Abstract In this paper, we prove an analogue of Kida's formula for the fine Selmer groups of elliptic curves. We study the growth behaviour of the fine Selmer groups in p-power degree extensions of the cyclotomic $\mathbb{Z}_p$-extension of a number field and obtain a precise formula for the $\mathbb{Z}_p$ co-rank of the fine Selmer group of an elliptic curve. As an application, we prove an analogous Riemann-Hurwitz like formula in the false-Tate curve extension.

Keywords Iwasawa Theory, Fine Selmer groups, Herbrand quotient

Mathematics Subject Classification (2010) Primary 11R23

An Analogue of Kida's Formula for Fine Selmer Groups of Elliptic Curves

Debanjana Kundu

December 16, 2019

1 Introduction

The classical Riemann-Hurwitz formula describes the relationship of the Euler characteristics of two surfaces when one is a ramified covering of the other. Suppose $\pi : R_1 \to R_2$ is an n-fold covering of compact, connected Riemann surfaces and $g_1,\ g_2$ are their respective genus. The classical Riemann-Hurwitz formula is the statement

$$2g_2 - 2 = (2g_1 - 2)n + \sum (e(P_2) - 1)$$

where the sum is over all points P_2 on R_2 and $e(P_2)$ denotes the ramification index of P_2 for the covering π [15, Chapter II Theorem 5.9]. An analogue of the above formula for algebraic number fields was proven in [10]. Kida's formula describes the change of Iwasawa λ-invariants in a p-extension in terms of the degree and the ramification index. In [8], Iwasawa proved this formula using the theory of Galois cohomology for extensions of $\mathbb{Q}$ which are not necessarily finite. More precisely,

Theorem. [8, Theorem 6] Let $p \geq 2$ and K be a number field. Let K_{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of K and $\mathcal{L}/K_{\mathrm{cyc}}$ be a cyclic extension of degree p, unramified at every infinite place of K_{cyc}. Assume that the classical μ-invariant, $\mu(K_{\mathrm{cyc}}) = 0$. Then

$$\lambda(\mathcal{L}) = p\lambda(K_{\mathrm{cyc}}) + \sum_w (e(w \mid v) - 1) + (p-1)(h_2 - h_1)$$

where w ranges over all non-p places of $\mathcal{L}$, h_i is the rank of the Abelian group $H^i(\mathcal{L}/K_{\mathrm{cyc}}, E_{\mathcal{L}})$, and $E_{\mathcal{L}}$ is the group of all units of $\mathcal{L}$.

D. Kundu
Department of Mathematics, University of Toronto
BA6290, St George Street
Toronto, ON, Canada
M5S 2E4
E-mail: dkundu@math.toronto.edu

In the study of rational points of Abelian varieties, the Selmer group plays a crucial role. In [12], Mazur introduced the study of the growth of the p-primary part of the Selmer group in the cyclotomic $\mathbb{Z}_p$-extension of number fields. In [4], Hachimori-Matsuno proved an analogue of Kida's formula for Selmer groups of elliptic curves in p-extensions of the cyclotomic $\mathbb{Z}_p$-extension of a number field. In [13], Pollack-Weston proved a similar statement for Selmer groups of a general class of Galois representations including the case of p-ordinary Hilbert modular forms and p-supersingular modular forms.

In [3], the study of the fine Selmer group was initiated. This subgroup of the classical Selmer group is known to better approximate the class group. It appears that not much work has been done in understanding the λ-invariant of fine Selmer groups. In Theorem 31, we use Galois cohomology to prove an analogue of Kida's formula for the fine Selmer group. The method of proof is similar to [4]; but at several places the computations are significantly different. In Section 5 we prove a corollary in the spirit of [1, Section 6.1] and [6]. In Section 6 we prove an analogue of Kida's formula for the fine Selmer groups in the false Tate curve extension.

2 Preliminaries

Let K be a number field and p be an odd prime. Let A be an Abelian variety defined over K and S be a finite set of primes of K including the archimedean primes, the primes where A has bad reduction and the primes of K above p. Fix an algebraic closure $\overline{K}/K$ and set $G_K = \mathrm{Gal}(\overline{K}/K)$. Denote by K_S the maximal subfield of $\overline{K}$ containing K which is unramified outside S and set the notation $G_S(K) = \mathrm{Gal}(K_S/K)$.

