Selmer Groups of Elliptic Curves with Complex Multiplication

(*to appear in Canadian Journal of Mathematics, vol. 56 (2004)*)

By A. SAIKIA

McGill University

Montreal, H3A 2K6 Canada.

Email : saikia@math.mcgill.ca

Abstract. Suppose K is an imaginary quadratic field and E is an elliptic curve over a number field F with complex multiplication by the ring of integers in K. Let p be a rational prime that splits as $\mathfrak{p}_1\mathfrak{p}_2$ in K. Let E_{p^n} denote the p^n-division points on E. Assume that $F(E_{p^n})$ is abelian over K for all $n \geq 0$. This paper proves that the Pontrjagin dual of the $\mathfrak{p}_1^\infty$-Selmer group of E over $F(E_{p^\infty})$ is a finitely generated free Λ-module, where Λ is the Iwasawa algebra of $\mathrm{Gal}\big(F(E_{p^\infty})/F(E_{\mathfrak{p}_1^\infty\mathfrak{p}_2})\big)$. It also gives a simple formula for the rank of the Pontrjagin dual as a Λ-module.

Acknowledgment. The author is indebted to J.H. Coates for many helpful suggestions at various stages of this paper. This paper would not have been possible without his guidance. The author also thanks S. Howson, L. Fu and the referee for their comments. The author was supported by Hodge Fellowship at IHES and CRM/CICMA post doctoral fellowship at McGill University during the progress of this work.

1. Introduction

Let K be an imaginary quadratic field. Suppose E is an elliptic curve over a number field F with complex multiplication by the ring of integers $\mathcal{O}$ in K. Let $p \neq 2, 3$ denote a rational prime such that $p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$ and assume that E has good reduction over both $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Pick any element π of $\mathcal{O}$ such that $\pi\mathcal{O} = \mathfrak{p}_1^h$ for some $h \geq 1$. Clearly, there is also an element $\bar{\pi}$ in $\mathcal{O}$ such that $\bar{\pi}\mathcal{O} = \mathfrak{p}_2^h$. Let L be an algebraic extension of F. For $n \geq 0$, the π^n-Selmer group of E over L is defined as

$$Sel_{\pi^n}(E/L) = \mathrm{Ker}\Big(H^1(L, E_{\pi^n}) \longrightarrow \prod_v H^1(L_v, E)_{\pi^n}\Big),$$

where v runs over all the places of L. The $\mathfrak{p}_1^\infty$-Selmer group of E/L is defined as

$$Sel_{\mathfrak{p}_1^\infty}(E/L) = \varinjlim_n Sel_{\pi^n}(E/L),$$

where the limit is with respect to the homomorphisms induced by the natural inclusion of E_{π^n} into $E_{\pi^{n+1}}$. The $\mathfrak{p}_1^\infty$-Selmer group fits into an exact sequence

$$0 \longrightarrow E(L) \otimes K_{\mathfrak{p}_1}/\mathcal{O}_{\mathfrak{p}_1} \longrightarrow Sel_{\mathfrak{p}_1^\infty}(E/L) \longrightarrow III(E/L)_{\mathfrak{p}_1^\infty} \longrightarrow 0, \qquad (1)$$

where $E(L)$ is the Mordell-Weil group of rational points on E defined over L and $III(E/L)$ is the Tate-Shafarevich group of E/L defined by

$$III(E/L) = \mathrm{Ker}\Big(H^1(L, E) \longrightarrow \prod_v H^1(L_v, E)\Big).$$

One of the basic questions in number theory is to understand the Mordell-Weil group and the Tate-Shafarevich group of E over various field extensions of $\mathbb{Q}$. Thus, the importance of the study of Selmer groups arise from the exact sequence (1) above.

There are some natural choices for the field extension L of F, over which we want to examine the structure of $Sel_{\mathfrak{p}_1^\infty}(E/L)$. We usually take L to be a field generated over F by the torsion points on E. In particular, we will consider

$$F_\infty = F(E_{p^\infty}),$$

and study $Sel_{\mathfrak{p}_1^\infty}(E/F_\infty)$, or rather its Pontrjagin dual $X(F_\infty)$. By definition,

$$X(F_\infty) = Hom\big(Sel_{\mathfrak{p}_1^\infty}(E/F_\infty), \mathbb{Q}_p/\mathbb{Z}_p\big).$$

It is compact and has the natural structure of $\mathrm{Gal}(F_\infty/F)$-module. This will be the primary object of our study in this paper.

2. Notation

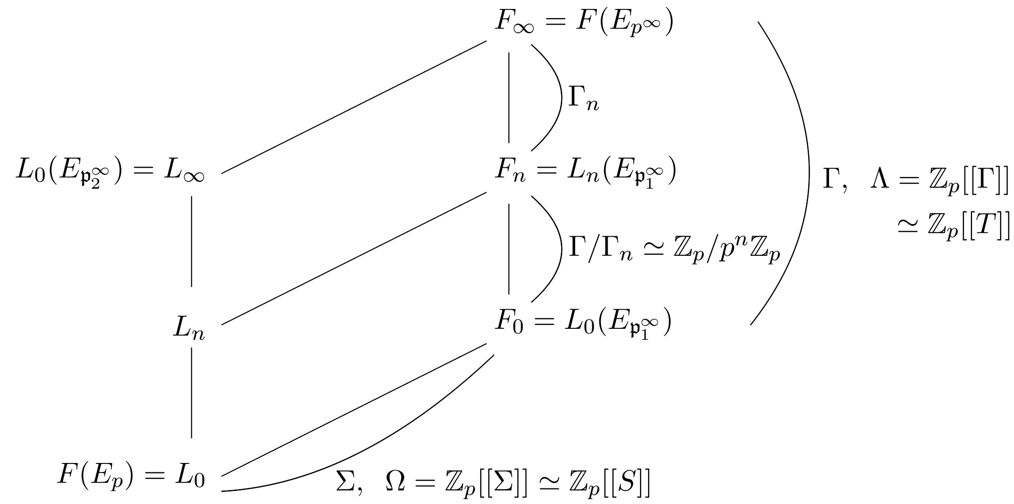
We define the following field extensions of the number field F generated by torsion points on E:

$$L_0 = F(E_p), \;\; F_0 = L_0(E_{\mathfrak{p}_1^\infty}), \;\; L_\infty = L_0(E_{\mathfrak{p}_2^\infty}), \;\; F_\infty = F(E_{p^\infty}).$$

Let Γ' be the Galois group of F_∞ over L_0, and Σ be the Galois group F_0 over L_0. Let Γ be the Galois group F_∞ over F_0, which can also be identified with the Galois group L_∞ over L_0. Clearly, Γ' is isomorphic to $\mathbb{Z}_p^2$, whereas Γ and Σ are isomorphic to $\mathbb{Z}_p$. We denote the unique subgroup of index p^n in Γ by Γ_n. Let L_n and F_n be the fixed fields of L_∞ and F_∞ respectively under the action of Γ_n. Then, we have the following Galois groups:

$$\mathrm{Gal}(L_\infty/L_n) \simeq \mathrm{Gal}(F_\infty/F_n) = \Gamma_n, \qquad \mathrm{Gal}(L_n/L_0) \simeq \mathrm{Gal}(F_n/F_0) = \Gamma/\Gamma_n \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p.$$

We have the following field diagram:



The Iwasawa algebra of Γ is defined as

$$\mathbb{Z}_p[[\Gamma]] = \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma_n],$$

where the inverse limit is taken with respect to canonical surjective maps. We denote the Iwasawa algebra of Γ by Λ, and that of Σ by Ω. Following Serre, we can identify Λ with $\mathbb{Z}_p[[T]]$ and Ω with $\mathbb{Z}_p[[S]]$. We note that $\mathbb{Z}_p[[\Gamma']]$ is isomorphic to $\mathbb{Z}_p[[T,S]]$. We will denote the Pontrjagin dual of $Sel_{\mathfrak{p}_1^\infty}(E/F_n)$ by $X(F_n)$.

