Recent Results in the GL_2 Iwasawa Theory of Elliptic Curves without Complex Multiplication

Yoshihiro Ochi

Korea Institute for Advanced Study (KIAS)
207-43 Cheongryangri-dong, Dongdaemun-gu
Seoul 130-012, South Korea
Email: ochi@kias.re.kr

Abstract

Recently new results have been obtained in the GL_2 Iwasawa theory of elliptic curves without complex multiplication. This article is a survey of some of those results.
Mathematics Subject Classification: 11G05, 11R23
Keywords: Selmer groups, Iwasawa theory, p-adic Lie groups.

1 The Cyclotomic Case

The GL_2 Iwasawa theory of elliptic curves without complex multiplication was first studied by M. Harris ([**?**] 1979). Let us begin by recalling the basic arguments in the Iwasawa theory for an elliptic curve over the cyclotomic $\mathbb{Z}_p$-extension, which was begun by B. Mazur ([**?**] 1972). Let E be an elliptic curve defined over $\mathbb{Q}$. Although the arguments hold for any elliptic curve or even abelian variety defined over a number field, we restrict ourselves to elliptic curves over $\mathbb{Q}$ for the remarkable results obtained in this case. This class of elliptic curves has a distinguished property: Any elliptic curve over $\mathbb{Q}$ is modular (Taniyama-Shimura-Weil conjecture -[**?**] p.355- proven by A.Wiles-R.Taylor, C.Breuil-B.Conrad-F.Diamond-R.Taylor). Hence there is a dominant morphism of the modular curve $X_0(N)$ to E, defined over $\mathbb{Q}$, where N is the conductor of E. The Hasse-Weil L-function $L(E,s)$ is also assured to have analytic continuation to the complex plane ([**?**] Appendix C §16). Let us fix a prime number p. For an algebraic extension K of $\mathbb{Q}$ we define the p-Selmer group as usual:

$$\mathrm{Sel}(E/K)\{p\} := \ker(H^1(K, E_{p^\infty}) \to \prod_{v:\text{all primes of } K} H^1(K_v, E)) \tag{1}$$

where $E_{p^n} := \ker(E(\overline{\mathbb{Q}}) \overset{\times p^n}{\to} E(\overline{\mathbb{Q}}))$ and $E_{p^\infty} = \cup_n E_{p^n}$. Since we will never vary p, we omit $\{p\}$ from the notation. Then, as is well known, we have a short exact sequence:

$$0 \to E(K) \otimes \mathbb{Q}_p / \mathbb{Z}_p \to \mathrm{Sel}(E/K) \to TS(E/K)\{p\} \to 0 \tag{2}$$

where $TS(E/K)$ is the Tate-Shafarevich group of E/K ([**?**] X §4). It is conjectured that $TS(E/K)$ is finite, if K is a finite extension of $\mathbb{Q}$. Assuming this conjecture, for $K/\mathbb{Q}$ finite, we have the Mordell-Weil rank of $E(K)$ equal to the $\mathbb{Z}_p$-corank of $\mathrm{Sel}(E/K)$, which explains the importance of the Selmer group in arithmetic geometry. The celebrated conjecture of Birch and Swinnerton-Dyer then predicts that the rank is equal to $\mathrm{ord}_{s=1} L(E,s)$, which shows the mystery of the function.

Let μ_{p^n} be the group of all p^n-power roots of unity and $\mu_{p^\infty} = \cup_n \mu_{p^n}$. The Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_p \times \Delta$ where Δ is a finite abelian group of order equal to $p-1$. Hence there is an infinite Galois extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$ contained in $\mathbb{Q}(\mu_{p^\infty})$ such that $\Gamma := \mathrm{Gal}(\mathbb{Q}_\infty / \mathbb{Q}) \cong \mathbb{Z}_p$. This $\mathbb{Q}_\infty$ is called the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. For any profinite group $G = \varprojlim G_i$, where each G_i is a finite group, we define its completed group algebra (or Iwasawa algebra) as follows:

$$\Lambda(G) = \mathbb{Z}_p[[G]] := \varprojlim_i \mathbb{Z}_p[G_i]. \tag{3}$$

For a $\Lambda(G)$-module M, we define its Pontrjagin dual to be $M^\vee := \mathrm{Hom}_{cont,\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$, where "cont" means continous, and $M^+ := \mathrm{Hom}_\Lambda(M, \Lambda)$. We will also use the following abbreviation: $\mathrm{E}^i(M) = \mathrm{Ext}^i_\Lambda(M, \Lambda)$.