K_S contains the cyclotomic $\mathbb{Z}_p$-extension K_{cyc}, and $\Gamma = \mathrm{Gal}(K_{\mathrm{cyc}}/K)$ is a p-adic Lie group. Denote the n-th layer of the cyclotomic tower by K_n and write $\Gamma_n = \mathrm{Gal}(K_n/K)$. The completed group ring, $\mathbb{Z}_p[[\Gamma]] = \varprojlim \mathbb{Z}_p[\Gamma/\Gamma_n]$ is identified with $\Lambda(\Gamma) = \mathbb{Z}_p[[T]]$, by fixing a topological generator of Γ. This allows us to regard any $\mathbb{Z}_p[[\Gamma]]$-module as a $\Lambda(\Gamma)$-module.

For any finite extension L/K, define the p^∞-fine Selmer group of A as

$$R_{p^\infty}(A/L) = \ker\left(H^1(G_S(L), A[p^\infty]) \to \bigoplus_{v\in S(L)} H^1(L_v, A[p^\infty])\right).$$

This definition is independent of the choice of S. For a G_K-module M, we use the notation $H^*(L_v, M)$ for the Galois cohomology of the decomposition group at v. Then

$$R_{p^\infty}(A/K_{\mathrm{cyc}}) := \varinjlim R_{p^\infty}(A/L)$$

where the inductive limit ranges over finite extensions of L/K contained in K_{cyc}. The Pontryagin dual $Y_{p^\infty}(A/K_{\mathrm{cyc}}) = Y(A/K_{\mathrm{cyc}})$, is a finitely generated compact $\Lambda(\Gamma)$-module by the action of Γ on $Y(A/K_{\mathrm{cyc}})$.

Assume $Y(A/K_{\text{cyc}})$ is $\Lambda(\Gamma)$-torsion. This is conjectured to be always true. There exists a pseudo-isomorphism

$$Y(A/K_{\text{cyc}}) \to \bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{n_j})$$

with s, t, m_i, n_j non-negative integers and $f_j(T)$ irreducible distinguished polynomials in $\mathbb{Z}_p[T]$.

The λ-invariant and the μ-invariant are defined as follows

$$\lambda_A(K) := \sum_j n_j \deg(f_j(T)), \quad \mu_A(K) := \sum_i m_j,$$

The following conjecture was made in [3].

Conjecture A. Let E be an elliptic curve over a number field K. $Y(E/K_{\text{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module i.e. it is $\Lambda(\Gamma)$-torsion and $\mu_E(K) = 0$.

In [9], Kato proved $\Lambda(\Gamma)$-torsion-ness of the fine Selmer group for elliptic curves over $\mathbb{Q}$ and when $K/\mathbb{Q}$ is an Abelian extension. Suppose Conjecture A holds for $Y(E/K_{\text{cyc}})$. Since it is a Noetherian torsion $\Lambda(\Gamma)$-module, its $\mathbb{Z}_p$-rank is equal to $\lambda_E(K)$.

We record here a technical lemma due to Y. Ochi, a proof of which using spectral sequences is also mentioned in [3, Lemma 3.1].

Lemma 21 *Let K_{cyc}/K be the cyclotomic $\mathbb{Z}_p$-extension. Then $Y(E/K_{\text{cyc}})$ is $\Lambda(\Gamma)$-torsion if and only if $H^2(G_S(K_{\text{cyc}}), E[p^\infty])$ is trivial.*

3 Kida's Formula

We state the main theorem, and reduce the proof to the calculation of Herbrand quotients. For computational simplicity we assume $p \geq 5$. If $p = 3$, the proof goes through under the additional assumption that E/K is semi-stable.

3.1 Main Result

We restrict ourselves to the special case of elliptic curves. The main theorem proved in this paper is the following.

Theorem 31 *Let $p \geq 5$ be a prime. Let E be an elliptic curve defined over a number field, K, with good ordinary reduction at all primes in K above p. Let L/K be a Galois p-extension. Assume $Y(E/K_{\text{cyc}})$ is finitely generated as a $\mathbb{Z}_p$-module. Then $Y(E/L_{\text{cyc}})$ is finitely generated as a $\mathbb{Z}_p$-module. Also,*

$$\lambda_E(L) = [L_{\text{cyc}} : K_{\text{cyc}}]\lambda_E(K) + \sum_{w \in P_1} (e_{L_{\text{cyc}}/K_{\text{cyc}}}(w) - 1) + 2 \sum_{w \in P_2} (e_{L_{\text{cyc}}/K_{\text{cyc}}}(w) - 1)$$

where $e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w)$ *is the ramification index of* w *in* $L_{\mathrm{cyc}}/K_{\mathrm{cyc}}$ *and* P_1, P_2 *are sets of primes in* L_{cyc} *defined as*

$$P_1 = \{w,\ w \nmid p :\ E \text{ has split multiplicative reduction at } w\}$$
$$P_2 = \{w,\ w \nmid p :\ E \text{ has good reduction at } w,\ E(L_{\mathrm{cyc},w})[p] \neq 0\}.$$

Set $G = \mathrm{Gal}(L_{\mathrm{cyc}}/K_{\mathrm{cyc}})$. The first task in proving Theorem 31 is a reduction step. The following lemma shows it is enough to prove the main theorem for the case $G = \mathbb{Z}/p\mathbb{Z}$.