3. *Statement of results*

Our goal is to study the structure of $X(F_\infty)$ as a module over the Iwasawa algebra $\Lambda \simeq \mathbb{Z}_p[[T]]$. We shall work under the following hypothesis :

(**Hyp**) The fields $F(E_{p^n})$ are abelian over K for all $n \geq 0$.

Note that when $F = K$, the hypothesis is true by theory of complex multiplication. It is well known (e.g. see [P-R 1]) that $X(F_\infty)$ is a finitely generated torsion module over the

Iwasawa algebra $\mathbb{Z}_p[[S,T]]$, whereas $X(F_n)$ is a finitely generated torsion $\mathbb{Z}_p[[S]]$-module under the above hypothesis. Let λ_0 be the rank of $X(F_0)$ as a $\mathbb{Z}_p$-module. In this paper, we shall prove the following two theorems about the Λ-module structure of $X(F_\infty)$:

Theorem 1 : $X(F_\infty)$ *is a finitely generated* Λ-*module.*

Theorem 2 : $X(F_\infty)$ *is a free* Λ-*module of rank* $\lambda_0 + r - 1$.

Here r is the number of primes of F_0 above $\mathfrak{p}_2$. Since the primes over $\mathfrak{p}_2$ do not split in the tower F_∞ over F_0, r is also the number of primes above $\mathfrak{p}_2$ of F_n for any $n \geq 0$.

4. The structure of $X(F_n)$

The key idea in the proof of the theorems 1 and 2 is to examine the relation between $X(F_\infty)$ and $X(F_n)$, and then exploit well-known facts about $X(F_n)$. Theorem 18 and proposition 20 in [P-R 1] show that $X(F_n)$ is a finitely generated torsion $\mathbb{Z}_p[[S]]$-module provided Leopoldt's conjecture is true for the $\mathbb{Z}_p$-extension F_n over L_n. Brumer proved that Leoplodt's conjecture is true for the $\mathbb{Z}_p$-extensions of an abelian extension of an imaginary quadratic field. Under our hypothesis (Hyp), L_n is an abelian extension of the imaginary quadratic field K. Therefore, Leopoldt's conjecture holds for F_n and as a consequence, we know that $X(F_n)$ is a finitely generated torsion $\mathbb{Z}_p[[S]]$-module. By structure theory of finitely generated torsion $\mathbb{Z}_p[[S]]$-module, there is a homomorphism

$$\phi : X(F_n) \longrightarrow \bigoplus \Big(\oplus_{i=1}^{s} \mathbb{Z}_p[[S]]/p^{n_i} \Big) \bigoplus \Big(\oplus_{j=1}^{t} \mathbb{Z}_p[[S]]/(f_j^{m_j}) \Big), \tag{2}$$

with finite kernel and cokernel. Here f_j are distinguished polynomials in $\mathbb{Z}_p[[S]]$ and s, t, n_i, m_j are non-negative integers. The *lambda*-invariant λ_n and the *mu*-invariant μ_n of the $\mathbb{Z}_p[[S]]$-module $X(F_n)$ are defined as

$$\lambda_n = \sum_{j=1}^{t} m_j.\deg(f_j), \quad \mu_n = \sum_{i=1}^{r} n_i.$$

When L_n is an abelian extension of K, Gillard ([Gi 1], [Gi 2]) has shown that $\mu_n = 0$. While [Gi 2] has the proof of vanishing of the *mu*-invariant without any assumption on the class number of K, the proof in [Gi 1] works under the assumption that the class number of K is 1 (that would have amounted to assuming that E is defined over K in our work). As L_n is abelian over K under our hypothesis (Hyp), Gillard's result implies that the p-torsion part in the right hand side of (2) does not occur. Moreover, it follows (as pointed out in theorem 25 of [P-R 1]) from the work of Greenberg ([Gr 1]) that $X(F_n)$ has no finite non-zero $\mathbb{Z}_p[[S]]$-submodule. Thus, the kernel of ϕ (*a priori* finite) is trivial. Hence, ϕ maps $X(F_n)$ injectively into a free $\mathbb{Z}_p$-module of rank λ_n with finite cokernel. We have now obtained the following information regarding the $\mathbb{Z}_p$-module structure of $X(F_n)$:

Proposition 3 : *$X(F_n)$ is a free $\mathbb{Z}_p$-module of rank λ_n under our hypothesis (Hyp).*

How the *lambda*-invariant λ_n of $X(F_n)$ varies along the tower of fields F_n $(n = 0, 1, 2, \ldots)$ will be very important to us. We will study this question in section 7 (c.f. lemma 11).

5. *A crucial proposition*

Let us fix an $n \geq 0$. Let S be the set of primes of F above p. Let F_S be the maximal extension of F unramified outside S. It is clear that $F_\infty \subset F_S$ and $E_{\mathfrak{p}_1^\infty} \subset E(F_S)$. The following result is a crucial ingredient in examining the relation between $X(F_\infty)$ and $X(F_n)$ [see the commutative diagram (c.d.) in section 6] :

Proposition 4 : *There is an exact sequence of Galois modules*

$$0 \longrightarrow Sel_{\mathfrak{p}_1^\infty}(E/F_n) \longrightarrow H^1(F_S/F_n, E_{\mathfrak{p}_1^\infty}) \longrightarrow \prod_{v|p} H^1(F_{n,v}, E)_{\mathfrak{p}_1^\infty} \longrightarrow 0.$$

The key part in the above proposition is the surjectivity. Hachimori and Matsuno [H-M] proved the above result for the cyclotomic $\mathbb{Z}_p$-extension of a number field. But their argument carries over to our situation of elliptic curves with complex multiplication. We will briefly describe how the methods of [H-M] can be adopted in our case. We will see that the sequence in proposition 4 comes from a five-term Cassels-Poitou-Tate sequence (5). It will be sufficient to show that the fourth term in (5) vanishes (lemma 5). As a consequence of this method of proof, we deduce that the fifth term in (5) (a H^2 term) also vanishes and deduce corollary 6. This vanishing (of H^2) will be needed for the calculations of section 7, especially lemma 12.