It is easily seen that $X = \mathrm{Sel}(E/\mathbb{Q}_\infty)^\vee$ is a finitely generated $\Lambda(\Gamma)$-module. The algebra $\Lambda(\Gamma)$ is isomorphic to the ring of formal power series of one variable $\mathbb{Z}_p[[T]]$ ([**?**], p223), and there is a structure theorem for finitely generated $\Lambda(\Gamma)$-modules, similar to the one for finitely generated abelian groups. To state it, let us first define the notion of "pseudo-null" module. Let R be a commutative ring of dimension d and M a finitely generated R-module. Then M is said to be *pseudo-null* if $dim_R(M) < d-1$. In the case that $R = \Lambda(\Gamma) = \mathbb{Z}_p[[T]]$, a pseudo-null module is nothing but a finite module. Then the structure theorem says that for any finitely generated $\Lambda(\Gamma)$-module M, there is a "pseudo-isomorphism":

$$M \sim \Lambda^r \oplus \bigoplus_{i=1}^{n} \Lambda/(f_i(T)^{n_i}) \oplus \bigoplus_{j=1}^{m} \Lambda/(p^{m_j}) \tag{4}$$

where f_i is a "Weierstrass" polynomial ([**?**] 5.3.29), and $\sim$ means there is a $\Lambda(\Gamma)$-homomorphism from M to $E(M)$ with pseudo-null (finite) kernel and cokernel. The invariant $\mu = \Sigma_{j=1}^m p^{m_j}$ is called the μ-invariant of M, and $\lambda = \Sigma_{i=1}^n n_i \mathrm{deg} f_i(T)$ is called the λ-invariant of M. If M is torsion, i.e., $r = 0$, then we define the "characteristic polynomial" of M by $F_M(T) := \prod_{j=1}^m p^{m_j} \prod_{i=1}^n f_i(T)^{n_i}$.

Mazur conjectured that X is torsion over $\Lambda(\Gamma)$ if E has good ordinary reduction at p. This has been proven by K. Kato:

Theorem 1.1 (Rubin, Kato) *$Sel(E/\mathbb{Q}_\infty)^\vee$ is torsion over $\Lambda(\Gamma)$ if E has good ordinary reduction at p.*

The theorem was proved by K. Rubin when E has complex multiplication ([**?**]). We write its characteristic polynomial $F_{sel}(T)$. Mazur and Swinnerton-Dyer constructed the p-adic L-function $L_{p-adic}(E, s)$, and showed that "essentially" $L_{p-adic} \in \Lambda(\Gamma)$ ([**?**]). There is a p-adic version of the conjecture of Birch and Swinnerton-Dyer ([**?**]), which claims "$\mathrm{ord}_{s=1} L_{p-adic}(E, s)$" equals the Mordell-Weil rank of $E(\mathbb{Q})$, where $\mathrm{ord}_{s=1} L_{p-adic}(E, s)$ is defined through the valuation in the discrete valuation ring $\Lambda(\Gamma)_\wp$ with a prime ideal $\wp$ of height one not containing p. The Main Conjecture is then stated as follows:

Conjecture 1.2 (Main Conjecture) *$(F_{sel}(T)) = (L_{p-adic})$ as ideals of $\Lambda(\Gamma)$.*

Kato has proved the following partial resolution of the Main Conjecture and (p-adic) Birch and Swinnerton-Dyer conjecture:

Theorem 1.3 ([?]) *(i) $L(E, 1) \neq 0 \Longrightarrow E(\mathbb{Q})$ is finite.*

(ii) $p^n L_{p-adic} \in (F_{sel}(T))$ for some integer $n \geq 0$.

(iii) The Mordell-Weil rank of $E(\mathbb{Q}) \leq \mathrm{ord}_{s=1} L_{p-adic}(E, s)$.

The proofs of the above results are highly technical with many ingenious ideas, in particular his Euler system ([**?**] for the definition of Euler system) coming from so-called "Beilinson elements" in the K-group "$K_2(X_0(N))$", and p-adic Hodge theory.

If the conjecture on the finiteness of the Tate-Shafarevic group for any number field is ture and E has good ordinary reduction at p, then it is proven that there are natural numbers λ, μ and ν independent of n such that $\#TS(E/\mathbb{Q}_n) = p^{\lambda n + \mu p^n + \nu}$ (the analogue of Iwasawa's similar theorem on the orders of the tower of ideal class groups, [**?**] 13.13). When E has supersingular reduction, it was said that "we do not even have a good guess"(R. Greenberg, [**?**]), but recently M. Kurihara has obtained the analogue in the supersingular case ([**?**]).