Lemma 32 *[11] Let* $K \subset L \subset M$ *be number fields such that* M/K *is a Galois* p*-extension. If Theorem 31 is true for any two extensions* M/L, M/K, L/K *it is true for the third one.*

Proof Let $v \nmid p$ be a prime in the cyclotomic $\mathbb{Z}_p$-extension, L_{cyc}. Let g be the number of primes above v in M_{cyc}. Since there is no p-extension of the residue field of L_{cyc} at v, $[M_{\mathrm{cyc}} : L_{\mathrm{cyc}}] = e_{M_{\mathrm{cyc}}/L_{\mathrm{cyc}}}(w)g$. Thus

$$[M_{\mathrm{cyc}} : L_{\mathrm{cyc}}](e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(v) - 1) = \sum_{w}(e_{M_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w) - e_{M_{\mathrm{cyc}}/L_{\mathrm{cyc}}}(w)).$$

Here on, assume $G = \mathrm{Gal}(L_{\mathrm{cyc}}/K_{\mathrm{cyc}}) = \mathbb{Z}/p\mathbb{Z}$. Since the definition of the p^∞-fine Selmer group is independent of S, we can choose it to include all primes of K that are ramified in L/K. Therefore, the maximal extension of L unramified outside $S(L)$ is in fact, K_S.

Proposition 33 *Let* $G = \mathbb{Z}/p\mathbb{Z}$. *Conjecture A holds for* $Y(E/K_{\mathrm{cyc}})$ *if and only if Conjecture A holds for* $Y(E/L_{\mathrm{cyc}})$.

Proof Consider the map

$$Y(E/L_{\mathrm{cyc}})_G \xrightarrow{\widetilde{\alpha}} Y(E/K_{\mathrm{cyc}}).$$

This map has a finite kernel and cokernel. Hence, Conjecture A holds for $Y(E/K_{\mathrm{cyc}})$ if and only if $Y(E/L_{\mathrm{cyc}})_G$ is finitely generated over $\mathbb{Z}_p$. Since $G = \mathbb{Z}/p\mathbb{Z}$, $R := \mathbb{Z}_p[G]$ is a local ring. The unique maximal ideal, $\mathfrak{m}$, is $pR + I_G$ where I_G is the augmentation ideal. Therefore we have an isomorphism,

$$Y(E/L_{\mathrm{cyc}})/\mathfrak{m} \simeq Y(E/L_{\mathrm{cyc}})_G/pY(E/L_{\mathrm{cyc}})_G.$$

By Nakayama lemma, $Y(E/L_{\mathrm{cyc}})_G$ is a finitely generated $\mathbb{Z}_p$-module if and only if $Y(E/L_{\mathrm{cyc}})/\mathfrak{m}$ is finite. By Nakayama lemma for compact local rings, the last statement is equivalent to $Y(E/L_{\mathrm{cyc}})$ being finitely generated over $\mathbb{Z}_p$ since G is a finite p-group.

With this the proof of the first part of Theorem 31 is complete.

3.2 Reduction to Calculation of Herbrand Quotients

This step is to reduce the proof to the calculation of Herbrand quotients. By hypothesis, $Y(E/K_{\text{cyc}})$ (and hence $Y(E/L_{\text{cyc}})$) is a finitely generated $\mathbb{Z}_p$-module. Thus,

$$\begin{aligned}\lambda_E(L) &= \text{corank}_{\mathbb{Z}_p}(R_{p^\infty}(E/L_{\text{cyc}}));\\ \lambda_E(K) &= \text{corank}_{\mathbb{Z}_p}(R_{p^\infty}(E/K_{\text{cyc}}))\\ &= \text{corank}_{\mathbb{Z}_p}(R_{p^\infty}(E/L_{\text{cyc}})^G)\end{aligned}$$

The last equality follows from the fact that $\ker\widetilde{\alpha}$ and $\text{coker}\,\widetilde{\alpha}$ are finite.

