/F^1E_{p^\infty}),$$

where the last map is induced by (7). Let

$$(E_{p^\infty}/F^1E_{p^\infty})^\vee := \mathrm{Hom}_{\mathbb{Z}_p}(E_{p^\infty}/F^1E_{p^\infty}, \mu_{p^\infty}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

denote the Cartier dual of $E_{p^\infty}/F^1E_{p^\infty}$. By our assumptions on p, we have that $((E_{p^\infty}/F^1E_{p^\infty})^\vee)^{I_p}$ is zero, and hence $(E_{p^\infty}/F^1E_{p^\infty})^\vee(K_p)$ is also zero. Then [8, prop. 1 and its corollary 2] shows that the Λ-module $H^1(K_{\infty,p}, E_{p^\infty}/F^1E_{p^\infty})$ is cofree of corank 2.

Step 2. Since by our assumptions $\mathcal{X}_\infty$ is Λ-torsion, lemma 4.4 implies directly that the conjectures 2.1 and 2.2 hold with $r = 0$. By theorem 3.1, $H^1(K_\Sigma/K_\infty, E_{p^\infty})^{\mathrm{dual}}$ has Λ-rank equal to 2 and has no non-trivial finite Λ-submodule.

Step 3. By dualizing the sequence (8), we find

$$(9)\quad 0 \to H^1(K_{\infty,p}, E_{p^\infty}/F^1E_{p^\infty})^{\mathrm{dual}} \to H^1(K_\Sigma/K_\infty, E_{p^\infty})^{\mathrm{dual}} \to \mathcal{X}_\infty \to 0,$$

where the injectivity of the first map follows from the fact that $\mathcal{X}_\infty$ is Λ-torsion and $H^1(K_{\infty,p}, E_{p^\infty}/F^1E_{p^\infty})^{\mathrm{dual}}$ is free of the same rank as

$$H^1(K_\Sigma/K_\infty, E_{p^\infty})^{\mathrm{dual}}.$$

Let $\tilde{C}$ be the preimage in $H^1(K_\Sigma/K_\infty, E_{p^\infty})^{\mathrm{dual}}$ of a finite Λ-submodule C of $\mathcal{X}_\infty$. By Step 1 and Step 2, $\tilde{C}$ is Λ-torsion free. Hence the theory of Λ-modules shows that $\tilde{C}$ must inject in a free Λ-module of rank 2, with finite cokernel. But this is possible only if $C = 0$. $\square$

Remarks.

1. If the Λ-rank of $\mathcal{X}_\infty$ is positive, then the first map of the sequence (9) is no longer injective, and the argument above cannot be performed (as one sees from easy examples). A natural situation where the rank of $\mathcal{X}_\infty$ is positive arises because of the presence of Heegner points defined over the layers of the anticyclotomic $\mathbb{Z}_p$-extension K_∞ of K. In the sections 5, 6 and 8 we study the structure of the Iwasawa modules $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ and $H^1(K_\Sigma/K_\infty, E_{p^\infty})$ in this case, and in particular the existence of non-trivial finite Λ-submodules of $\mathcal{X}_\infty$.
2. Assume that E is in the generic case and that p is a prime of good ordinary reduction for E. Conjecturally, the rank of $\mathcal{X}_\infty$ is positive if and only if K_∞ is the anticyclotomic $\mathbb{Z}_p$-extension of K and there exist Heegner points defined over K_∞. For, the conjectures of section 2 combined with lemma 4.4 predict that the the rank of $\mathcal{X}_\infty$ is positive when K_∞ is anticyclotomic and the sign of $(E, K_\infty/K)$ is -1. If E is modular, this is precisely the assumption that guarantees the existence of Heegner points (see the next section).

5. Growth numbers and Heegner points

We have observed that if $\mathcal{X}_\infty$ is a torsion Λ-module, then the conjectures 2.1 and 2.2 are verified, with $r = 0$. In this section, let K_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K and p be a prime of good ordinary reduction for E (subject to certain technical conditions). Assuming the existence of Heegner points defined over K_∞ satisfying a mild non-triviality assumption, we show that the conjectures 2.1 and 2.2 hold, with $r = 1$. In particular, we may apply theorem 3.1 in this setting.

Let K be such that $\mathrm{disc}(K)$ is prime to the conductor N of E. In order to ensure the existence of Heegner points on E defined over the layers of K_∞, we make the following assumption.

Assumption A.
The L-series $L(E/K, s)$ vanishes to odd order at $s = 1$.

The above assumption implies that E is in the generic case. The condition on $L(E/K, s)$ is equivalent to $\epsilon(N) = 1$, where recall that ϵ denotes the Dirichlet character attached to K. It follows that for all finite order characters χ of Γ the L-series $L(E/K, \chi, s)$ vanishes to odd order at $s = 1$.

Under assumption A, we can construct Heegner points defined over the layers of K_∞ coming from a Shimura curve parametrization $X \to E$ of E, the definition of the curve X depending on which prime factors of N are split or inert in K. In the case when all the primes dividing N are split in K, X is the modular curve $X_0(N)$. See [5] for more details.

The extension K_n is contained in a ring class field $K[p^{k_n}]$ of conductor p^{k_n}. Assume that k_n is minimal. (For example, if p does not divide the class group of K, $k_n = n+1$.) For all n we may define a Heegner point $\alpha_n \in E(K_n)$ by tracing from $K[p^{k_n}]$ down to K_n a Heegner point in $E(K[p^{k_n}])$. By viewing α_n as a point of $E(K_n)_p = E(K_n) \otimes \mathbb{Z}_p$, define the submodule

$$\mathcal{E}(E/K_n)_p := \mathbb{Z}_p[G_n]\alpha_n$$

of $E(K_n)_p$, generated by the G_n-orbit of α_n. The module $\mathcal{E}(E/K_n)_p$ does not depend on the choice of the Heegner point α_n, but does depend on the choice of modular parametrization. Let a_p denote the Fourier coefficient $1 + p - \#E(\mathbb{F}_p)$. In order to be able to apply directly the results of [1], we impose the same assumptions as in [1], with the exception that we do not require that the Heegner points α_n come necessarily from a parametrization of E by the modular curve $X_0(N)$. Since the formal properties of the α_n are the same in all cases (see [5]), the arguments of [1] go through unchanged and the results contained there hold in our more general setting. (Some of the other assumptions could also be weakened somewhat.)

Assumption B.

(1) The imaginary quadratic field K is such that $\mathrm{disc}(K)$ is prime to N and $\mathcal{O}_K^\times = \{\pm 1\}$.