It is an interesting problem to ask whether $\mathrm{Sel}(E/\mathbb{Q}_\infty)$ has a nontrivial pseudo-null $\Lambda(\Gamma)$-submodule, i.e., nonzero finite submodule. If it has no finite submodule with $\mu = 0$, and is torsion over $\Lambda(\Gamma)$, then we have $\mathrm{Sel}(E/\mathbb{Q}_\infty) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$. For this problem, see [**?**], [**?**] and [**?**]. In particular it can happen that the Selmer group has a nonzero finite submodule.

2 p-adic Lie Extensions

We would like to have Iwasawa theory not only over a $\mathbb{Z}_p$-extension, but also over various other extensions. Noting that the additive group $\mathbb{Z}_p$ is a p-adic analytic group of dimension 1, we consider infinite Galois extensions whose Galois groups are p-adic analytic groups. A p-adic analytic (=Lie) group G is a group in the category of p-adic analytic varieties and hence is always nonsingular. Typical examples are $\mathbb{Z}_p^r$, $GL_n(\mathbb{Z}_p)$, $SL_n(\mathbb{Z}_p)$ or their closed subgroups. This generalization was already carried out firstly to $\mathbb{Z}_p^r$-extensions (e.g.,[**?**]). In the next section we will also consider non-abelian extensions. An extension of fields k_∞/k is a *p-adic Lie extension* if it is a Galois extension and the Galois group $\mathrm{Gal}(k_\infty/k)$ is a compact p-adic Lie group of positive dimension. If it is a pro-p Lie group, we say k_∞/k is a pro-p Lie extension. If G is a compact p-adic Lie group, then $\Lambda(G)$ is a complete Noetherian ring, and it has $\mathbb{Z}_p[G]$ dense in it as a subring ([**?**] 2.2.2 and 2.2.4). If G is a pro-p group, then the completed group algebra is a local ring with the maximal ideal $\mathfrak{M} = (p, I)$, where $I := \ker(\Lambda \overset{\text{natural}}{\to} \mathbb{Z}_p)$, and there is the Nakayama Lemma: For any pro-p compact Λ-module M, $M = \mathfrak{M}M$ implies $M = 0$, and $M/\mathfrak{M}M$ being finite implies M is a finitely generated Λ-module (see [**?**]).

Let E be an elliptic curve over a number field k. Assume K/k is finite. Then there is the following long exact sequence:

$$0 \to \mathrm{Sel}(E/K) \to H^1(G_S(K), E_{p^\infty}) \to \bigoplus_{v\in S} H^1(K_v, E)(p)$$

$$\to \mathrm{Sel}(K, T_pE)^\vee \to H^2(G_S(K), E_{p^\infty}).$$

where S is a finite set of places of K which contains all primes over p and all primes at which E has bad reduction, and $G_S(K) = \mathrm{Gal}(k_S/k)$, k_S denotes the maximal extension, unramified outside S, and finally

$$\mathrm{Sel}(K, T_pE) := \varprojlim_n \ker(H^1(K, E_{p^n}) \to \prod_{v:\text{all primes of } K} H^1(K_v, E)). \tag{5}$$

Let us assume E has good reduction at each prime over p. If each reduction is ordinary, we say E has good ordinary reduction *over* p. If $K = k_\infty$, then $\mathrm{Sel}(E/k_\infty) = \varinjlim_i \mathrm{Sel}(E/k_i)$. The basic conjecture here is the following:

Conjecture 2.1 *Assume k_∞/k is a p-adic Lie extension containing the cyclotomic $\mathbb{Z}_p$-extension of k. Then*

1. $H^2(G_S(k_\infty), E_{p^\infty}) = 0$.
2. $\varprojlim Sel(k_n, T_pE) = 0$.

The conjecture implies that if E has good ordinary reduction over p, then $\mathrm{Sel}(E/k_\infty)^\vee$ is a Λ-torsion module (see Theorem **??** in the next section).

3 GL_2 Iwasawa Theory

The cyclotomic $\mathbb{Z}_p$-extension of a number field k is contained in the field $k_{cycl} = k(\mathbb{G}_m[p^\infty])$ with finite index, where $\mathbb{G}_m[p^\infty]$ is all p-power torsion points of the multiplicative group scheme

$\mathbb{G}_m \otimes \bar{k}$. In the Iwasawa theory for elliptic curves we have an elliptic curve E over k. Hence it is natural to consider a tower of extensions:

$$k \subset k_0 = k(E_p) \subset k_1 = k(E_{p^2}) \subset \cdots \subset k_n = k(E_{p^{n+1}}) \subset \cdots \subset k(E_{p^\infty}) =: k_\infty. \tag{6}$$

By the Weil pairing we have $k_{cycl} \subset k_\infty$.