Recall some classical theory of $\mathbb{Z}_p$-modules from [8, Section 9]. Let G be a cyclic group of order p and M be a co-finitely generated $\mathbb{Z}_p[G]$-module. The Herbrand quotient is defined as follows

$$h_G(M) := \frac{\#H^2(G,M)}{\#H^1(G,M)}.$$

The following equation is known to hold (see [4, Page 589])

$$\text{corank}_{\mathbb{Z}_p}(M) = p\,\text{corank}_{\mathbb{Z}_p}(M^G) + (p-1)\,\text{ord}_p\left(h_G(M)\right).$$

In our case, $M = R_{p^\infty}(E/L_{\text{cyc}})$. This gives us the main formula which we will need to evaluate.

$$\lambda_E(L) = p\lambda_E(K) + (p-1)\,\text{ord}_p\left(h_G(R_{p^\infty}(E/L_{\text{cyc}}))\right). \tag{1}$$

4 Herbrand Quotient Calculation

The main goal is to calculate $h_G(R_{p^\infty}(E/L_{\text{cyc}}))$ obtained in Equation 1. Using the definition of fine Selmer groups and an elementary property of Herbrand quotients we have

$$h_G\left(R_{p^\infty}(E/L_{\text{cyc}})\right) = \frac{h_G\left(H^1(G_S(L_{\text{cyc}}), E[p^\infty])\right)}{h_G\left(\bigoplus_w H^1(L_{\text{cyc},w}, E[p^\infty])\right)}. \tag{2}$$

4.1 Simplify the Numerator

First simplify the numerator using the Hochschild-Serre spectral sequences.

Lemma 41 $h_G(H^1(G_S(L_{\text{cyc}}), E[p^\infty])) = h_G(E(L_{\text{cyc}})[p^\infty]) = 1.$

Proof The first equality follows, if for $i = 1,\ 2$ we can prove

$$H^i(G, H^1(G_S(L_{\text{cyc}}), E[p^\infty])) \simeq H^i(G, E(L_{\text{cyc}})[p^\infty]).$$

From [14], both $G_S(L_{\mathrm{cyc}})$ and $G_S(K_{\mathrm{cyc}})$ are known to have p-cohomological dimension at most 2. By hypothesis, Conjecture A holds for $Y(E/L_{\mathrm{cyc}})$. By Lemma 21, this is equivalent to $H^2(G_S(L_{\mathrm{cyc}}), E[p^\infty]) = 0$. Therefore for $i \geq 2$,

$$H^i(G_S(L_{\mathrm{cyc}}), E[p^\infty]) = H^i(G_S(K_{\mathrm{cyc}}), E[p^\infty]) = 0$$

By Hochschild-Serre spectral sequences, obtain the following exact sequence

$$\begin{aligned}\cdots \to H^2(G_S(K_{\mathrm{cyc}}), E[p^\infty]) \to H^1(G, H^1(G_S(L_{\mathrm{cyc}}), E[p^\infty])) \xrightarrow{f_1} H^3(G, E(L_{\mathrm{cyc}})[p^\infty]) \\ \to H^3(G_S(K_{\mathrm{cyc}}), E[p^\infty]) \to H^2(G, H^1(G_S(L_{\mathrm{cyc}}), E[p^\infty])) \xrightarrow{f_2} H^4(G, E(L_{\mathrm{cyc}})[p^\infty]) \\ \to H^4(G_S(K_{\mathrm{cyc}}), E[p^\infty]) \to \cdots\end{aligned} \tag{3}$$

From the above discussion, f_1, f_2 are isomorphisms. The first equality follows from noting that $H^i(G, E(L_{\mathrm{cyc}})[p^\infty]) = H^{i+2}(G, E(L_{\mathrm{cyc}})[p^\infty])$, as G is cyclic.

Finally, $h_G(E(L_{\mathrm{cyc}})[p^\infty]) = 1$ because $E(L_{\mathrm{cyc}})[p^\infty]$ is finite [7].