Let us denote the $\mathbb{Z}_p$-extension F_n of L_n by T_∞. We know that the Galois group $\Sigma \simeq \mathrm{Gal}(T_\infty/L_n)$ has a unique subgroup Σ_m of index p^m. Let T_m be the fixed field of T_∞ under the action of Σ_m. We have a field diagram

$$\begin{tikzcd}
F_n = L_n(E_{\mathfrak{p}_1^\infty}) = T_\infty \arrow[d, dash] \\
T_m \arrow[d, dash] \arrow[u, dash, bend right, "\Sigma_m"'] \\
L_n \arrow[uu, dash, bend right=60, "{\Sigma,\ \ \Omega \simeq \mathbb{Z}_p[[\Sigma]]}"']
\end{tikzcd}$$

By Cassels-Poitou-Tate sequence for the number fields T_m, we have a long exact sequence (where $\widehat{M}$ denotes the Pontrjagin dual of M)

$$\begin{aligned}
0 &\longrightarrow Sel_{\pi^k}(E/T_m) \longrightarrow H^1(F_S/T_m, E_{\pi^k}) \longrightarrow \prod_{v|p} H^1(T_{m,v}, E)_{\pi^k} \\
&\longrightarrow \widehat{Sel_{\bar{\pi}^k}(E/T_m)} \longrightarrow H^2(F_S/T_m, E_{\pi^k}) \longrightarrow \prod_{v|p} H^2(T_{m,v}, E_{\bar{\pi}^k}) \\
&\longrightarrow \widehat{H^0(F_S/T_m, E_{\bar{\pi}^k})} \longrightarrow 0.
\end{aligned} \tag{3}$$

We note that in applying Poitou-Tate duality, one has to consider not only the primes above p, but also the infinite primes and the primes of bad reduction. However, E has good reduction everywhere over L_0 by theory of complex multiplication, and we can also ignore the infinite primes as p is odd. The inclusion $E_{\pi^k} \hookrightarrow E_{\pi^{k+1}}$ induces a map $H^i(F_S/T_m, E_{\pi^k})$ to $H^i(F_S/T_m, E_{\pi^{k+1}})$, and its dual is given by 'multiplication by π'. By taking direct limits in (3) as k goes to infinity, we get a five term exact sequence

$$\begin{aligned}
0 &\longrightarrow Sel_{\mathfrak{p}_1^\infty}(E/T_m) \longrightarrow H^1(F_S/T_m, E_{\mathfrak{p}_1^\infty}) \longrightarrow \prod_{v|p} H^1(T_{m,v}, E)_{\mathfrak{p}_1^\infty} \\
&\longrightarrow \Big(\varprojlim_k Sel_{\bar{\pi}^k}(E/T_m)\Big)^{\wedge} \longrightarrow H^2(F_S/T_m, E_{\mathfrak{p}_1^\infty}) \longrightarrow 0.
\end{aligned} \tag{4}$$

We remark that when we take direct limit with respect to k, the sixth term in (3) vanishes by Tate local duality (see Ch.II prop. 16 in [Se]). There is a restriction map from $H^i(F_S/T_m, E_{\mathfrak{p}_1^\infty})$ to $H^i(F_S/T_{m+1}, E_{\mathfrak{p}_1^\infty})$, and the dual map is given by corestriction which acts like the norm map on H^0. We now take direct limits in (4) as m goes to infinity, and obtain a five term exact sequence

$$\begin{aligned}
0 &\longrightarrow Sel_{\mathfrak{p}_1^\infty}(E/T_\infty) \longrightarrow H^1(F_S/T_\infty, E_{\mathfrak{p}_1^\infty}) \longrightarrow \prod_{v|p} H^1(T_{\infty,v}, E)_{\mathfrak{p}_1^\infty} \\
&\longrightarrow \Big(\varprojlim_m \varprojlim_k Sel_{\bar{\pi}^k}(E/T_m)\Big)^{\wedge} \longrightarrow H^2(F_S/T_\infty, E_{\mathfrak{p}_1^\infty}) \longrightarrow 0.
\end{aligned} \tag{5}$$

Let us denote the fourth term in the above sequence as $\hat{W}$, i.e.,

$$W = \varprojlim_{m} \varprojlim_{k} Sel_{\bar{\pi}^k}(E/T_m).$$

Proposition 4 claims that the fourth term in the above sequence (5) vanishes.

Lemma 5 :

$$W = \varprojlim_{m} \varprojlim_{k} Sel_{\bar{\pi}^k}(E/T_m) = 0.$$

Proof : We adopt an argument similar to the one in proposition 2.3 of [H-M]. We have an exact sequence (see lemma 1.8 in [C-S])

$$0 \longrightarrow E_{\bar{\pi}^\infty}(T_m) \longrightarrow \varprojlim_{k} Sel_{\bar{\pi}^k}(E/T_m) \longrightarrow Hom_{\mathbb{Z}_p}\big(\widehat{Sel_{\bar{\pi}^\infty}(E/T_m)}, \mathbb{Z}_p\big) \longrightarrow 0.$$

We now take inverse limit with respect to corestriction maps as m goes to infinity. These maps act like norm maps on the first term, and it vanishes in the limit since only finitely many $\bar{\pi}$-torsion points of E are defined over T_∞. Thus, we obtain an injection

$$W = \varprojlim_{m} \varprojlim_{k} Sel_{\bar{\pi}^k}(E/T_m) \hookrightarrow \varprojlim_{m} Hom_{\mathbb{Z}_p}\big(\widehat{Sel_{\mathfrak{p}_2^\infty}(E/T_m)}, \mathbb{Z}_p\big).$$

The kernel of the restriction map $Sel_{\mathfrak{p}_2^\infty}(E/T_m) \longrightarrow Sel_{\mathfrak{p}_2^\infty}(E/T_\infty)^{\Sigma_m}$ is finite and its order is bounded independent of m (this kernel is contained in $H^1(\Sigma_m, E_{\mathfrak{p}_2^\infty}(T_\infty))$, and this group is bounded independent of m, as shown in lemma 3.1 of [Gr 2]). Therefore, we have an injection

$$\varprojlim_{m} Hom_{\mathbb{Z}_p}\big(\widehat{Sel_{\mathfrak{p}_2^\infty}(E/T_m)}, \mathbb{Z}_p\big) \hookrightarrow \varprojlim_{m} Hom_{\mathbb{Z}_p}\big((\widehat{Sel_{\mathfrak{p}_2^\infty}(E/T_\infty)})_{\Sigma_m}, \mathbb{Z}_p\big).$$

The latter module has the same underlying set as $Hom_\Omega\big(\widehat{Sel_{\mathfrak{p}_2^\infty}(E/T_\infty)}, \Omega\big)$ (e.g., §2, lemma 4(ii) in [P-R 2]).