(2) $p \nmid 6N\mathrm{disc}(K)\#\mathrm{Pic}(\mathcal{O}_K)\#(E/E^0)$, where E/E^0 denotes the group of connected components of the Néron model of E over $\mathrm{Spec}(\mathcal{O}_K)$.

(3) The Galois representation $\rho_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E_{p^\infty})$ is surjective.

(4) $a_p \not\equiv 0, 1, 2 \pmod{p}$ if p splits in K, and $a_p \not\equiv 0, 1, -1 \pmod{p}$ if p is inert in K.

Fixing E and K, assumption B holds for a set of primes p of density 1: see [1, §2.2] for more details. In the sequel of this section, we will tacitly work under the assumptions A and B.

Lemma 5.1. *For all n, corestriction induces surjective maps*

$$\mathrm{cores}_{K_{n+1}/K_n}: \mathcal{E}(E/K_{n+1})_p \to \mathcal{E}(E/K_n)_p.$$

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

Proof. See [1, §2.1, prop. 4] (based on computations contained in [14]). □

Define the *Iwasawa module of the Heegner points* to be

$$\hat{\mathcal{E}}(E/K_\infty)_p := \lim_{\substack{\leftarrow \\ n}} \mathcal{E}(E/K_n)_p,$$

where the inverse limit is taken with respect to the corestriction maps. The module $\hat{\mathcal{E}}(E/K_\infty)_p$ is cyclic over Λ. Moreover, it injects naturally in $\hat{S}_p(E/K_\infty)$ (the latter module being defined in section 1). Since the Λ-module $\hat{S}_p(E/K_\infty)$ is torsion-free by lemma 1.1, we conclude that either $\hat{\mathcal{E}}(E/K_\infty)_p$ is isomorphic to Λ or it is zero. One checks that $\hat{\mathcal{E}}(E/K_\infty)_p$ is non-zero if and only if α_n has infinite order for some n. (See [1, §2.1] for details.)

Remark. By modifying the definition of the $\mathcal{E}(E/K_n)_p$ as in [14], it is possible to define an Iwasawa module of Heegner points enjoying the same properties of $\hat{\mathcal{E}}(E/K_\infty)_p$ under weaker assumptions than the ones above. For simplicity, we do not pursue this here.

Define the Λ-module

$$\hat{E}(K_{\infty,p})_p := \lim_{\substack{\leftarrow \\ n}} E(K_{n,p})_p,$$

the inverse limit being taken with respect to the the corectriction maps.

Proposition 5.2. *1. The Λ-module $\hat{E}(K_{\infty,p})_p$ is free of rank 2.*

2. The natural maps

$$(\hat{E}(K_{\infty,p})_p)_{\Gamma_n} \to E(K_{n,p})_p$$

are isomorphisms. (Thus, by part 1, $E(K_{n,p})_p$ is isomorphic to $\mathbb{Z}_p[G_n]^2$.)

Proof. Part 1. By the local Tate duality, $\hat{E}(K_{\infty,p})_p$ is identified with the Pontryagin dual of $H^1(K_{\infty,p}, E)_{p^\infty}$. Consider the local descent exact sequence

$$0 \to E(K_{\infty,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(K_{\infty,p}, E_{p^\infty}) \to H^1(K_{\infty,p}, E)_{p^\infty} \to 0.$$

Let $\mathbb{F}_{K_p}$ denote the residue algebra of K_p. Assumption B implies that $E_p(\mathbb{F}_{K_p})$ is zero. Then the sequence (1) of section 4 induces the exact sequence

$$0 \to H^1(K_{\infty,p}, F^1E_{p^\infty}) \to H^1(K_{\infty,p}, E_{p^\infty}) \to H^1(K_{\infty,p}, E_{p^\infty}/F^1E_{p^\infty}) \to 0.$$

This sequence ends with a zero since $G_{K_{\infty,p}}$ has p-cohomological dimension 1 (see [21]). The results of [6] show that the image of $H^1(K_{\infty,p}, F^1E_{p^\infty})$ in $H^1(K_{\infty,p}, E_{p^\infty})$ equals the image of $E(K_{\infty,p})\otimes\mathbb{Q}_p/\mathbb{Z}_p$ in $H^1(K_{\infty,p}, E_{p^\infty})$. It follows that $H^1(K_{\infty,p}, E)_{p^\infty}$ is identified with $H^1(K_{\infty,p}, E_{p^\infty}/F^1E_{p^\infty})$. Since $(E_{p^\infty}/F^1E_{p^\infty})^\vee(K_p)$ is zero under our assumptions, we also have that $(E_{p^\infty}/F^1E_{p^\infty})^\vee(K_{\infty,p})$ is zero. Then [8, proposition 1 and its corollary 2] implies that $H^1(K_{\infty,p}, E)_{p^\infty}$ is Λ-cofree of rank 2. This concludes the proof of part 1.

Part 2. Under our assumptions, the results of [10, ch. 4] show that the corestriction maps

$$\mathrm{cores}_{K_{n+1,p}/K_{n,p}} : E(K_{n+1,p})_p \to E(K_{n,p})_p$$

are surjective. Therefore, the natural maps $(\hat{E}(K_{\infty,p})_p)_{\Gamma_n} \to E(K_{n,p})_p$ are also surjective. By part 1, $(\hat{E}(K_{\infty,p})_p)_{\Gamma_n}$ is isomorphic to $\mathbb{Z}_p[G_n]^2$; in particular, it has $\mathbb{Z}_p$-rank equal to $2p^n$. Since the $\mathbb{Z}_p$-rank of $E(K_{n,p})_p$ is equal to $2p^n$ by the theory of formal groups, we conclude that $(\hat{E}(K_{\infty,p})_p)_{\Gamma_n} \to E(K_{n,p})_p$ is an isomorphism. □

Theorem 5.3. *Assume that $\hat{\mathcal{E}}(E/K_\infty)_p$ is non-zero. Then the conjectures 2.1 and 2.2 hold, with $r(E, K_\infty/K) = 1$.*

Proof. Part 1
Under our assumptions, the results of [1, §3.1] show that the Λ-rank of $\mathcal{X}_\infty$ is equal to 1. Lemma 4.4 implies that conjecture 2.1 holds with $r(E, K_\infty/K) = 1$.

Part 2

Step 1. Consider the natural localization maps

$$\sigma_{n,p} : \mathcal{E}(E/K_n)_p \to E(K_{n,p})_p.$$

By taking the inverse limit with respect to the corestriction mappings, we obtain a map

$$\sigma_{\infty,p} : \hat{\mathcal{E}}(E/K_\infty)_p \to \hat{E}(K_{\infty,p})_p.$$

By our assumptions, $\hat{\mathcal{E}}(E/K_\infty)_p$ is a free Λ-module of rank 1. By proposition 5.2, $\hat{E}(K_{\infty,p})_p$ is torsion-free. Hence $\sigma_{\infty,p}$ is injective if and only if it is non-zero. This is equivalent to saying that $\sigma_{n,p}$ is non-zero for some n. But we know that α_n has infinite order for some n, and hence $\sigma_{n,p}(\alpha_n)$ is non-zero. In conclusion, $\sigma_{\infty,p}$ is injective.