4.2 Simplify the Denominator

To simplify the denominator of Equation 2, we divide it into two cases, when $v \nmid p$ and when $v \mid p$. Rewrite

$$h_G\left(\bigoplus_{w \in S(L_{\mathrm{cyc}})} H^1(L_{\mathrm{cyc},w}, E[p^\infty])\right) = \bigoplus_{v \in S(K_{\mathrm{cyc}})} h_G\left(\bigoplus_{w|v} H^1(L_{\mathrm{cyc},w}, E[p^\infty])\right).$$

Lemma 42 *Let $v \in S(K_{\mathrm{cyc}})$ be a prime not above p. For $i = 1, 2$,*

$$H^i\left(G, \bigoplus_{w|p} H^1(L_{\mathrm{cyc},w}, E[p^\infty])\right) = \begin{cases} 0 & v \text{ splits in } L_{\mathrm{cyc}}/K_{\mathrm{cyc}} \\ H^i(G, E(L_{\mathrm{cyc},w})[p^\infty]) & \text{otherwise} \end{cases}$$

Proof When $w \mid v$ is totally split,

$$\bigoplus_{w|v} H^1(L_{\mathrm{cyc},w}, E[p^\infty]) \simeq H^1(K_{\mathrm{cyc},v}, E[p^\infty]) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G].$$

The right hand side is cohomologically trivial.

Now consider the non-split case.

The p-part of the Brauer group, $\mathrm{Br}(L_{\mathrm{cyc},w})[p^\infty] = 0$ [14, Ch II, Lemma 3]. Thus, the p-cohomological dimension of $L_{\mathrm{cyc},w}$ is 1. By the same argument, the p-cohomological dimension of $K_{\mathrm{cyc},v}$ is also 1. Applying the Hochschild-Serre spectral sequence gives an exact sequence like Equation 3. Thus,

$$H^i(G, H^1(L_{\mathrm{cyc},w}, E[p^\infty])) \simeq H^i(G, E(L_{\mathrm{cyc},w})[p^\infty]).$$

When $v \mid p$, the argument is less elementary. We have the following lemma.

Lemma 43 *Let $v \in S(K_{\mathrm{cyc}})$ be a prime lying above p. Then for $i = 1, 2$,*

$$h_G\left(\bigoplus_{w|v} H^1(L_{\mathrm{cyc},w}, E[p^\infty])\right) = 1$$

Proof If v splits completely in $L_{\mathrm{cyc}}/K_{\mathrm{cyc}}$, by the same argument as above,

$$H^i\left(G, \bigoplus_{w|v} H^1(L_{\mathrm{cyc},w}, E[p^\infty])\right) = 0.$$

We need to study the case when v does not split in the extension $L_{\mathrm{cyc}}/K_{\mathrm{cyc}}$.

The absolute Galois group of both $K_{\mathrm{cyc},v}$ and $L_{\mathrm{cyc},w}$ have p-cohomological dimension at most 2. Further, by Tate duality [2, Proof of Theorem 1.12]

$$H^2(L_{\mathrm{cyc},w}, E[p^\infty]) = H^2(K_{\mathrm{cyc},v}, E[p^\infty])) = 0.$$

Using a Hochschild-Serre spectral sequence argument as before, we have the following isomorphism for $i = 1, 2$,

$$H^i(G, H^1(L_{\mathrm{cyc},w}, E[p^\infty])) \simeq H^i(G, E(L_{\mathrm{cyc},w})[p^\infty]).$$

It is enough to show that $E(L_{\mathrm{cyc},w})[p^\infty]$ is finite. This will imply that the required Herbrand quotient is 1.

Let $\mathcal{F}$ be the formal group law of E. Then

$$0 \to \mathcal{F}(\mathfrak{m}_w)[p^\infty] \to E(L_{\mathrm{cyc},w})[p^\infty] \to \widetilde{E}(l_w)[p^\infty] \to 0,$$

where $\mathfrak{m}_w$ is the maximal ideal of $\mathcal{O}_{L_{\mathrm{cyc},w}}$ and l_w is the residue field. $\widetilde{E}$ is the reduction of E modulo $\mathfrak{m}_w$.

Since l_w is the residue field, it is finite and $\widetilde{E}(l_w)[p^\infty]$ is a finite group. Showing $\mathcal{F}(\mathfrak{m}_w)[p^\infty]$ is finite will finish the proof. The argument is identical to that of [5, Proposition 3.12, Page 459].