We again invoke proposition 20 in [P-R 1] which says that $Sel_{\mathfrak{p}_2^\infty}(E/T_\infty)$ is Ω-cotorsion provided Leopoldt's conjecture is true for the $\mathbb{Z}_p$-extension T_∞ of L_n. But Leopoldt's conjecture is true for the $\mathbb{Z}_p$-extension T_∞ of the abelian [under our hypothesis (Hyp)] extension L_n of the imaginary quadratic field K. Therefore, $Sel_{\mathfrak{p}_2^\infty}(E/T_\infty)$ is Ω-cotorsion and $Hom_\Omega\big(\widehat{Sel_{\mathfrak{p}_2^\infty}(E/T_\infty)}, \Omega\big) = 0$.

Thus, the compact Ω-module W can be embedded into the null module. □

With this lemma, the proof of proposition 4 is now complete. The following corollary to lemma 5 will be a vital step in our proof of theorem 2 (lemma 12 in section 7).

Corollary 6 : For any $n \geq 0$, $H^2\big(F_S/F_n, E_{\mathfrak{p}_1^\infty}\big) = 0$.

Proof : From the Cassels-Poitou-Tate sequence (5) and lemma 5, it is clear that $H^2\big(F_S/T_\infty, E_{\mathfrak{p}_1^\infty}\big) = 0$. But T_∞ stands for any of the F_n for $n \geq 0$. $\square$

6. *Relation between $X(F_\infty)$ and $X(F_n)$*

In order to examine the relation between $X(F_\infty)$ and $X(F_n)$, the following commutative diagram is of crucial importance:

$$\begin{tikzcd}
0 \arrow[r] & Sel_{\mathfrak{p}_1^\infty}(E/F_\infty)^{\Gamma_n} \arrow[r] & H^1(F_S/F_\infty, E_{\mathfrak{p}_1^\infty})^{\Gamma_n} \arrow[r] & \prod_{v|p}\Big(\prod_{w|v} H^1(F_{\infty,w}, E)_{\mathfrak{p}_1^\infty}\Big)^{\Gamma_n} & \\
0 \arrow[r] & Sel_{\mathfrak{p}_1^\infty}(E/F_n) \arrow[r] \arrow[u, "\alpha_n"] & H^1(F_S/F_n, E_{\mathfrak{p}_1^\infty}) \arrow[r] \arrow[u, "\beta_n"] & \prod_{v|p} H^1(F_{n,v}, E)_{\mathfrak{p}_1^\infty} \arrow[r] \arrow[u, "\gamma_n=\prod_{v|p}\gamma_{n,v}"'] & 0
\end{tikzcd}$$

Commutative Diagram (c.d.)

The horizontal maps originate from Cassels-Poitou-Tate sequence, whereas the vertical maps are induced by restriction. All of our work in section 5 has been to establish the exactness of the bottom row in the above diagram. We are primarily interested in the kernel and cokernel of the map α_n above. By the snake lemma, we have an exact sequence

$$0 \longrightarrow \mathrm{Ker}(\alpha_n) \longrightarrow \mathrm{Ker}(\beta_n) \longrightarrow \mathrm{Ker}(\gamma_n) \longrightarrow \mathrm{Coker}(\alpha_n) \longrightarrow \mathrm{Coker}(\beta_n) \ldots \qquad (6)$$

In order to understand the structure of $\mathrm{Ker}(\alpha_n)$ and $\mathrm{Coker}(\alpha_n)$, we will first study the kernels and cokernels of the maps β_n and γ_n.

Lemma 7 : $\mathrm{Ker}(\beta_n) \simeq \mathbb{Q}_p/\mathbb{Z}_p$, and $\mathrm{Coker}(\beta_n) = 0$.

Proof : Recall that all the points in $E_{\mathfrak{p}_1^\infty}$ are defined over F_n $(n = 0, 1, \ldots)$. By the inflation-restriction sequence of cohomology, $\mathrm{Ker}(\beta_n)$ equals $H^1(\Gamma_n, E_{\mathfrak{p}_1^\infty})$, and $\mathrm{Coker}(\beta_n)$ is contained in $H^2(\Gamma_n, E_{\mathfrak{p}_1^\infty})$. But Γ_n is isomorphic to $\mathbb{Z}_p$, and hence it has p-cohomological dimension 1. Therefore, $H^2(\Gamma_n, E_{\mathfrak{p}_1^\infty})$ vanishes and it follows that $\mathrm{Coker}(\beta_n)$ is trivial. Moreover, Γ_n acts trivially on $E_{\mathfrak{p}_1^\infty}$ and hence $H^1(\Gamma_n, E_{\mathfrak{p}_1^\infty})$ equals $Hom(\Gamma_n, \mathbb{Q}_p/\mathbb{Z}_p)$. We can now conclude that $\mathrm{Ker}(\beta_n) \simeq \mathbb{Q}_p/\mathbb{Z}_p$. $\square$

Lemma 8 : *For $v|\mathfrak{p}_1$, $Ker(\gamma_{n,v}) = 0$.*

We shall give a short and direct proof of this lemma, though it follows from a more general result of Perrin-Riou (lemma 9 in [P-R 1]).

Proof : By Shapiro's lemma,

$$\Big(\prod_{w|v} H^1(F_{\infty,w}, E)\Big)^{\Gamma_n}_{\mathfrak{p}_1^\infty} = H^1(F_{\infty,w}, E)^{\Gamma_{n,v}}_{\mathfrak{p}_1^\infty},$$

where $\Gamma_{n,v}$ is the decomposition subgroup of Γ_n. By the inflation-restriction sequence,

$$\mathrm{Ker}(\gamma_{n,v}) = H^1\big(\Gamma_{n,v}, E(F_{\infty,w})\big)_{\mathfrak{p}_1^\infty}.$$

Clearly,

$$F_{\infty,w} = \bigcup_M L_{\infty,v'}M,$$

where M runs over the finite extensions of $L_{n,\tilde{v}}$ contained in $F_{n,v}$, and v', $\tilde{v}$ are the primes below w of L_∞ and L_n respectively. Now,

$$\mathrm{Ker}(\gamma_{n,v}) = \varinjlim_M H^1\big(G(L_{\infty,v'}M/M), E(L_{\infty,v'}M)\big)_{\mathfrak{p}_1^\infty}.$$

Note that E has good reduction over $L_{n,\tilde{v}}$. Therefore, $L_{\infty,v'}$ is unramified over $L_{n,\tilde{v}}$ and so is $L_{\infty,v'}M$ over M. Hence, $H^1\big(G(L_{\infty,v'}M/M), E(L_{\infty,v'}M)\big) = 0$ (see [Mi, p. 58]). This concludes the proof of lemma 8. $\square$

Lemma 9 : *For $v|\mathfrak{p}_2$, $Ker(\gamma_{n,v}) \simeq \mathbb{Q}_p/\mathbb{Z}_p$.*

Proof : The extension F_∞ is totally ramified over F_n at the prime v over $\mathfrak{p}_2$. Therefore, there is only one prime w of F_∞ over v and the decomposition group $\Gamma_{n,v}$ is the Galois group Γ_n. By the inflation-restriction sequence,

$$\mathrm{Ker}(\gamma_{n,v}) = H^1\big(\Gamma_{n,v}, E(F_{\infty,v})\big)_{\mathfrak{p}_1^\infty}.$$