Theorem 3.1 $H^2(G_S(k_\infty), E_{p^\infty}) = 0$.

This follows from Iwasawa's theorem on the weak Leopoldt conjecture (see [**?**] 10.3.25 and [**?**] 4.7). Fixing a basis of T_pE we have a representation of $G_{\mathbb{Q}}$:

$$\rho : G_k \to \mathrm{Aut}(T_pE) = GL_2(\mathbb{Z}_p). \tag{7}$$

The kernel of ρ is $\mathrm{Gal}(\bar{k}/k_\infty)$, which is a normal closed subgroup, hence it is a p-adic Lie group and k_∞/k is a p-adic Lie extension with an embedding $G(k_\infty/k) \hookrightarrow GL_2(\mathbb{Z}_p)$. Assume that E has complex multiplication by an imaginary quadratic field K over which E is defined. Then it is known that $G(k_\infty/k) \hookrightarrow GL_2(\mathbb{Z}_p)^{ab} \cong \mathbb{Z}_p^2 \times N$ with finite index, where N is a finite abelian group. we have $G := G(k_\infty/k) \cong \mathbb{Z}_p^2 \times \Delta$ with a finite abelian group Δ. If we assume that $k = k_0$, then $\Delta = 0$. In this case $\Lambda = \mathbb{Z}_p[[G]] \cong \mathbb{Z}_p[[T, S]]$ and for any finitely generated Λ-module M there is the following structure theorem:

$$M \sim R \oplus \bigoplus_{i=1}^{n} \Lambda/(f_i(T,S)^{n_i}) \oplus \bigoplus_{j=1}^{m} \Lambda/(p^{m_j}) \tag{8}$$

where R is a reflexive module: $R^{++} = R$ ([**?**] V §1). This existence of a nice structure theorem makes things less difficult. Exploiting the Iwasawa theory of this case Coates and Wiles were able to manage to prove, among other things, the following

Theorem 3.2 ([?]) *Let E be an elliptic curve with complex multiplication by an imaginary quadratic field K. Assume E is defined over K. If $L(E,1) \neq 0$, then $E(\mathbb{Q})$ is finite.*

This is the first substantial result for the Birch and Swinnerton-Dyer's conjecture. For the idea and sketch of proof see [**?**], or [**?**] for more details. The Main Conjecture (see [**?**]) was proven by K. Rubin ([**?**]). B. Perrin-Riou proved the following

Theorem 3.3 ([?] 2.4) *Let E be as in the above theorem of Coates-Wiles. Assume $Sel(E/k_\infty)^\vee$ is Λ-torsion and assume also a "weak Leopoldt conjecture"(see the introduction of [?]). Then $Sel(E/k_\infty)^\vee$ has no nonzero pseudo-null Λ-submodule.*

As is seen from these, if E has complex multiplication with good ordinary reduction over p, quite a lot has been proven including the Main Conjecture ([**?**] or Rubin's article in [**?**]).

J. Coates writes in [**?**] (1984) that "In conclusion, I want to stress that there would be great interest in finding a formulation of the Main Conjecture for the Iwasawa module $\mathrm{Sel}(E/k_\infty)$, where $k_\infty = k(E_{p^\infty})$ and p is a prime above which E has ordinary reduction, when E does not admit complex multiplication" (Notation changed by the author). If E does not have complex multiplication, then a famous theorem of Serre says the image of ρ is open in $GL_2(\mathbb{Z}_p)$ ([**?**]), hence in particular the Galois group $\mathrm{Gal}(k_\infty/k)$ is not abelian. As a result the Iwasawa algebra $\Lambda(G)$ is not a commutative ring, which has been one of the difficulties in this Iwasawa theory. In [**?**] Harris established a basic framework of the theory with important results. Let G_0 be the Galois group $\mathrm{Gal}(k_\infty/k_0)$. Then G_0 is a uniform pro-p group ([**?**]). Let us recall the definition. A pro-p group G is called *powerful* if $[G,G] \subset G^p$ ($[G,G] \subset G^4$ if $p = 2$) and *uniform* if it is powerful and $P_i(G)/P_{i+1}(G) \overset{\times p}{\to} P_{i+1}(G)/P_{i+2}(G)$ is isomorpshim for any $i \geq 1$, where $\{P_i(G)\}$ are the lower central p-series defined by $P_1(G) = G$ and $P_{i+1}(G) = P_i(G)^p[P_i(G), G]$ for $i \geq 1$.

Putting $G_i := \mathrm{Im}(\rho_i : G_k \to \mathrm{Aut}(E[p^{i+1}]) = GL_2(\mathbb{Z}/p^{i+1}\mathbb{Z}))$, $\{G_i\}$ forms the lower central p-series for G_0.