4.3 Putting it Together

The series of lemmas above simplifies Equation 2 to

$$h_G\left(R_{p^\infty}(E/L_{\mathrm{cyc}})\right) = \frac{1}{\bigoplus_{w \in S'(L_{\mathrm{cyc}})} h_G\left(E(L_{\mathrm{cyc},w})[p^\infty]\right)}. \tag{4}$$

Here, w runs over those primes of $S(L_{\mathrm{cyc}})$ which are not above p and which do not split in the extension $L_{\mathrm{cyc}}/K_{\mathrm{cyc}}$. Set $H_w = \mathrm{ord}_p(h_G(E(L_{\mathrm{cyc},w})[p^\infty]))$. Rewrite Equation 1 as

$$\lambda_E(L) = [L_{\mathrm{cyc}} : K_{\mathrm{cyc}}]\lambda_E(K) - (p-1)\sum_w H_w \tag{5}$$

4.4 Calculating H_w

Calculation of H_w is similar to that of [4]. We need to study the p-primary torsion points of E on the unramified $\mathbb{Z}_p$-extension of an ℓ-adic field. By the earlier computations, we can focus only on the case $p \neq \ell$. We record the result and refer the reader to [4, Corollary 5.2] for the proof.

Proposition 44 *For $w \in S'(L_{\mathrm{cyc}})$, we have*

$$H_w = \begin{cases} -1 & \text{if } w \in P_1 \\ -2 & \text{if } w \in P_2 \\ 0 & \text{otherwise} \end{cases}$$

where P_1, P_2 were defined in Theorem 31.

The proof of Theorem 31 is complete by plugging in the values of H_w in Equation 5.

5 Applications

Set up: Let K be a number field, E be an elliptic curve defined over K and p be an odd prime. Set the notation, $K_n = K(E[p^{n+1}])$, i.e. the field obtained by adjoining the p^{n+1}-torsion points of E to K. Set K_∞ to be the field obtained by adjoining all the p-power torsion points on E to K. Let $G_\infty = \mathrm{Gal}(K_\infty/K)$. When E has CM by an imaginary quadratic field, upon performing a finite base change, $G_\infty \simeq \mathbb{Z}_p^2$. The Galois group is Abelian, and it is a p-adic Lie group of dimension 2. When E does not have CM, G_∞ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$; the Galois group is a non-Abelian, p-adic Lie group of dimension 4.

Let E be an elliptic curve without CM. When $p \geq 5$ and $R_{p^\infty}(E/K_n^{\mathrm{cyc}})$ is co-finitely generated as a $\mathbb{Z}_p$-module, as $n \to \infty$,

$$\mathrm{corank}_{\mathbb{Z}_p}(R_{p^\infty}(E/K_n^{\mathrm{cyc}})) = O(p^{3n}).$$

In the CM case, under the same assumptions as above, as $n \to \infty$,

$$\mathrm{corank}_{\mathbb{Z}_p}(R_{p^\infty}(E/K_n^{\mathrm{cyc}})) = O(p^{n}).$$

These would follow from asymptotic results proved in [6, Lemma 3.4.1]. More precise results can be obtained using Theorem 31. The following result is in the spirit of [1, Proposition 6.9].

The proof in the CM and non-CM case are identical. We provide a proof in the non-CM case.

Proposition 51 *Assume the following*

1. $p \geq 5$
2. $G_\infty = \mathrm{Gal}(K_\infty/K)$ *is a pro-p group*
3. $Y(E/K_{\mathrm{cyc}})$ *is a finitely generated $\mathbb{Z}_p$-module.*

Let $r(n)$ be the number of primes of F_n^{cyc} not dividing p and at which E has split multiplicative reduction. Let m be the smallest non-negative integer such that

$$\mathrm{Gal}(K_\infty/K_n) = \ker\left(\mathrm{GL}_2(\mathbb{Z}_p) \xrightarrow{red} \mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})\right).$$

Then, for $n \geq m$,

$$\lambda_E(K_n^{\mathrm{cyc}}) = [\lambda_E(K_m^{\mathrm{cyc}}) + r(m)]p^{3(n-m)} - r(n).$$

Proof By hypothesis, Theorem 31 gives the formula

$$\lambda_E(K_n^{\mathrm{cyc}}) = [K_n^{\mathrm{cyc}} : K_m^{\mathrm{cyc}}]\lambda_E(K_m^{\mathrm{cyc}}) + \sum_{w \in P_1}(e_{n,m}(w) - 1).$$

The third term in the general formula gives no contribution for the extension K_n/K_m. $w \nmid p$, therefore $K_{n,w}^{\mathrm{cyc}}/K_{m,w}^{\mathrm{cyc}}$ is totally ramified. The assumptions force that E has split multiplicative reduction over $K_{n,w}^{\mathrm{cyc}}$ if and only if E has split multiplicative reduction over $K_{m,w}^{\mathrm{cyc}}$. P_1 is the set of those $r(n)$ primes of K_n^{cyc} which divide the $r(m)$ primes of K_m^{cyc}, do not divide p, and at which E has split multiplicative reduction. So,

$$\sum_{w \in P_1}(e_{n,m}(w) - 1) = [K_n^{\mathrm{cyc}} : K_m^{\mathrm{cyc}}]r(m) - r(n).$$

The formula follows from the choice of m.
Justification: for $n \geq m$, K_{n+1}/K_n has degree p^4. By Weil pairing, the intersection $K_n^{\mathrm{cyc}} \cap K_{n+1}$ is the field generated over K_n by the p^{n+2}-th roots of unity. Therefore, $[K_{n+1}^{\mathrm{cyc}} : K_n^{\mathrm{cyc}}] = p^3$ for all $n \geq m$. This finishes the proof.