Let $\mathfrak{m}_{\infty,v}$ be the maximal ideal of $F_{\infty,v}$ and $k_{\infty,v}$ be the residue field. Let $\hat{E}$ be the formal group attached to E giving the kernel of reduction at v. We have the following exact sequence of $\Gamma_{n,v}$-modules:

$$0 \longrightarrow \hat{E}(\mathfrak{m}_{\infty,v}) \longrightarrow E(F_{\infty,v}) \longrightarrow \tilde{E}_v(k_{\infty,v}) \longrightarrow 0.$$

Taking Galois cohomology, we get the following exact sequence:

$$\ldots \longrightarrow H^1\big(\Gamma_{n,v}, \hat{E}(\mathfrak{m}_{\infty,v})\big)_{\mathfrak{p}_1^\infty} \longrightarrow H^1\big(\Gamma_{n,v}, E(F_{\infty,v})\big)_{\mathfrak{p}_1^\infty}$$
$$\longrightarrow H^1\big(\Gamma_{n,v},\ \tilde{E}_v(k_{\infty,v})\big)_{\mathfrak{p}_1^\infty} \longrightarrow H^2\big(\Gamma_{n,v}, \hat{E}(\mathfrak{m}_{\infty,v})\big)_{\mathfrak{p}_1^\infty} \rightarrow \ldots.$$

Since $v|\mathfrak{p}_2$, π is an automorphism of $\hat{E}$. Therefore, $H^i\big(\Gamma_{n,v},\ \hat{E}(\mathfrak{m}_{\infty,v})\big)_{\mathfrak{p}_1^\infty}$=0 $\forall\ i \geq 0$. Hence we have

$$H^1\big(\Gamma_{n,v},\ E(F_{\infty,v})\big)_{\mathfrak{p}_1^\infty} \xrightarrow{\sim} H^1\big(\Gamma_{n,v},\ \tilde{E}_v(k_{\infty,v})\big)_{\mathfrak{p}_1^\infty}.$$

As $\tilde{E}_v(k_{\infty,v})$ is a torsion module, we can take the $\mathfrak{p}_1^\infty$-torsion inside the cohomology group. Since $F_{\infty,w}$ is totally ramified over $F_{n,v}$, the group $\Gamma_{n,v}$ acts trivially on $\tilde{E}_v(k_{\infty,v})$. Therefore, the right hand side in the previous expression is

$$Hom(\Gamma_{n,v}, \tilde{E}_{v,\mathfrak{p}_1^\infty}) \simeq Hom(\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) = \mathbb{Q}_p/\mathbb{Z}_p. \qquad \Box$$

Note that there are r primes above $\mathfrak{p}_2$ in F_n $(n = 0, 1, \ldots)$. It follows from lemma 8 and lemma 9 that

$$\mathrm{Ker}(\gamma_n) = \bigoplus_{v|p} \mathrm{Ker}(\gamma_{n,v}) \simeq \big(\mathbb{Q}_p/\mathbb{Z}_p\big)^r.$$

We can now rewrite the exact sequence (6) as

$$0 \longrightarrow \mathrm{Ker}(\alpha_n) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \Big(\mathbb{Q}_p/\mathbb{Z}_p\Big)^r \longrightarrow \mathrm{Coker}(\alpha_n) \longrightarrow 0. \tag{7}$$

The above exact sequence enables us to deduce the following result about the Λ-module structure of $X(F_\infty)$:

Lemma 10 : $X(F_\infty)_{\Gamma_n}$ is a free $\mathbb{Z}_p$-module.

Proof : Taking the Pontrjagin dual of the exact sequence (7), we obtain

$$0 \longrightarrow \widehat{\mathrm{Coker}(\alpha_n)} \longrightarrow \mathbb{Z}_p^r \longrightarrow \ldots$$

This tells us that $\widehat{\mathrm{Coker}(\alpha_n)}$ is a finitely generated free $\mathbb{Z}_p$-module. Taking Pontrjagin dual in the first column of the commutative diagram (c.d.), we have

$$0 \longrightarrow \widehat{\mathrm{Coker}(\alpha_n)} \longrightarrow X(F_\infty)_{\Gamma_n} \longrightarrow X(F_n).$$

By proposition 3, we know that $X(F_n)$ is a free $\mathbb{Z}_p$-module. As both $\widehat{\mathrm{Coker}}(\alpha_n)$ and $X(F_n)$ have no $\mathbb{Z}_p$-torsion, it is clear that $X(F_\infty)_{\Gamma_n}$ is a free $\mathbb{Z}_p$-module. $\Box$

Proof of theorem 1 : We shall show that the exact sequence (7) and lemma 10 imply theorem 1. By considering the $\mathbb{Z}_p$-coranks of the terms in the exact sequence (7), we find that

$$corank_{\mathbb{Z}_p}\big(\mathrm{Coker}(\alpha_n)\big) - corank_{\mathbb{Z}_p}\big(\mathrm{Ker}(\alpha_n)\big) = r-1. \tag{8}$$

The left vertical map in the commutative diagram (c.d.) implies that

$$\begin{aligned} & corank_{\mathbb{Z}_p}\big(Sel_{\mathfrak{p}_1^\infty}(E/F_\infty)^{\Gamma_n}\big) \\ &= corank_{\mathbb{Z}_p}\big(\mathrm{Coker}(\alpha_n)\big) - corank_{\mathbb{Z}_p}\big(\mathrm{Ker}(\alpha_n)\big) + corank_{\mathbb{Z}_p}\big(Sel_{\mathfrak{p}_1^\infty}(E/F_n)\big) \\ &= r-1+corank_{\mathbb{Z}_p}\big(Sel_{\mathfrak{p}_1^\infty}(E/F_n)\big), \ \ [\text{by } \ (8)] \end{aligned}$$

i.e.,

$$rank_{\mathbb{Z}_p}\big(X(F_\infty)\big)_{\Gamma_n} = \lambda_n + r - 1. \tag{9}$$

By lemma 10, we can conclude that

$$\big(X(F_\infty)\big)_{\Gamma_0} \simeq \mathbb{Z}_p^{\lambda_0+r-1}.$$

In particular, we have

$$X(F_\infty)/(p,T) \simeq \big(\mathbb{Z}_p/p\big)^{\lambda_0+r-1} = \text{a finite module}.$$

Since (p,T) is the maximal ideal of $\mathbb{Z}_p[[T]] \simeq \Lambda$, theorem 1 follows from Nakayama's lemma (e.g., see pp. 126 of [La]) for compact Λ-modules. $\square$

7. Λ-*rank of* $X(F_\infty)$

We have shown in the preceding section that $X(F_\infty)$ is a finitely generated Λ-module. We want to compute its Λ-rank and its Λ-torsion submodule. By structure theory of Λ-modules [see (16) and 'General Lemma' near the end of this section], it will be enough to show that $(X(F_\infty))_{\Gamma_n}$ is a free $\mathbb{Z}_p$-module of rank $p^n.c$, where c is a constant independent of n. Then, the 'General Lemma' would imply that $X(F_\infty)$ is a free Λ-module of rank c. Since the $\mathbb{Z}_p$-rank of $(X(F_\infty))_{\Gamma_n}$ is $(\lambda_n + r - 1)$ by (9), we want to know how the λ_n's vary with n as we go along the tower of fields F_n over F_0.