Step 2. By fixing isomorphisms $\hat{\mathcal{E}}(E/K_\infty)_p \simeq \Lambda$ and $\hat{E}(K_{\infty,p})_p \simeq \Lambda^2$, $\sigma_{\infty,p}$ is identified with an embedding

$$\sigma_{\infty,p} : \Lambda \hookrightarrow \Lambda^2.$$

Let $\sigma_{\infty,p}(1) = (f,g)$, where $f = (f_n)_{n\geq 1}$ and $g = (g_n)_{n\geq 1}$, with $f_n, g_n \in \mathbb{Z}_p[G_n]$. By proposition 5.2, the image of $\sigma_{n,p}$ is identified with $\mathbb{Z}_p[G_n](f_n, g_n)$. Hence, by the theory of Λ-modules, we find

$$\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Im}(\sigma_{n,p}) = p^n + O(1).$$

Step 3. Since $\sigma_{n,p}$ is the restriction to $\mathcal{E}(E/K_n)_p$ of the map

$$\rho_{n,p} : S_p(E/K_n) \to E(K_{n,p})_p,$$

the above equality gives

$$\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Im}(\rho_{n,p}) \geq p^n + O(1).$$

The claim follows from part 1, since $\mathrm{rank}_{\mathbb{Z}_p} S_p(E/K_n) \geq \mathrm{rank}_{\mathbb{Z}_p}\mathrm{Im}(\rho_{n,p})$. $\square$

Remark. As we have observed in section 2, in our setting $L'(E/K,\chi,1)$ is conjectured to be non-zero for all but finitely many finite order characters χ of Γ. A natural generalization of the Gross-Zagier formula states that $L'(E/K,\chi,1)$ is equal to the canonical height of the χ-component of the Heegner point α_n, up to a non-zero constant. This would imply that for n large enough α_n has infinite order. Thus, it is natural to conjecture that $\hat{\mathcal{E}}(E/K_\infty)_p$ is always non-zero: see [11, sec. 19].

By combining theorem 3.1 with theorem 5.3, we obtain the following.

Theorem 5.4. *Assume that $\hat{\mathcal{E}}(E/K_\infty)_p$ is non-zero.*

1. The discrete Λ-module $H^1(K_\Sigma/K_\infty, E_{p^\infty})$ has corank over Λ equal to 2. Moreover, its Pontryagin dual has no non-zero finite submodule.

2. $H^2(K_\Sigma/K_\infty, E_{p^\infty}) = 0$.

Remark. Proposition 5.2 and theorem 5.3 may be viewed as analogues in our setting of the results of Iwasawa on the structure of the modules of the local units and the cyclotomic units over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. (See for example [9].)

6. A duality theorem

In this section, we prove a general duality theorem which will be used in the next section to study the existence of finite submodules of $\mathcal{X}_\infty$, in the case of the anticyclotomic $\mathbb{Z}_p$-extension of K. Here, K will be a number field and K_∞ an arbitrary $\mathbb{Z}_p$-extension of K. We make the following assumptions on $(E, p, K_\infty/K)$.

1. $p \nmid 2\#(E/E^0)$, where E/E^0 denotes the group of connected components of the Néron model of E over the ring of integers of K.

2. E has good reduction above p.

3. The Galois representation $\rho_p : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(E_p)$ contains a Cartan subgroup of $\mathrm{Aut}(E_p) \simeq \mathrm{GL}_2(\mathbb{F}_p)$.
4. The local norm mappings $N_v : E(K_{n,v}) \to E(K_v)$ are surjective for all primes v of K.

Remark. In the case when E is an elliptic curve defined over the rationals and K is an imaginary quadratic field, one checks by using the results of [10, ch. 4] that these assumptions follow from the assumption B of the previous section. By condition 3, $E_p(K)$ is zero, and hence $E_p(K_\infty)$ is also zero. Condition 4 implies that E has ordinary reduction at all the primes of K which are ramified in K_∞ ([10, ch. 4]).

Define the *universal norm submodule* of $S_p(E/K)$ to be

$$US_p(E/K) = \bigcap_n \mathrm{cores}_{K_n/K} S_p(E/K_n).$$

Theorem 6.1. *Under the above assumptions, there exists a perfect canonical pairing*

$$\langle\!\langle\ ,\ \rangle\!\rangle : S_p(E/K)/US_p(E/K) \times \mathrm{Sel}_{p^\infty}(E/K_\infty)_\Gamma \to \Gamma \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p.$$

Remark. The existence of a pairing like the one above, having finite right radical, is often used to define the p-adic height pairing on $S_p(E/K)$ attached to K_∞. See [18], [19] and [15]. For our purposes, we need that the pairing $\langle\!\langle\ ,\ \rangle\!\rangle$ is perfect, not just up to quasi-isomorphisms. The proof uses theorem 3.2 of [4].

We study the existence of finite submodules of $\mathcal{X}_\infty$ by means of the following corollary.

Corollary 6.2. *$\mathcal{X}_\infty$ has no non-trivial finite Λ-submodule if and only if $S_p(E/K)/US_p(E/K)$ has no torsion.*

Proof. Theorem 6.1 gives an identification of $S_p(E/K)/US_p(E/K)$ with $\mathcal{X}_\infty^\Gamma$. If M is a non-trivial finite Λ-submodule of $\mathcal{X}_\infty$, then M^Γ is a non-trivial finite submodule of $\mathcal{X}_\infty^\Gamma$. Conversely, if the torsion subgroup of $S_p(E/K)/US_p(E/K)$ is non-trivial, the corresponding finite submodule of $\mathcal{X}_\infty^\Gamma$ is a non-trivial finite Λ-submodule of $\mathcal{X}_\infty$ (such that the action of Λ factors through $\Lambda/(\gamma-1)\Lambda = \mathbb{Z}_p$). $\square$

If $\mathcal{X}_\infty$ is a torsion Λ-module, so that $US_p(E/K)$ is zero, corollary 6.2 gives under the current more restrictive assumptions a new proof of the result of Greenberg recalled in section 4. Our goal is to apply the above corollary to an elliptic curve defined over the rationals with values in the anticyclotomic $\mathbb{Z}_p$-extension K_∞ of an imaginary quadratic field, in the case when $\mathcal{X}_\infty$ has positive Λ-rank due to the presence of Heegner points over the layers of K_∞.