One merit to have G uniform is that $\Lambda(G)$ is an integral domain, and Noetherian by Lazard, so that it has a quotient field (uniquely determined) $Q(\Lambda)$, and we define the Λ-rank of M to be $dim_{Q(\Lambda)}(M \otimes_\Lambda Q(\Lambda))$ for any finitely generated Λ-module M. Assume $k = k_0$ so that G is uniform. Harris showed the following in [**?**] and [**?**]:

- A finitely generated Λ-module M has rank r if and only if the $\mathbb{Z}_p$-rank of $M_{G(k_\infty/k_n)}$ is $p^{4rn} + O(p^{3n})$ for $n \gg 0$.
- If E has ordinary reduction over p, then for each n the natural map
$$\mathrm{Sel}(E/k_n) \to \mathrm{Sel}(E/k_\infty)^{G(k_\infty/k_n)} \tag{9}$$
has finite kernel and cokernel, the numbers of the generators of which are bounded independently of n.
- Let L_∞ be the maximal unramifiued abelian p-extension of k_∞. Then the Λ-module $\mathrm{Gal}(L_\infty/k_\infty)$ is finitely generated and torsion over Λ. (cf. [**?**] for another proof.)

Thanks to Theorem **??** we are able to determine the rank of other modules appearing in the long exact sequence:

$$0 \to \mathrm{Sel}(E/k_\infty) \to H^1(G_S(k_\infty), E_{p^\infty}) \to \bigoplus_{v\in S} H^1(k_{\infty,v}, E)(p) \to (\varprojlim \mathrm{Sel}(k_n, T_pE))^\vee \to 0.$$

Theorem 3.4 ([?], [?]) *If E has good ordinary reduction over p and $k = k_0$, then*

$$rk_\Lambda(H^1(G_S(k_\infty), E_{p^\infty})^\vee) = rk_\Lambda(\bigoplus_{v\in S} H^1(k_{\infty,v}, E)(p)^\vee) = [k : \mathbb{Q}]$$

where $\Lambda = \Lambda(G(k_\infty/k))$ and rk_Λ denotes the Λ-rank.

For this result it does not matter whether E has CM or not. Assume from now on that E has no complex multiplication and good ordinary reduction over p. Assume now also that $\mathrm{Sel}(E/k)$ is finite. Then $\mathrm{Sel}(E/k_{cycl})$ is cotorsion and the theorem of Perrin-Riou and P. Schneider tells that its characteristic polynomial $F_{sel}(T)$ has a value at $T = 0$ which is equal to $\chi(\Gamma, \mathrm{Sel}(E/k_{cycl})) = \#\mathrm{Sel}(E/k_{cycl})^\Gamma/\#\mathrm{Sel}(E/k_{cycl})_\Gamma$ also p-adically approximating the value $L(E, 1)$ ([**?**] 4.1). Coates and S. Howson have calculated $\chi(G, \mathrm{Sel}(E/k_\infty)) = \prod_{i=0}^4 (\#H^i(G, \mathrm{Sel}(E/k_\infty)))^{(-1)^i}$ under the same assumption but $k = k_0$ need not be assumed. The result they have obtained is similar to $\chi(\Gamma, \mathrm{Sel}(E/k_{cycl}))$:

Theorem 3.5 ([?]) *Under the assumptions above,*

$$\chi(G, Sel(E/k_\infty)) = \#TS(E/k)\{p\} \prod_{\nu|p} |\#\tilde{E}(k_v)|_p^{-2}/(\#E(k)\{p\})^2 \times \prod_v |c_v|_p^{-1} \times \prod_{v\in S} |L_v(E, 1)|_p.$$

For the notation we would like the reader to refer to their paper [**?**]. This result indicates some still hidden connection of this theory with a p-adic L-function. The next theorem on the Selmer group is the following due to Greenberg:

Theorem 3.6 ([?] Theorem 6) $dim_{\mathbb{Q}_p}(Sel(E/k_\infty)^\vee \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = \infty$.