Lemma 11 : $\lambda_{n+1} = p\lambda_n + (p-1)(r-1)$.

We prove lemma 11 using ideas from [H-M]. Let G be the Galois group $\mathrm{Gal}(F_{n+1}/F_n)$. It is obvious that G is a cyclic group of order p. Formula (3.3) in [H-M] implies that

$$\begin{aligned}&corank_{\mathbb{Z}_p}\big(Sel_{\mathfrak{p}_1^\infty}(F_{n+1})\big)\\ &= p.corank_{\mathbb{Z}_p}\big(Sel_{\mathfrak{p}_1^\infty}(F_n)\big) + (p-1)\mathrm{ord}_p\big(h_G(Sel_{\mathfrak{p}_1^\infty}(F_{n+1}))\big),\end{aligned}$$

where h_G denotes the Herbrand quotient. In our notation, the above formula becomes

$$\lambda_{n+1} = p.\lambda_n + (p-1)\mathrm{ord}_p\big(h_G(Sel_{\mathfrak{p}_1^\infty}(F_{n+1}))\big). \tag{10}$$

We will now calculate the Herbrand quotient of the Selmer group in the above expression, since it will determine the explicit relation between λ_{n+1} and λ_n. The second exact sequence in the commutative diagram (c.d.) of section 6 implies that

$$h_G(Sel_{\mathfrak{p}_1^\infty}(F_{n+1})) = \frac{h_G\big(H^1(G(F_S/F_{n+1}), E_{\mathfrak{p}_1^\infty})\big)}{\prod\limits_{v|p} h_G\big(H^1(F_{n+1,v}, E)_{\mathfrak{p}_1^\infty}\big)}. \tag{11}$$

We shall evaluate the numerator and the denominator in the above expression with the next three propositions. We shall adopt arguments of Hachimori and Matsuno who dealt with the cyclotomic situation. The following lemma simplifies the calculation of the right hand side of (11).

Lemma 12 : For $i = 1, 2$, we have

$$\begin{aligned}&(a) H^i\big(G, H^1(G(F_S/F_{n+1}), E_{\mathfrak{p}_1^\infty})\big) = H^i(G, E_{\mathfrak{p}_1^\infty}),\\ &(b) H^i\big(G, H^1(F_{n+1,v}, E)_{\mathfrak{p}_1^\infty}\big) = H^i\big(G, E(F_{n+1,v})\big)_{\mathfrak{p}_1^\infty}.\end{aligned}$$

Proof : (a) The Galois group $\mathrm{Gal}(F_S/F_{n+1})$ has p-cohomological dimension at most 2 (see Prop. 8.3.17 in [N-S-W]). Combining this with corollary 6, we conclude that $H^2(F_S/F_{n+1},\ E_{\mathfrak{p}_1^\infty})$ vanishes for $i \geq 2$. Then, we have a long exact Hochschild-Serre spectral sequence

$$\begin{aligned}&\ldots H^2(F_S/F_n,\ E_{\mathfrak{p}_1^\infty}) \longrightarrow H^1\big(G,\ H^1(F_S/F_{n+1},\ E_{\mathfrak{p}_1^\infty})\big) \longrightarrow H^3(G,\ E(F_{n+1})_{\mathfrak{p}_1^\infty})\\ &\longrightarrow H^3\big(F_S/F_n,\ E_{\mathfrak{p}_1^\infty}\big) \longrightarrow H^2\big(G,\ H^1(F_S/F_{n+1},\ E_{\mathfrak{p}_1^\infty})\big) \longrightarrow H^4\big(G,\ E(F_{n+1})_{\mathfrak{p}_1^\infty}\big)\\ &\longrightarrow H^4(F_S/F_n,\ E_{\mathfrak{p}_1^\infty})\ldots\end{aligned}$$

As G is a finite cyclic group, we have

$$H^i(G,\ A) = H^{i+2}(G,\ A) \quad \forall i \geq 0,$$

where A is any G-module. As $H^i(F_S/F_n,\ E_{\mathfrak{p}_1^\infty}) = 0$ for $i \geq 2$, this part of the lemma holds.

(b) The Galois group $\mathrm{Gal}(\bar{F}_{n+1,v}/F_{n+1,v})$ has strict cohomological dimension at most 2 (see Prop. 1 and 4, Ch.II in [Se]). Moreover, $H^2(F_{n+1,v}, E)$ is trivial because

$$H^2(F_{n+1,v}, E) = \varinjlim_{\substack{\mathbb{Q}_p \subset M \subset F_{n+1,v} \\ [M:\mathbb{Q}_p]<\infty}} H^2(M, E),$$

and by Tate local duality (see Ch.II prop. 16 in [Se]), $H^2(M, E)$ vanishes for any finite extension M of $\mathbb{Q}_p$. As in the previous proposition, we have a long exact Hochschild-Serre spectral sequence and we can conclude that

$$H^i\big(G, H^1(F_{n+1,v}, E)\big)_{\mathfrak{p}_1^\infty} = H^{i+2}\big(G, E(F_{n+1,v})\big)_{\mathfrak{p}_1^\infty} \ \text{ for } \ i = 1, 2.$$

As $H^1(F_{n+1,v}, E)$ is a torsion group and G is cyclic, the above expression reduces to

$$H^i\big(G, H^1(F_{n+1,v}, E)_{\mathfrak{p}_1^\infty}\big) = H^i\big(G, E(F_{n+1,v})\big)_{\mathfrak{p}_1^\infty} \quad \text{for } \ i = 1, 2. \quad \square$$

Proposition 13 : $h_G\big(H^1(G(F_S/F_{n+1}), E_{\mathfrak{p}_1^\infty})\big) = \frac{1}{p}$.

Proof : By the first part of lemma 12,

$$h_G\big(H^1(G(F_S/F_{n+1}), E_{\mathfrak{p}_1^\infty})\big) = h_G(E_{\mathfrak{p}_1^\infty}).$$

Clearly, G acts trivially on $E_{\mathfrak{p}_1^\infty}$ as these points are defined over F_n. Let s be a generator of G and suppose $N = \sum_{i=o}^{p-1} s^i$. Then

$$\begin{aligned} H^2(G,\ E_{\mathfrak{p}_1^\infty}) &= (E_{\mathfrak{p}_1^\infty})^G / N(E_{\mathfrak{p}_1^\infty}) = 0, \\ H^1(G,\ E_{\mathfrak{p}_1^\infty}) &= \mathrm{Ker}(N)/(s-1)E_{\mathfrak{p}_1^\infty} = E_{\mathfrak{p}_1}. \end{aligned}$$

Therefore,

$$h_G\big(H^1(G(F_S/F_{n+1}), E_{\mathfrak{p}_1^\infty})\big) = h_G(E_{\mathfrak{p}_1^\infty}) = \frac{1}{p}. \quad \square$$

We calculate the denominator in (11) by proving the following two propositions.