Proof of theorem 6.1. It follows by combining the following results.

Fix positive integers m and n. To ease notation in the next lemma, let $H := K_n$ and $G := G_n$. Denote by I the augmentation ideal of the group ring $\mathbb{Z}/p^m\mathbb{Z}[G]$. Thus, we have a canonical identification $G/G^{p^m} = I/I^2$.

Proposition 6.3. *There is perfect canonical pairing of Tate cohomology groups*

$$\langle\ ,\ \rangle_{H,m} : \hat{H}^0(G, \mathrm{Sel}_{p^m}(E/H)) \times \hat{H}^{-1}(G, \mathrm{Sel}_{p^m}(E/H)) \to I/I^2.$$

Proof. Under our assumptions, the Hochschild-Serre spectral sequence can be used to show that the restriction map induces an isomorphism between $\mathrm{Sel}_{p^m}(E/K)$ and $\mathrm{Sel}_{p^m}(E/H)^G$ (see for example [1, §2.3]). In particular, we may identify $\mathrm{Sel}_{p^m}(E/K)$ with a submodule of $\mathrm{Sel}_{p^m}(E/H)$.

Write $\mathrm{cores}_{H/K}\mathrm{Sel}_{p^m}(E/H)$, resp. $\mathrm{Sel}_{p^m}(E/H)^0$ for the image, resp. the kernel of the corestriction map $\mathrm{cores}_{H/K} : \mathrm{Sel}_{p^m}(E/H) \to \mathrm{Sel}_{p^m}(E/K)$. Thus, the group $\hat{H}^0(G, \mathrm{Sel}_{p^m}(E/H))$, resp. $\hat{H}^{-1}(G, \mathrm{Sel}_{p^m}(E/H))$ is equal by definition to

$$\mathrm{Sel}_{p^m}(E/K)/\mathrm{cores}_{H/K}\mathrm{Sel}_{p^m}(E/H), \text{ resp. } \mathrm{Sel}_{p^m}(E/H)^0/(\gamma-1)\mathrm{Sel}_{p^m}(E/H).$$

Let γ be a generator for G. By [4, theorem 3.2], given $y \in \mathrm{Sel}_{p^m}(E/H)^0$ there exists $z \in H^1(H, E_{p^m})$ such that $y = (\gamma - 1)z$.

If v is a prime of K, we write $\bar{z}_v$ for the natural image of z in $H^1(H_v, E)_{p^m}$. Clearly, $\bar{z}_v$ belongs to $H^1(H_v, E)_{p^m}^G$. By the assumption 4, an argument based on the Hochschild-Serre spectral sequence shows that restriction gives an isomorphism between $H^1(K_v, E)_{p^m}$ and $H^1(H_v, E)_{p^m}^G$. It follows that we may identify $\bar{z}_v$ with an element of $H^1(K_v, E)_{p^m}$. Write

$$[\ ,\ ]_v : E(K_v)/p^m E(K_v) \times H^1(K_v, E)_{p^m} \to \mathbb{Z}/p^m\mathbb{Z}$$

for the local Tate pairing ([13, ch. 1]). We define a pairing

$$[\ ,\ ]_H : \mathrm{Sel}_{p^m}(E/K) \times \mathrm{Sel}_{p^m}(E/H)^0 \to I/I^2$$

by letting

$$[x, y]_H = \sum_v [x_v, \bar{z}_v]_v \cdot (\gamma - 1) \pmod{I^2},$$

where x_v denotes the natural image of x in $E(K_v)/p^m E(K_v)$ and the sum runs over all primes of K. Observe that the pairing $[\ ,\ ]_H$ is well defined. For, if $(\gamma - 1)z = (\gamma - 1)u$ for elements u and z in $H^1(H, E_{p^m})$, then $z - u$ belongs to $H^1(H, E_{p^m})^G$. Since $E_p(H)$ is zero, the restriction map induces an isomorphism of $H^1(K, E_{p^m})$ onto $H^1(H, E_{p^m})^G$. Thus, we may regard $z - u$ as an element in $H^1(K, E_{p^m})$. The global duality theorem of class field theory ([13, lemma 6.15, p. 105]) gives $\sum_v [x_v, \bar{z}_v - \bar{u}_v]_v = 0$. Moreover, $[\ ,\ ]_H$ does not depend on the choice of the generator γ.

Observe that y belongs to the right kernel of $[\ ,\ ]_H$ if and only if there exists $u \in H^1(K, E_{p^m})$ such that $z - u$ belongs to $\mathrm{Sel}_{p^m}(E/H)$ ([13, lemma 6.15, p. 105]). This is equivalent to saying that y belongs to $(\gamma - 1)\mathrm{Sel}_{p^m}(E/H)$.

Now, assume that x is equal to $\mathrm{cores}_{H/K}(\tilde{x})$, with $\tilde{x} \in \mathrm{Sel}_{p^m}(E/H)$. Then $[x, y]_H = 0$ for all y in $\mathrm{Sel}_{p^m}(E/H)$. For, the global duality theorem gives

$$\sum_v [x_v, \bar{z}_v]_v = \sum_w [\tilde{x}_w, \bar{z}_w]_w = 0,$$

where the second sum is over all the primes w of H, we let $[\ ,\ ]_w$ stand for the local Tate pairing relative to H_w and we write $\bar{z}_w$ for the image of z in $H^1(H_w, E)_{p^m}$.

Thus far we have proved that $[\ ,\ ]_H$ induces a right non-degenerate pairing

$$\langle\ ,\ \rangle_{H,m} : \hat{H}^0(G, \mathrm{Sel}_{p^m}(E/H)) \times \hat{H}^{-1}(G, \mathrm{Sel}_{p^m}(E/H)) \to I/I^2.$$

But the groups $\hat{H}^0(G, \mathrm{Sel}_{p^m}(E/H))$ and $\hat{H}^{-1}(G, \mathrm{Sel}_{p^m}(E/H))$ have the same order, since G is cyclic and $\mathrm{Sel}_{p^m}(E/H)$ is finite. Hence, $\langle\ ,\ \rangle_{H,m}$ is non-degenerate. This concludes the proof of proposition 6.3. $\square$

We shall define the duality of theorem 1 by compiling a limit of the pairings defined in proposition 6.3. We begin with a compatibility property. For $m \le m'$, $n \le n'$, let

$$\mathrm{res} = \mathrm{res}_{m,n}^{m',n'} : \mathrm{Sel}_{p^m}(E/K_n) \to \mathrm{Sel}_{p^{m'}}(E/K_{n'})$$

be defined by composing the restriction map with the map induced by the inclusion $E_{p^n} \subset E_{p^{n'}}$. Under our assumptions, the map res gives an isomorphism ([1, §2.3])

$$\mathrm{Sel}_{p^m}(E/K_n) \xrightarrow{\sim} \mathrm{Sel}_{p^{m'}}(E/K_{n'})[p^m]^{\mathrm{Gal}(K_{n'}/K_n)}\ .$$