For a proof see the Appendix in [**?**]. Note that $dim_{\mathbb{Q}_p}(\mathrm{Sel}(E/k_{cycl})^\vee \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) < \infty$ if it torsion as is seen from the structure theorem. In particular shows that we have always $\mathrm{Sel}(E/k_\infty) \neq 0$. Another one is:

Theorem 3.7 ([?]) *If E does not have CM and $G = G(k_\infty/k)$ has no p-torsion elements, and $Sel(E/k_\infty)^\vee$ is torsion over $\Lambda(G)$, its $\Lambda(G)$-projective dimension is 2.*

In lack of a good structure theorem, as an alternative approach there is U. Jannsen's homotopy theory of Iwasawa modules, in particular Galois groups as Iwasawa modules (the classical case). Results obtained in [**?**], [**?**] and [**?**] depend on the work of Jannsen and its applications to the Iwasawa theory of elliptic curves. Jannsen defines the stable category of finitely generated Λ-modules and on the category a few functors are defined (see [**?**], [**?**] V or [**?**]). Here we are only interested in the "transpose functor" D. Using this functor we have the following exact sequence:

$$0 \to \mathrm{E}^1(DM) \to M \to M^{++} \to \mathrm{E}^2(DM) \to 0. \tag{10}$$

It turns out that $\mathrm{E}^1(DM)$ is the set of all torsion elements in M (note M^{++} is torsion free). For the study of Iwasawa modules in commutative cases, the notion of "pseudo-null module" plays an important role, as is seen above. It was missing in the noncommutative case but O. Venjakob has succeeded in giving the generalized definition of "pseudo-null" module in his Heidelberg PhD thesis [**?**] with a help of previous work of J-E. Björk. Let Λ be a Noetherian ring with finite global dimension $d = gl.dim(\Lambda) < \infty$. According to [**?**] 1.5, M has a canonical filtration of Λ-modules:

$$\mathrm{T}_0(M) \subset \mathrm{T}_1(M) \subset \cdots \subset T_{d_1}(M) \subset T_d(M) = M. \tag{11}$$

Then the number $\delta := \min\{i | T_i(M) = M\}$ is defined to be the dimension of M and M is defined to *pseudo-null* if $dim(M) \leq d - 2$. These definitions coincide with the usual ones when Λ is commutative. For its applications to Iwasawa theory Venjakob has proved that the Iwasawa algebra $\Lambda(G)$ is an "Auslander regular ring" ([**?**] 1.5.27), where G is a compact p-adic analytic group without p-torsion elements. The notion and theory of pseudo-null modules being available in the GL_2 Iwasawa theory, the analogue of the theorem of Perrion-Riou (Theorem **??**) has been proved:

Theorem 3.8 ([?] 5.1) *Assume that $G = G(k_\infty/k)$ has no p-torsion elements and $Sel(E/k_\infty)^\vee$ is torsion over $\Lambda(G)$. Then it has no nonzero pseudo-null $\Lambda(G)$-submodule.*

This theorem brings the following

Theorem 3.9 ([?] 6.1) *Assume that $k = k_0$ and $Sel(E/k_{cycl})^\vee$ is torsion over $\Lambda(G(k_{cycl}/k))$ with μ-invariant equal to 0. Then $Sel(E/k_\infty)$ is torsion-free as a $\Lambda(H)$-module, where $H = \mathrm{Gal}(k_\infty/k_{cycl})$.*

It is Coates and Howson who showed that under the assumption in Theorem **??**, $\mathrm{Sel}(E/k_\infty)^\vee$ is finitely generated over $\Lambda(H)$ ([**?**] 6.4), and it was Coates' idea that Theorem **??** should hold.

Let us have a look at the structure theorem (**??**). It shows that any torsion-free $\mathbb{Z}_p[[T, S]]$-module is embedded into a reflexive module with a pseudo-null cokernel. We are also able to have this in our situation, for the exact sequence (**??**) says there is

$$M \hookrightarrow M^{++} \to \mathrm{E}^2(DM) \to 0. \tag{12}$$

It is proven that M^{++} is reflexive and for any finitely generated module M, and $\mathrm{E}^i(M)$ is pseudo-null for any $i \geq 2$ ([**?**] 3.3). From now on let G denote a compact p-analytic group without p-torsion elements and $\Lambda = \Lambda(G)$. The following was predicted by Coates: Any p-torsion finitely generated Λ-module should be isomorphic to an "elementary module" $\bigoplus_{j=1}^n \Lambda/p^{m_j}$ up to pseudo-null modules. Of course this is true in the commutative cases. Let $\Lambda - mod$ be the category of finitely generated Λ-modules. For this question Venjakob has obtained the following

Theorem 3.10 ([?] 1.5.37) *Let $\Lambda - mod(p)$ be the subcategory of $\Lambda - mod$ consisting of all p-torsion modules and $PN(\Lambda)(p)$ the subcategory of $\Lambda - mod(p)$ consisting of all pseudo-null submodules. Then in the quotient category $\Lambda - mod(p)/PN(\Lambda)(p)$ there is an isomorphism:*

$$M \equiv \bigoplus_{j=1}^{n} \Lambda/p^{m_j}.$$

Note that this isomorphism does not imply existence of Λ-homomorphism from M to $\bigoplus_{j=1}^{n} \Lambda/p^{m_j}$ with pseudo-null kernel and cokernel. There $\{m_j\}$ is determined uniquely and the number $\Sigma_{j=1}^{n} m_j$ is defined to be the μ-invariant of M. This μ-invariant behaves similarly as in the commutative cases. For more about this μ-invariant, see [?] 1.5.3.