Proposition 14 : $h_G\big(H^1(F_{n+1,v}, E)_{\mathfrak{p}_1^\infty}\big) = 1 \ \ \forall v \mid \mathfrak{p}_1$.

Proof : By the second part of lemma 12, we need to calculate the ratio of the order of $H^i\big(G, E(F_{n+1,v})\big)_{\mathfrak{p}_1^\infty}$ for $i = 2, 1$. We consider the following exact sequence of G-modules

$$0 \to \hat{E}(\mathfrak{m}_{n+1,v}) \to E(F_{n+1,v}) \to \tilde{E}_v(k_{n+1,v}) \to 0, \tag{12}$$

where $\mathfrak{m}_{n+1,v}$ is the maximal ideal of $F_{n+1,v}$, and $k_{n+1,v}$ is the residue field. Taking G-cohomology, we have a long exact sequence

$$\begin{aligned} \ldots \longrightarrow H^1\big(G, \hat{E}(\mathfrak{m}_{n+1,v})\big)_{\mathfrak{p}_1^\infty} \longrightarrow H^1\big(G, E(F_{n+1,v})\big)_{\mathfrak{p}_1^\infty} \longrightarrow \\ H^1\big(G,\ \tilde{E}_v(k_{n+1,v})\big)_{\mathfrak{p}_1^\infty} \longrightarrow H^2\big(G, \hat{E}(\mathfrak{m}_{n+1,v})\big)_{\mathfrak{p}_1^\infty} \longrightarrow \ldots . \end{aligned} \tag{13}$$

For $v|\mathfrak{p}_1$, $F_{n+1,v}$ is deeply ramified. By a result of Coates and Greenberg (Theorem 3.1 in [C-G]), $H^i\big(G, \hat{E}(\mathfrak{m}_{n+1,v})\big) = 0\ \forall i \geq 1$. Moreover, $\tilde{E}_v(k_{n+1,v})$ is a torsion group and we can take the $\mathfrak{p}_1^\infty$-torsion inside the cohomology in (13). We now have

$$H^i\big(G, E(F_{n+1,v})\big)_{\mathfrak{p}_1^\infty} = H^i\big(G, \tilde{E}_v(k_{n+1,v})_{\mathfrak{p}_1^\infty}\big) \quad \text{for}\ \ i = 1, 2. \tag{14}$$

For $v|\mathfrak{p}_1$, $k_{n+1,v}$ is the residue field of a ramified $\mathbb{Z}_p$-extension of a finite extension of $\mathbb{Q}_p$, and hence $k_{n+1,v}$ is a finite field. Let us now consider the $\mathfrak{p}_1$-primary part in (12):

$$0 \to \hat{E}(\mathfrak{m}_{n+1,v})_{\mathfrak{p}_1^\infty} \to E(F_{n+1,v})_{\mathfrak{p}_1^\infty} = \mathbb{Q}_p/\mathbb{Z}_p \to \tilde{E}_v(k_{n+1,v})_{\mathfrak{p}_1^\infty} = \text{a finite module} \to 0.$$

But $\mathbb{Q}_p/\mathbb{Z}_p$ has no nontrivial finite quotient, and we deduce that $\tilde{E}_v(k_{n+1,v})_{\mathfrak{p}_1^\infty} = 0$. Therefore, $H^i\big(G, \tilde{E}_v(k_{n+1,v})_{\mathfrak{p}_1^\infty}\big)$=0. By lemma 12 (b) and (14), we now conclude that

$$H^i\big(G, H^1(F_{n+1,v}, E)_{\mathfrak{p}_1^\infty}\big) = 0\ \ \forall v \mid \mathfrak{p}_1 \quad \text{for}\ \ i = 1, 2.$$

In particular, the Herbrand quotient h_G is 1. $\square$

Proposition 15 : $h_G\big(H^1(F_{n+1,v}, E)_{\mathfrak{p}_1^\infty}\big) = \frac{1}{p}\ \ \forall v \mid \mathfrak{p}_2$.

Proof : We proceed as in the previous proposition. However, π is an automorphism of $\hat{E}$ for v not dividing π. Therefore, $H^i\big(G, \hat{E}(\mathfrak{m}_{n+1,v})\big)_{\mathfrak{p}_1^\infty} = 0\ \forall\ i \geq 0$. By (13),

$$H^i\big(G, E(F_{n+1,v})\big)_{\mathfrak{p}_1^\infty} = H^i\big(G, \tilde{E}_v(k_{n+1,v})\big)_{\mathfrak{p}_1^\infty}\ \ \forall i \geq 0. \tag{15}$$

As before, we can take the $\mathfrak{p}_1^\infty$-torsion inside the cohomology on the right hand side of (15). Since the extension $F_{n+1,v}$ is totally ramified over $F_{n,v}$, the Galois group G acts trivially on $\tilde{E}_v(k_{n+1,v})$. Clearly,

$$\begin{aligned} \mid H^1\big(G, \tilde{E}_v(k_{n+1,v})\big)_{\mathfrak{p}_1^\infty} \mid &= \mid Hom(G, \mathbb{Q}_p/\mathbb{Z}_p) \mid = p \\ \mid H^2\big(G, \tilde{E}_v(k_{n+1,v})\big)_{\mathfrak{p}_1^\infty} \mid &= \mid H^2(G, \mathbb{Q}_p/\mathbb{Z}_p) \mid = 1. \end{aligned}$$

From lemma 12 (b) and (15), it is now obvious that $h_G\big(H^1(F_{n+1,v}, E)_{\mathfrak{p}_1^\infty}\big) = \frac{1}{p}$. $\square$

We can now derive the relation between λ_{n+1} and λ_n, as stated in lemma 11. We substitute the values obtained by the three previous propositions in (11). We find that

$$h_G\big(Sel_{\mathfrak{p}_1^\infty}(F_{n+1})\big) = \frac{\frac{1}{p}}{(\frac{1}{p})^r} = p^{r-1},$$

recalling that r is the number of primes above $\mathfrak{p}_2$ in F_{n+1} for any n. Now, it follows from (10) that

$$\lambda_{n+1} = p\lambda_n + (p-1)(r-1).$$

This completes the proof of lemma 11.

Lemma 16 : $X(F_\infty)_{\Gamma_n}$ is a free $\mathbb{Z}_p$-module of rank $p^n(\lambda_0 + r - 1)$.