By abusing notation somewhat, we also write res for the induced map

$$\mathrm{res} : \hat{H}^{-1}(G_n, \mathrm{Sel}_{p^m}(E/K_n)) \to \hat{H}^{-1}(G_{n'}, \mathrm{Sel}_{p^{m'}}(E/K_{n'})).$$

Let

$$m_p = m_p^{m,m'} : \mathrm{Sel}_{p^{m'}}(E/K) \to \mathrm{Sel}_{p^m}(E/K)$$

be the map induced by $E_{p^{m'}} \xrightarrow{p^{m'-m}} E_{p^m}$. Since $m_p(\mathrm{cores}_{K_{n'}/K}\mathrm{Sel}_{p^{m'}}(E/K_{n'}))$ is contained in $\mathrm{cores}_{K_n/K}\mathrm{Sel}_{p^m}(E/K_n)$ we obtain a map, still denoted by m_p,

$$m_p : \hat{H}^0(G_{n'}, \mathrm{Sel}_{p^{m'}}(E/K_{n'})) \to \hat{H}^0(G_n, \mathrm{Sel}_{p^m}(E/K_n)).$$

Write $I_{m,n}$ for the augmentation ideal of $\mathbb{Z}/p^m\mathbb{Z}[G_n]$. Let $i = i_{n,n'} : G_n \hookrightarrow G_{n'}$ be the canonical injection defined by $i(g) = \tilde{g}^{p^{n'-n}}$, where $\tilde{g}$ is any lift of g to $G_{n'}$ with respect to the natural projection $G_{n'} \to G_n$. The map i induces a canonical map $j = j_{m,n}^{m',n'} : I_{m,n}/I_{m,n}^2 \to I_{m',n'}/I_{m',n'}^2$.

Lemma 6.4. *We have*

$$\langle x, \operatorname{res}(y)\rangle_{K_{n'},m'} = j\langle m_p x, y\rangle_{K_n,m},$$

for any given $x \in \hat{H}^0(G_{n'}, \mathrm{Sel}_{p^{m'}}(E/K_{n'}))$ *and* $y \in \hat{H}^{-1}(G_n, \mathrm{Sel}_{p^m}(E/K_n))$.

Proof. It follows directly from the definition of our pairings. □

Lemma 6.5. *We have*

$$\varinjlim_{n} \varinjlim_{m} \hat{H}^{-1}(G_n, \mathrm{Sel}_{p^m}(E/K_n)) = \mathrm{Sel}_{p^\infty}(E/K_\infty)_\Gamma,$$

where the limit is taken with respect to the maps res.

Proof. Note that $\mathrm{Sel}_{p^m}(E/K_n)$ injects via restriction into $\mathrm{Sel}_{p^m}(E/K_{n+m})^0$. Thus,

$$\varinjlim_{n} \varinjlim_{m} \mathrm{Sel}_{p^m}(E/K_n)^0 = \mathrm{Sel}_{p^\infty}(E/K_\infty).$$

Let γ be a topological generator of Γ. The claim follows by taking the direct limit of the short exact sequences

$$0 \to \mathrm{Sel}_{p^m}(E/K_n) \xrightarrow{\gamma-1} \mathrm{Sel}_{p^m}(E/K_n)^0 \to \hat{H}^{-1}(G_n, \mathrm{Sel}_{p^m}(E/K_n)) \to 0.$$

□

Lemma 6.6. *We have*

$$\varprojlim_{n} \varprojlim_{m} \hat{H}^0(G_n, \mathrm{Sel}_{p^m}(E/K_n)) = S_p(E/K)/US_p(E/K),$$

the limit being taken with respect to the maps m_p.

Proof. We start by showing that

$$\varprojlim_{n} \varprojlim_{m} \mathrm{cores}_{K_n/K} \mathrm{Sel}_{p^m}(E/K_n) = US_p(E/K).$$

First, we see that

$$\varprojlim_{m} \mathrm{cores}_{K_n/K} \mathrm{Sel}_{p^m}(E/K_n) = \mathrm{cores}_{K_n/K} S_p(E/K_n).$$

This follows from taking the inverse limit of the maps

$$\mathrm{Sel}_{p^m}(E/K_n) \overset{N_{K_n/K}}{\twoheadrightarrow} \mathrm{cores}_{K_n/K} \mathrm{Sel}_{p^m}(E/K_n) \hookrightarrow \mathrm{Sel}_{p^m}(E/K),$$

where $N_{K_n/K}$ denotes multiplication by $\sum_{g\in G_n} g \in \mathbb{Z}_p[G_n]$. (Note that we are working with finite modules, hence the inverse limit is an exact functor.) Moreover, we have the equality

$$\varprojlim_n \mathrm{cores}_{K_n/K} S_p(E/K_n) = \bigcap_n \mathrm{cores}_{K_n/K} \mathrm{Sel}_{p^n}(E/K_n) = US_p(E/K).$$

Now take $\varprojlim_m$ of the short exact sequence

$$0 \to \mathrm{cores}_{K_n/K} \mathrm{Sel}_{p^m}(E/K_n) \to \mathrm{Sel}_{p^m}(E/K) \to \hat{H}^0(G_n, \mathrm{Sel}_{p^m}(E/K_n)) \to 0.$$

We find

$$0 \to \mathrm{cores}_{K_n/K} S_p(E/K_n) \to S_p(E/K) \to \varprojlim_m \hat{H}^0(G_n, \mathrm{Sel}_{p^m}(E/K_n)) \to 0.$$

Although the modules in the above sequence are not finite, a simple topological argument (see the sublemma 6.7 below), based on the completeness of $S_p(E/K)$ in the p-adic topology, shows that $\varprojlim_n$ is exact on the above sequences, thereby proving lemma 6.6. □

Sublemma 6.7. *Let X be a finitely generated $\mathbb{Z}_p$-module. Let X_n, $n \geq 1$ be a sequence of $\mathbb{Z}_p$-submodules of X such that $X_n \supset X_{n+1}$ for all n. Then*

$$\varprojlim_n X/X_n = X/\bigcap_n X_n,$$

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

Proof. Write X_∞ for $\bigcap_n X_n$, and let Y, resp. Y_n stand for X/X_∞, resp. X_n/X_∞. Hence, $\bigcap_n Y_n = (0)$. Our claim is equivalent to showing that the inverse limit of the Y_n with respect to the natural projections is equal to Y. Note that the $\mathbb{Z}_p$-rank of Y_n is constant for all n greater than a positive integer n_0. By the theory of elementary divisors, we may write $Y = Z \oplus W$, where Z contains with finite index Y_n if $n > n_0$. We have

$$\varprojlim_n Y/Y_n = (\varprojlim_{n>n_0} Z/Y_n) \oplus W.$$

Since Z is complete in the p-adic topology and the Y_n are a basis of neighbourhoods of the identity of Z, we conclude that $\varprojlim_n Z/Y_n = Z$. This proves the sublemma. □

Theorem 1 is proved by combining the results 6.3-6.6, since the direct limit of $I_{m,n}/I_{m,n}^2$ with respect to the maps j is naturally identified with $\Gamma \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$.