After this, Schneider has succeeded in generalizing Venjakob's theorem to general torsion modules by showing that the Iwasawa algebra $\Lambda(G)$ satisfies the axioms of a general class of rings (noncommutative Krull rings) first studied by M. Chamarie and then by appealing to a structure theorem for those rings proven by Chamarie ([?]) (Email communication):

Theorem 3.11 (Chamarie, Schneider) *Let $\Lambda - mod(tor)$ be the subcategory of $\Lambda - mod$ consisting of all torsion modules and $PN(\Lambda)$ the subcategory of $\Lambda - tors$ consisting of all pseudo-null submodules. Then in the quotient category $\Lambda - mod(tor)/PN(\Lambda)$ every $\Lambda(G)$-torsion module M is isomorphic to a direct sum of cyclic modules:*

$$M \equiv \bigoplus_{j=1}^{n} \Lambda/\mathfrak{a}_j.$$

Recall that a (left) Λ-module M is cyclic if $M \cong \Lambda\alpha$ for some $\alpha \in \Lambda$. Again the isomorphism does not imply existence of Λ-homomorphism from M to $\bigoplus_{j=1}^{n} \Lambda/\mathfrak{a}_j$ with pseudo-null kernel and cokernel. What can be said from this is the isomorphism, say f, gives a morphism $M' \to \bigoplus_{j=1}^{n} \Lambda/\mathfrak{a}_j$ with a pseudo-null cokernel, where M' is some submodule of M with the pseudo-null quotient. Also f^{-1} gives $N \to M$ with a pseudo-null cokernel, where N is some submodule of $\bigoplus_{j=1}^{n} \Lambda/\mathfrak{a}_j$ with the pseudo-null quotient. Nonetheless these results seem to show at least a beginning of obtaining a good structure theorem and a Main Conjecture in the GL_2 Iwasawa theory.

4 Final Remarks

The books [?] and [?] (Chapters V and XI), Greenberg's article [?], and Iwasawa's paper [?] are recommended for original Iwasawa's theory. For a general introduction to Iwasawa theory for elliptic curves we recommend Greenberg's [?], Coates' article [?] and articles in Springer Lecture Notes (LNM) volume 1716 "Arithmetic Theory of Ellitpic Curves" ([?]).

The p-adic Tate module $\mathrm{T}_p E$ of an elliptic curve over k is a two-dimensional Galois representation of G_k. Iwasawa theory has been generalized to p-adic Galois representations coming from motives ([?], [?], [?], [?]). So it would be interesting to consider Iwasawa modules attached to p-adic representations over general p-adic Lie extensions. For this see [?], [?], [?] and [?].

References

[ATEC] J. Coates, R. Greenberg, K. A. Ribet, K. Rubin (authors), C. Viola (editor), Arithmetic Theory of Elliptic Curves, LNM 1716, Springer 1999.

[Ch] M. Chamarie, Springer Lecture Notes, 1029, pp283-310.

[Co1] J. Coates, *Elliptic curves and Iwasawa theory*, in Modular Forms (ed. R.A.Raskin, John Wiley & Sons), 51-73, 1984.

[Co2] J. Coates, *Fragments of the GL_2 Iwasawa theory of elliptic curve without complex multiplication*, in Arithmetic Theory of Elliptic Curves, LNM 1716, Springer 1999.

[CH] J. Coates and S. Howson, *Euler characteristics and elliptic curves II*, to appear in The Journal of the Mathematical Society of Japan, 53(1), pp 175-235, 2001.

[CP] J. Coates and B. Perrin-Riou, *On p-adic L-functions attached to Motives over $\mathbb{Q}$*, Advanced Studies in Pure Mathematics 17, Algebraic Number Theory-in honour of K. Iwasawa pp.23-54, 1989.

[CW] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent.Math. 39 (1977), 223-251.

[DSMS] J.D. Dixon, M.P.F. du Sautoy, A. Mann, D. Segal. Analytic Pro-p Groups, Cambridge Studies in Advanced Mathematics 61, Cambridge University Press, 2nd edition, 1999.

[Gr1] R. Greenberg, *Iwasawa theory for p-adic representations*, Advanced Studies in Pure Mathematics 17, Algebraic Number Theory-in honour of K. Iwasawa 97-137, 1989.