Proof : We already saw that $X(F_\infty)_{\Gamma_n}$ is a free $\mathbb{Z}_p$-module [c.f. lemma 10] of rank $(\lambda_n + r - 1)$ [c.f. (9)]. By using lemma 11 recursively, we obtain that

$$\lambda_n = p^n\lambda_0 + (r-1)(p^n - 1).$$

Substituting in (9), we find that

$$rank_{\mathbb{Z}_p}\big(X(F_\infty)\big)_{\Gamma_n} = p^n(\lambda_0 + r - 1). \qquad \square$$

We can now prove Theorem 2 with the following result about the structure of Λ-modules (the proof is included for the sake of completeness):

General Lemma : Let Y be a Λ-module such that Y_{Γ_n} is a free $\mathbb{Z}_p$-module of rank cp^n. Then Y is a free Λ-module of rank c.

Proof : Recall that $\Lambda \simeq \mathbb{Z}_p[[T]]$. By structure theory of finitely generated $\mathbb{Z}_p[[T]]$-modules, there is a homomorphism ψ of $\mathbb{Z}_p[[T]]$-modules

$$0 \longrightarrow A \longrightarrow Y \xrightarrow{\psi} N = \bigoplus \mathbb{Z}_p[[T]]^a \bigoplus \Big(\oplus_{i=1}^s \mathbb{Z}_p[[T]]/p^{n_i}\Big) \bigoplus \Big(\oplus_{j=1}^t \mathbb{Z}_p[[T]]/(f_j^{m_j})\Big) \longrightarrow B \longrightarrow 0, \tag{16}$$

where A and B are finite. For sufficiently large n, Γ_n acts trivially on the finite modules A and B. Therefore, $B^{\Gamma_n} = B$, $A_{\Gamma_n} = A$ for n sufficiently large. We can rewrite (16) as

$$0 \longrightarrow A \longrightarrow Y \longrightarrow \mathrm{Im}(\psi) \longrightarrow 0,$$
$$0 \longrightarrow \mathrm{Im}(\psi) \longrightarrow N \longrightarrow B \longrightarrow 0.$$

Therefore, we have exact sequences

$$\mathrm{Im}(\psi)^{\Gamma_n} \longrightarrow A_{\Gamma_n} \longrightarrow Y_{\Gamma_n} \longrightarrow \big(\mathrm{Im}(\psi)\big)_{\Gamma_n} \longrightarrow 0, \tag{17}$$

$$N^{\Gamma_n} \longrightarrow B^{\Gamma_n} \longrightarrow \big(\mathrm{Im}(\psi)\big)_{\Gamma_n} \longrightarrow N_{\Gamma_n} \longrightarrow B_{\Gamma_n} \longrightarrow 0. \tag{18}$$

By our assumption, it is now clear from (17) that $\big(\mathrm{Im}(\psi)\big)_{\Gamma_n}$ is a free $\mathbb{Z}_p$-modules of rank $p^n c$. From (18), we can now deduce that $a = c$ and N has no $\mathbb{Z}_p[[T]]$-torsion part (note that the order of B_{Γ_n} is bounded independent of n). Thus, $N = \mathbb{Z}_p[[T]]^c$. Therefore, $N^{\Gamma_n} = 0$ and $B^{\Gamma_n} \hookrightarrow \big(\mathrm{Im}(\psi)\big)_{\Gamma_n}$. Since $\big(\mathrm{Im}(\psi)\big)_{\Gamma_n}$ does not have any nontrivial finite $\mathbb{Z}_p$-submodule, $B^{\Gamma_n} = 0$ for all n. Thus, $B = 0$ and $\mathrm{Im}(\psi) = N = \mathbb{Z}_p[[T]]^c$. Now, $\mathrm{Im}(\psi)^{\Gamma_n} = 0$, and (17) implies that $A_{\Gamma_n} \hookrightarrow Y_{\Gamma_n}$. But Y_{Γ_n} does not have any nontrivial finite $\mathbb{Z}_p$-submodule. Thus, $A_{\Gamma_n} = 0$ for all n. Therefore, $A = 0$. We can now rewrite (16) as

$$Y \cong \mathbb{Z}_p[[T]]^c. \qquad \square$$

Proof of Theorem 2 : Theorem 2 follows directly from lemma 16 and the 'General Lemma' above. $\square$

We can conclude that when $F(E_{p^n})$ is abelian over K for all $n \geq 0$, the Pontrjagin dual $X\big(F(E_{p^\infty})\big)$ of the $\mathfrak{p}_1^\infty$-Selmer group of E over $F(E_{p^\infty})$ is a free $\mathbb{Z}_p[[T]]$-module of rank $\lambda_0 + r - 1$. In particular, it is true when E is defined over K as the abelian property is implied by theory of complex multiplication.

References

[C-G] Coates, J. and Greenberg, R.; *Kummer Theory for abelian varieties over local fields*, Invent. Math., vol. 124 (1996), pp. 129–174.

[C-H 1] Coates, J. and Howson, S.; *Euler Characteristics and Elliptic Curves*, Proc. Nat. Acad. Sci. U.S.A. vol. 94 (1997) no. 21, pp. 11115–11117.

[C-H 2] Coates, J. and Howson, S.; *Euler Characteristics and Elliptic Curves II*, J. Math. Soc. Japan vol. 53 (2001) no. 1, 175–235.

[C-S] Coates, J. and Sujatha, R.; *Galois Cohomology of Elliptic Curves*, [Tata Institute of Fundamental Research Lectures on Mathematics, 2000.]

[Gi 1] Gillard, R,; *Transformation de Mellin-Leopoldt des fonctions elliptiques*, J. Number Theory, vol. 25 (1987) no. 3, pp. 379–393.

[Gi 2] Gillard, R,; *Fonctions L p-adiques des corps quadratiques imaginaires et de leurs extensions abeliennes*, J. Reine Angew Math., vol. 358 (1985), pp. 76–91.

[Gr 1] Greenberg R.; *On the structure of certain Galois groups*, Inv. Math. vol. 72 (1978), pp. 85-99.

[Gr 2] Greenberg, R.; *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves, (Cetraro, 1997), Springer-Verlag, pp. 51–144.

[H] Howson, S.; Euler characteristics as invariants of Iwasawa modules (preprint).

[H-M] Hachimori, Y. and Matsuno, K.; *An Analogue of Kida's Formula for the Selmer Groups of Elliptic Curves*, J. Alg. Geometry 8 (1999) no 3 pp. 581–601.

[H-S] Hochschild G. and Serre, J.P.; *Cohomology of group extensions*, Trans. A.M.S., (1953) pp. 110–134.

[La] Lang, S.; Cyclotomic Fields, (1978) Springer-Verlag.

[Mi] Milne, J.S.; *Arithmetic Duality Theorems*, [Academic Press, 1986].

[N-S-W] Neukrich, J., Schmidt, A. and Wingberg, K.; Cohomology of Number Fields (1999) Springer

[P-R 1] Perrin-Riou, B.; *Arithmetique des courbes elliptiques et theórie d'Iwasawa*, memoire 17 de la Soc. Math. France (1984) France.

[P-R 2] Perrin-Riou, B., *'Foctions L p-adiques, theórie d'Iwasawa et points de Heegner'*, Bull. Soc. Math. France **115** (1987) 399–456.

[Se] Serre, J.P.; Galois Cohomology, (1997) Springer-Verlag.