7. On the structure of $\mathrm{Sel}_{p^\infty}(E/K_\infty)^{\mathrm{dual}}$

We return to the study of elliptic curves defined over the rationals, with values in a $\mathbb{Z}_p$-extension of an imaginary quadratic field. In section 4, we reviewed results of Greenberg which show that $\mathcal{X}_\infty$ has no non-trivial finite Λ-submodule, if p is a prime of good ordinary reduction for E and $\mathcal{X}_\infty$ is a torsion Λ-module. In this section, we consider the case where the Λ-module $\mathcal{X}_\infty$ has positive rank and p is an ordinary prime. (If E has supersingular reduction at p, we have seen in section 4 (proposition 4.3) that $\mathcal{X}_\infty$ is essentially equal to the Pontryagin dual of $H^1(K_\Sigma/K_\infty, E_{p^\infty})$, and we may apply theorem 3.1 to understand its structure.)

In view of the conjectures of section 2, if we exclude curves in the exceptional case $\mathcal{X}_\infty$ can have positive Λ-rank only when K_∞ is the anticyclotomic $\mathbb{Z}_p$-extension of K and there are Heegner points defined over the layers of K_∞. Therefore, it is natural to place ourselves in the setting of section 5, under the assumptions A and B made there.

The main result of this section (theorem 7.1) gives a sufficient condition ensuring that $\mathcal{X}_\infty$ does not have non-trivial finite Λ-submodules. As an application (theorem 7.2), we obtain a strengthening of the main result of [1].

Let $\mathcal{E}_n$ denote the natural image of the module of Heegner points $\mathcal{E}(E/K_n)_p$ in $E(K_n)/pE(K_n)$, and let $\text{Ш}(E/K_n)$ be the Shafarevich-Tate group of E/K_n. Define $\text{Ш}(E, K_{n+1}/K_n)$ to be the kernel of the restriction map $\text{Ш}(E/K_n) \to \text{Ш}(E/K_{n+1})$.

Theorem 7.1. *Assume:*

1. $\mathcal{E}_n \neq 0$ *for some* n*;*

2. $\text{Ш}(E, K_{n+1}/K_n) = 0$ *for all* $n \geq 0$.

Then $\mathcal{X}_\infty$ *has no non-trivial finite* Λ*-submodule.*

Remark. There is theoretical as well as experimental evidence in support of the expectation that Heegner points tend to be non-trivial modulo p. See also the discussion in [3, section 2].

We recall the results of [1]. Assume that the Iwasawa module of the Heegner points $\hat{\mathcal{E}}(E/K_\infty)_p$ is non-zero. Then, theorem 1 of [1, §3.1] shows that $\hat{S}_p(E/K_\infty)$ is a free Λ-module of rank 1. Write $\rho_\infty \in \Lambda$ for a characteristic power series of the cyclic torsion Λ-module $\hat{S}_p(E/K_\infty)/\hat{\mathcal{E}}(E/K_\infty)_p$, and let $(\mathcal{X}_\infty)_{\mathrm{tors}}$ be the Λ-torsion submodule of $\mathcal{X}_\infty$. Let γ be a topological generator of Γ. Theorem 1 of [1, §3.2] states the following:

1. $(\gamma - 1)\rho_\infty \cdot \mathcal{X}_\infty$ is a finite Λ-module;
2. if $\gamma - 1$ does not divide ρ_∞, then $\rho_\infty \cdot \mathcal{X}_\infty$ is a finite Λ-module.

Thus, in any case, $\rho_\infty^2 \cdot \mathcal{X}_\infty$ is finite.

Note that the condition $\mathcal{E}_n \neq 0$ implies that $\hat{\mathcal{E}}(E/K_\infty)_p \neq 0$. By imposing on $\hat{\mathcal{E}}(E/K_\infty)_p$ the stronger assumptions of theorem 7.1, we obtain the following strengthening of the above results.

Theorem 7.2. *Under the assumptions of theorem 7.1 we have:*

1. $(\gamma - 1)\rho_\infty \cdot \mathcal{X}_\infty = 0$.

2. If $\gamma - 1$ *does not divide* ρ_∞*, then* $\rho_\infty \cdot \mathcal{X}_\infty = 0$.

Thus, we have always $\rho_\infty^2 \cdot \mathcal{X}_\infty = 0$.

Proof of theorem 7.1. The rest of this section is devoted to the proof of theorem 7.1.

Let R_n be the group ring $\mathbb{Z}/p\mathbb{Z}[G_n]$. With γ as above, denote by γ_n the natural image of γ in G_n and by ω_n the element $\gamma_n - 1$ of R_n. The ring R_n is a local principal ideal ring, whose maximal ideal is generated by ω_n. Since R_n may be identified with the quotient $\bar{\Lambda}/(\gamma-1)^{p^n}$ of the PID $\bar{\Lambda} := \Lambda \otimes \mathbb{F}_p$, we can apply to R_n-modules the structure theory for modules over PID's. Therefore, if M is a finitely generated R_n-module, there is an isomorphism

$$M \simeq \bigoplus_{k=1}^{r} R_n/(\omega_n)^{i_k},$$

where $0 \leq i_k \leq p^n$. Note also that the R_n-module $R_n/(\omega_n)^i$, for $0 \leq i \leq p^n$, is isomorphic to $(\omega_n)^{p^n-i}$ via the map induced by multiplication by $\omega_n^{p^n-i}$. Moreover, the dimension of the $\mathbb{F}_p$-vector space $R_n/(\omega_n)^i$ is equal to i. (See [3, section 3] for more details.)

We will apply the above remarks to the structure of the R_n-modules $\mathrm{Sel}_p(E/K_n)$ and $\mathcal{E}_n$.