[Gr2] R. Greenberg, *Galois Theory for Selmer groups of Abelian Varieties*, preprint, available from his homepage www. math.washington.edu/$\tilde{g}$reenber/personal.html

[Gr3] R. Greenberg, *Iwasawa Theory-Past and Present*, available from his home page.

[Gr4] R. Greenberg, *Iwasawa theory for elliptic curves*, in Arithmetic of Elliptic Curves, LNM 1716, Springer, 1999, or also available from his homepage.

[Gr5] R. Greenberg, *Introduction to Iwasawa theory for elliptic curves*, available from his homepage.

[Ha1] M. Harris, *p-adic Representations arising from descent on abelian varieties*, Compositio Math., 39(1979), 177-245.

[Ha2] M. Harris, *Correction to "p-adic Representations arising from descent on abelian varieties"* , Compositio Math., 121(2000), 105-108.

[HM] Y. Hachimori and K. Matsuno, *On finite Λ-submodules of Selmer groups of elliptic curves*, Proc.Amer.Math.Soc. 128, pp 2539-2541, 2000.

[Ho] S. Howson, *Iwasawa theory of elliptic curves over p-adic Lie extensions*, PhD thesis, Cambridge University, 1998.

[Iw] K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*, Ann of Math., 98, 246-326, 1973.

[Ja] U. Jannsen, *Iwasawa modules up to isomorphism*, Advanced Studies in Pure Mathematics 17, Algebraic Number Theory-in honour of K. Iwasawa 171-207, 1989.

[Ka1] K. Kato, *Iwasawa theory and p-adic Hodge theory*, Kodai Math.J., 16 (1993), 1-31.

[Ka2] K. Kato, *Euler systems, Iwasawa theory, and Selmer groups*, Kodai Math.J., 22 (1999), 313-372.

[Ka3] K. Kato, Cambridge Kuwait Lectures, May 2000.

[Ka4] K. Kato, Fermat's Last Theorem (book, in Japanese) Nihon Hyouron Sha.

[Ku] M. Kurihara, *Iwasawa theory of elliptic curves with supersingular reduction* (in Japanese), research report.

[La] M. Lazard, *Groupes analytiques p-adiques*, Publ. Math. I. H. E. S., 26, 1965.

[Ma] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math., 18 (1972), 183-226.

[MS-D] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math.25 (1974), 1-61.

[MTT] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogue of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math., 84 (1986), 1-48.

[Ng] T. Nguyen-Quang-Do, *Formations de classes et modules d'Iwasawa*, in Number Theory Noordwigerhout 1983, LNM 1068, Spinger 1984.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Springer 2000.

[Oc] Y. Ochi, *Iwasawa modules via homotopy theory*, PhD thesis, University of Cambridge, 1999.

[OV1] Y. Ochi and O. Venjakob, *On the structure of Selmer groups over p-adic Lie extensions*, to appear in Journal of Algebraic Geometry.

[OV2] Y. Ochi and O. Venjakob, *On the rank of Iwasawa modules over p-adic Lie extensions*, preprint.

[Pe] B. Perrin-Riou, *Groupe de Selmer d'une courbe elliptique a multiplication complexe*, Compo. Math., vol. 43 (1981), 387-417.

[Ru1] K. Rubin, *On the main conjecture of Iwasawa theory for imaginary quadratic fields*, Invent. Math.,93 (1988), 701-713.

[Ru2] K. Rubin, *The "main conjecture" of Iwasawa theory for imaginary quadratic fields*, Invent. Math.,103 (1991), 25-68.

[Sc1] P. Schneider, *Iwasawa L-functions of varieties over algebraic number fields, a first approach*, Invent. Math. 71 (1983), 251-293.

[Sc2] P. Schneider, *Motivic Iwasawa theory*, Advanced Studies in Pure Mathematics 17, Algebraic Number Theory-in honour of K. Iwasawa pp.421-456, 1989.

[Se] J-P. Serre, Abelian ℓ-adic Representations and Elliptic Curves, Benjamin, New York, 1968.

[dS] E. de Shalit, Iwasawa Theory of Elliptic Curves with Complex Multiplication, Academic Press (1987).

[Si] J. Silverman, The Arithmetic of Ellipitic Curves, Springer 1986.

[Su] R. Sujatha, *Euler-Poincare characteristics of p-adic Lie groups and arithmetic*, preprint, 2000.

[Ve] O. Venjakob, *Iwasawa theory of p-adic Lie extensions*, Dissertation, University of Heidelberg, 2000.

[Wa] L. C. Washington, Introduction to Cyclotomic Fields, Second Edition, Springer, 1997.