6 Kida's Formula in the false Tate Curve Extension

We begin by recalling the definition of a false Tate curve extension. Let p be a fixed odd prime and K be a number field containing μ_p. The *false Tate curve extension* denoted $\mathcal{K}_\infty$ is obtained by adjoining the p-power roots of a fixed integer $m > 1$ to K_{cyc}, i.e.

$$\mathcal{K}_\infty = K\left(\mu_{p^\infty},\ m^{\frac{1}{p^n}} : n = 1, 2, \ldots\right).$$

The Galois group $\mathrm{Gal}\,(\mathcal{K}_\infty/K) \simeq \mathbb{Z}_p \rtimes \mathbb{Z}_p$. This is a non-Abelian p-adic Lie extension. Further, set $H_K = \mathrm{Gal}\,(\mathcal{K}_\infty/K_{\mathrm{cyc}})$.

Let E/K be an elliptic curve such that p is a prime of good reduction. Let S be any finite set of primes of K containing the Archimedean primes, the primes above p, the primes of bad reduction of E and primes dividing m. Then, $\mathcal{K}_\infty$ is an S-admissible extension in the sense of [3]. The fine Selmer group $R_{p^\infty}(E/\mathcal{K}_\infty)$ is defined as in Section 2. Throughout this section, assume Conjecture A holds for $Y(E/K_{\mathrm{cyc}})$.

The following theorem is well-known and follows from an analysis of the Fundamental Diagram in this setting.

Theorem 61 *[3, Theorem 4.11] Consider the notation as above, the dual fine Selmer group $Y(E/K_\infty)$ is a finitely generated $\Lambda(H_K)$-module.*

The following related conjecture was made in [3].

Conjecture B. With notation as introduced above, $Y(E/\mathcal{K}_\infty)$ is a finitely generated torsion $\Lambda(H_K)$-module.

Let G be a pro-p, p-adic Lie group without any elements of order p. The last condition can be guaranteed by taking $p \geq 5$. The Iwasawa algebra $\Lambda(G)$ is a left (and right) Noetherian local domain. If M is a finitely generated $\Lambda(G)$-module, the $\Lambda(G)$-rank of M is defined as

$$\operatorname{rank}_{\Lambda(G)} M = \sum_{i \geq 0} (-1)^i \operatorname{rank}_{\mathbb{Z}_p} H^i(G,\ M).$$

For finitely generated $\Lambda(H_K)$-modules, Coates-Howson proposed that $\Lambda(H_K)$-rank is the right analogue of the classical λ-invariant [1]. Before stating the next theorem, we need to introduce some more notation.

For the false Tate curve extension $\mathcal{K}_\infty/K$, define for $i \geq 0$,

$$\mathcal{Z}^i(E/\mathcal{K}_\infty) = \varprojlim_L H^i(G_S(L), T_p(E)),$$

where $T_p(E)$ is the Tate module associated to the elliptic curve. The natural map from $\mathcal{Z}^1(E/\mathcal{K}_\infty)$ to $\mathcal{Z}^1(E/K_{\mathrm{cyc}})$ induces a canonical map

$$\rho_K : \mathcal{Z}^1(E/\mathcal{K}_\infty)_{H_K} \to \mathcal{Z}^1(E/K_{\mathrm{cyc}}).$$

Let $T(K)$ be the set of primes of K_{cyc} which are ramified in $\mathcal{K}_\infty$. This set consists of primes of F_{cyc} which either divide p or divide m. Define the subsets

$$T_1(K) = \{w \in T(K_{\mathrm{cyc}}),\ w \nmid p :\ E \text{ has split multiplicative reduction at } w\}$$
$$T_2(K) = \{w \in T(K_{\mathrm{cyc}}),\ w \nmid p :\ E \text{ has good reduction at } w, E(K_{\infty,w})[p] \neq 0\}.$$

Theorem 62 *[3, Theorem 4.11] Let $\mathcal{K}_\infty$ be the false Tate curve extension of K and p be an odd prime such that E/K has good reduction at all primes above p. Suppose Conjecture A holds for $Y(E/K_{\mathrm{cyc}})$. Then*

$$\operatorname{rank}_{H_K}(Y(E/K_\infty)) + \operatorname{rank}_{\mathbb{Z}_p}(\operatorname{coker}(\rho_K)) = \lambda_E(K) + t_1(K) + 2t_2(K),$$

where $t_i(K) = \#T_i(K)$.