Let $\mathcal{G}_n := \mathrm{Gal}(K_{n+1}/K_n)$. Note that the restriction map induces an isomorphism

$$(*) \qquad \mathrm{Sel}_p(E/K_n) \xrightarrow{\sim} \mathrm{Sel}_p(E/K_{n+1})^{\mathcal{G}_n}.$$

(See, for example, [1, §2.2].) Thus, we may regard, and we will in the sequel, $\mathrm{Sel}_p(E/K_n)$ as a submodule of $\mathrm{Sel}_p(E/K_{n+1})$. By combining $(*)$ with the surjectivity of the corestriction maps on Heegner points (lemma 5.1), we obtain the equality

$$\mathcal{E}_n = N_{K_{n+1}/K_n}\mathcal{E}_{n+1},$$

where N_{K_{n+1}/K_n} denotes the norm operator $\sum g \in \mathbb{Z}[\mathcal{G}_n]$. In particular, we may view $\mathcal{E}_n$ as a submodule of $\mathcal{E}_{n+1}$.

We are assuming that there exists n_0 such that the R_{n_0}-module $\mathcal{E}_{n_0}$ is non-zero. Hence, $\mathcal{E}_{n_0}$ is isomorphic to $(\omega_{n_0})^{t_0}$, for $0 \leq t_0 < p^{n_0}$. From the norm-compatibility of Heegner points, we deduce that there is an isomorphism

$$\mathcal{E}_n \simeq (\omega_n)^{t_0}$$

for all n. For $n \geq n_0$, define U_n to be $\mathcal{E}_{n+1}^{\mathcal{G}_n}$. One checks that U_n is equal to $\omega_{n+1}^{p^{n+1}-p^n-t_0}\mathcal{E}_{n+1}$. Observe that U_n is an R_n-module in the natural way, and it is free of rank 1. If $n < n_0$, define U_n to be $\mathcal{E}_{n_0}^{\mathrm{Gal}(K_{n_0}/K_n)}$. Again, U_n is a free R_n-module of rank 1. It follows from the isomorphisms $(*)$ that U_n is a submodule of $\mathrm{Sel}_p(E/K_n)$.

Proposition 7.3. *For all $n \geq 1$, we have an equality of R_n-modules*

$$\mathrm{Sel}_p(E/K_n) = U_n \oplus T_n,$$

where the R_n-module T_n is annihilated by $\omega_n^{t_0}$.

Proof. See [2, theorem 12]. □

Remarks.

1. Theorem 12 of [2] is proved by building upon Kolyvagin's methods applied to the Euler System of Heegner points.

2. Since $t_0 < p^{n_0}$, we have the natural identification

$$R_n/(\omega_n)^{t_0} = R_{n_0}/(\omega_{n_0})^{t_0}.$$

Thus by proposition 7.3, for $n \geq n_0$, T_n is fixed by $\mathrm{Gal}(K_n/K_{n_0})$. By the isomorphisms $(*)$, we may assume that T_n is equal to T_{n_0}, for all $n \geq n_0$. In particular, the growth with n of the R_n-module $\mathrm{Sel}_p(E/K_n)$ is fully accounted for by the "universal norm" submodule U_n.

The free rank 1 R_n-module U_n, constructed from Heegner points, is a submodule of the p-Selmer group $\mathrm{Sel}_p(E/K_n)$. Under our assumptions, a stronger statement holds.

Proposition 7.4. *For all $n \geq 0$, U_n is a submodule of $E(K_n)/pE(K_n)$.*

Proof. By taking the $\mathcal{G}_n$-cohomology of the exact sequence

$$0 \to E(K_{n+1}) \xrightarrow{p} E(K_{n+1}) \to E(K_{n+1})/pE(K_{n+1}) \to 0$$

we obtain the exact sequence

$$0 \to E(K_n)/pE(K_n) \to (E(K_{n+1})/pE(K_{n+1}))^{\mathcal{G}_n} \to H^1(\mathcal{G}_n, E(K_{n+1})) \to 0.$$

For all places v of K_n, the local cohomology group $H^1((\mathcal{G}_n)_v, E((K_{n+1})_v))$ is zero. For, this group is the dual of $\hat{H}^0((\mathcal{G}_n)_v, E((K_{n+1})_v))$, by local Tate duality. But this last group is zero, by assumption B, (4) of section 5. Therefore, the group $H^1(\mathcal{G}_n, E(K_{n+1}))$ is equal to $Ш(E, K_{n+1}/K_n)$, which is trivial by our assumptions. Thus, the above exact sequence gives a natural isomorphism

$$E(K_n)/pE(K_n) \simeq (E(K_{n+1})/pE(K_{n+1}))^{\mathcal{G}_n}.$$

By construction, U_n belongs to $(E(K_{n+1})/pE(K_{n+1}))^{\mathcal{G}_n}$, when $n \geq n_0$, or to $E(K_{n_0})/pE(K_{n_0}))^{\mathrm{Gal}(K_{n_0}/K_n)}$, when $n < n_0$. Hence it is a submodule of $E(K_n)/pE(K_n)$, and this proves the claim. $\square$

As before, let $US_p(E/K)$ denote the universal norm submodule of $S_p(E/K)$. It is known (see lemma 1.1 and [1, §2.1]) that

$$\mathrm{rank}_{\mathbb{Z}_p} US_p(E/K) = \mathrm{rank}_\Lambda \hat{S}_p(E/K_\infty) = \mathrm{rank}_\Lambda \mathcal{X}_\infty.$$

Under the assumptions of theorem 7.1, the Iwasawa module of Heegner points $\hat{\mathcal{E}}(E/K_\infty)_p$ is free of rank 1 over Λ. Thus, the above equalities show that the $\mathbb{Z}_p$-rank of $US_p(E/K)$ is ≥ 1. Theorem 1 of [1, §3.1] (recalled after the statement of theorem 7.1) shows that the $\mathbb{Z}_p$-rank of $US_p(E/K)$ is equal to 1. In the next proposition, we give another proof of this fact under the current assumptions, more restrictive than those of [1], by working "modulo p" and using proposition 7.3. Moreover, we show that the quotient $S_p(E/K)/US_p(E/K)$ is torsion free. Combined with corollary 6.2, this concludes the proof of theorem 7.1.

Recall that $E(K)_p$ denotes the p-adic completion $E(K) \otimes \mathbb{Z}_p$ of the Mordell-Weil group $E(K)$.

Proposition 7.5. *The module $US_p(E/K)$ of universal norms is a free rank 1 $\mathbb{Z}_p$-module, and it is generated by an element of $E(K)_p$ not divisible by p.*

Proof. Step 1. One checks that the Pontryagin dual $\mathrm{Sel}_p(E/K_\infty)^{\mathrm{dual}}$ of $\mathrm{Sel}_p(E/K_\infty)$ is equal to $\mathcal{X}_\infty/p\mathcal{X}_\infty$. Hence, the Λ-rank of $\mathcal{X}_\infty$ is less than or equal to the $\bar{\Lambda}$-rank of $\mathrm{Sel}_p(E/K_\infty)^{\mathrm{dual}}$ (where recall that $\bar{\Lambda}$ is equal to $\Lambda \otimes \mathbb{F}_p$). Proposition 7.3 implies directly that $\mathrm{rank}_{\bar{\Lambda}} \mathrm{Sel}_p(E/K_\infty)^{\mathrm{dual}}$ is ≤ 1, and hence $\mathrm{rank}_{\mathbb{Z}_p} US_p(E/K)$ is ≤ 1. By combining this with the opposite inequality, which we have observed before the statement of proposition 7.5, we conclude that $US_p(E/K)$ is isomorphic to $\mathbb{Z}_p$.

Step 2. Denote by $\tilde{U}_n$ a lift of U_n to $E(K_n)_p$ by the natural projection. The $\mathbb{Z}_p[G_n]$-module $\tilde{U}_n$ is free of rank 1. Let u_n be a generator. For all $n \geq 1$, the natural inclusion of points induces an isomorphism

$$E(K)/pE(K) \simeq (E(K_n)/pE(K_n))^{G_n}.$$

(This is a consequence of the proof of proposition 7.4.) It follows directly that the norm $v_n \in E(K)_p$ of u_n from K_n to K is not divisible by p. Since $E(K)_p$ is compact in the p-adic topology, we can extract from the sequence

$\{v_n\}_{n\geq 1}$ a subsequence $\{v_{n_i}\}_{i\geq 1}$, converging to an element $v_\infty \in E(K)_p$ such that:

1. $v_\infty = v_{n_i} + p^i\epsilon_i$ for some $\epsilon_i \in E(K)_p$,
2. $v_{n_i} = N_{K_i/K} w_i$ for some $w_i \in E(K_i)_p$.

Hence $v_\infty = N_{K_i/K}(w_i + \epsilon_i)$ for all $i \geq 1$, i.e., v_∞ belongs to the module $US_p(E/K)$ of universal norms. Moreover, since the v_n are not divisible by p in $E(K)_p$, the element v_∞ is also not divisible by p. Hence, by step 1, v_∞ is a generator of $US_p(E/K)$.

This concludes the proof of proposition 7.5, and the proof of theorem 7.1. □

The proof of theorem 7.1 also gives the following byproduct.

Proposition 7.6. *Let n_0 be such that $\mathcal{E}_{n_0} \neq 0$.*

1. For all $n \geq n_0$, we have

$$\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K_n) = p^n + e,$$

where $e = \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K_{n_0}) - p^{n_0}$ is a non-negative integer independent of n.

2. For all $n \geq n_0$,

$$\mathrm{rank}_{\mathbb{Z}} E(K_n) = p^n + e',$$

where $e' = \mathrm{rank}_{\mathbb{Z}} E(K_{n_0}) - p^{n_0}$ is a non-negative integer independent of n.

Proof. 1. It follows directly from proposition 7.3 and the remark 2 after it.

2. The $\mathbb{Z}$-rank of $E(K_n)$ is equal to the $\mathbb{F}_p$-dimension of $E(K_n)/pE(K_n)$ for all n, since $E(K_n)$ has no p-torsion. The claim follows from proposition 7.3 and the proof of proposition 7.4. □

References

[1] M. BERTOLINI, *Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions.* Compositio Math. **99** (1995), 153–182.

[2] M. BERTOLINI, *An annihilator for the p-Selmer group by means of Heegner points.* Atti Acc. Naz. Lincei, Classe di Sc. Fis., Mat. e Nat., Rendiconti Lincei, Mat. e Appl., Serie 9, Vol. 5, Fasc. 2 (1994), 129–140.

[3] M. BERTOLINI, *Growth of Mordell-Weil groups in anticyclotomic towers.* Symposia Mathematica, Proceedings of the Symposium in Arithmetic Geometry, Cortona 1994, E. Bombieri, et al., eds., Cambridge Univ. Press, to appear.

[4] M. BERTOLINI, H. DARMON, *Derived heights and generalized Mazur-Tate regulators.* Duke Math. Journal **76** (1994), 75–111.

[5] M. BERTOLINI, H. DARMON, *Heegner points on Mumford-Tate curves.* Inventiones Math., to appear.

[6] J. COATES, R. GREENBERG, *Kummer theory for Abelian varieties over local fields.* Inventiones Math. **124** (1996), 129–174.

[7] J. COATES, G. MCCONNELL, *Iwasawa theory of modular elliptic curves of analytic rank at most* 1. J. London Math. Soc. (2) **50** (1994), 243–264.

[8] R. Greenberg, *Iwasawa theory for p-adic representations*. Algebraic Number Theory – in honor of K. Iwasawa, J. Coates et al., editors, Advanced Studies in Pure Mathematics, 1989, Academic Press.

[9] S. Lang, *Cyclotomic fields I and II* (Combined second edition,) GTM 121, 1990, Springer.

[10] B. Mazur, *Rational points of Abelian Varieties with values in towers of number fields*. Inventiones Math. **18** (1972), 183–266.

[11] B. Mazur, *Modular Curves and Arithmetic*, Proc. Int. Cong. of Math. 1983, Warszawa.

[12] B. Mazur, *Elliptic curves and towers of number fields*. Unpublished manuscript.

[13] J-S. Milne, *Arithmetic duality theorems*. Perspective in Math., Academic Press, 1986.

[14] B. Perrin-Riou, *Fonctions L p-adiques, Théorie d'Iwasawa et points de Heegner*. Bull. Soc. Math. de France **115** (1987), 399–456.

[15] B. Perrin-Riou, *Théorie d'Iwasawa et hauteurs p-adiques*. Inventiones Math. **109** (1992), 137–185.

[16] D. Rohrlich, *On L-functions of elliptic curves and anti-cyclotomic towers*. Inventiones Math. **64** (1984), 393–408.

[17] D. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*. Inventiones Math. **75** (1984), 409–423.

[18] P. Schneider, *Iwasawa L-functions of varieties over algebraic number fields. A first approach*. Inventiones Math. **71** (1983), 251-293.

[19] P. Schneider, *p-adic height pairings II*. Inventiones Math. **79** (1985), 329–374.

[20] P. Schneider, *Arithmetic of formal groups and applications. I. Universal norm subgroups*. Inventiones Math. **87** (1987), 587–602.

[21] J.-P. Serre, *Cohomologie Galoisienne*. LNM 5 (cinquième édition), Springer, 1994.

Massimo Bertolini
Dipartimento di Matematica Pura e Applicata
Università degli Studi di Padova
Via Belzoni 7
35121 Padova - Italy
E-mail : massimo@math.unipd.it