The main result of this section is the following. We remind the reader the definition of certain sets of primes made earlier

$$P_1(L) = \{w \in L_{cyc},\ w \nmid p :\ E \text{ has split multiplicative reduction at } w\}$$
$$P_2(L) = \{w \in L_{\mathrm{cyc}},\ w \nmid p :\ E \text{ has good reduction at } w, E(L_{\mathrm{cyc},w})[p] \neq 0\}.$$

Theorem 63 *Let p be fixed odd prime and K be a number field containing μ_p. Let L/K be a Galois extension of degree p. Consider the false Tate curve extensions $\mathcal{K}_\infty/K$ and $\mathcal{L}_\infty/L$. Assume Conjecture A holds for $Y(E/K_{\mathrm{cyc}})$. Then*

$$\begin{aligned}\operatorname{rank}_{H_L}\left(Y\left(E/\mathcal{L}_\infty\right)\right)+\operatorname{rank}_{\mathbb{Z}_p}\left(\operatorname{coker}\left(\rho_L\right)\right) &= p\operatorname{rank}_{H_K}\left(Y\left(E/\mathcal{K}_\infty\right)\right)\\ &\quad + p\operatorname{rank}_{\mathbb{Z}_p}\left(\operatorname{coker}\left(\rho_K\right)\right)\\ &\quad + \sum_{w\nmid m, w\in P_1(L)}\left(e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w)-1\right)\\ &\quad + 2\sum_{w\nmid m, w\in P_2(L)}\left(e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w)-1\right)\end{aligned}$$

Lemma 64 *With notation as in Theorem 63,*

$$\sum_{w\in P_i(L)}\left(e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w)-1\right)=pt_i(K)-t_i(L)+\sum_{w\in P_i(L),w\nmid m}\left(e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w)-1\right).$$

Proof Suppose v is a prime of K_{cyc} and $w \mid v$ be a prime of L_{cyc}. Observe that $v \in T_i(K)$ if and only if $w \in T_i(L)$. Further, since $w \nmid p$, the residue degree $f_w\left(L_{\mathrm{cyc}}/K_{\mathrm{cyc}}\right)=1$ for primes in $T_i(L)$. Thus,

$$\begin{aligned}\sum_{w\in P_i(L)}\left(e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w)-1\right) &= \sum_{w\in T_i(L)}\left(e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w)-1\right)\\ &\quad + \sum_{w\in P_i(L),w\nmid m}\left(e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w)-1\right)\\ &= pt_i(K)\ -t_i(L)\ +\sum_{w\in P_i(L),w\nmid m}\left(e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w)-1\right)\end{aligned}$$

We can now give a proof of the main theorem in this section.

Proof (Proof of Theorem 63) Theorem 62 for $\mathcal{L}_\infty/L$ yields,

$$\operatorname{rank}_{H_L}\left(Y\left(E/\mathcal{L}_\infty\right)\right)+\operatorname{rank}_{\mathbb{Z}_p}\left(\operatorname{coker}\left(\rho_L\right)\right)=\lambda_E(L)+t_1(L)+2t_2(L). \quad (6)$$

Using Theorem 31, it is possible to rewrite $\lambda_E(L)$,

$$\lambda_E(L)=p\lambda_E(K)+\sum_{w\in P_1(L)}\left(e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w)-1\right)+2\sum_{w\in P_2(L)}\left(e_{L_{\mathrm{cyc}}/K_{\mathrm{cyc}}}(w)-1\right). \quad (7)$$

On the other hand, by rearranging terms and multiplying throughout by p, Theorem 62 for $\mathcal{K}_\infty/K$ yields,

$$p\lambda_E(K)=p\operatorname{rank}_{H_K}\left(Y\left(E/\mathcal{K}_\infty\right)\right)+p\operatorname{rank}_{\mathbb{Z}_p}\left(\operatorname{coker}\left(\rho_K\right)\right)-pt_1(K)-2pt_2(K). \quad (8)$$

Substituting the formula in Lemma 64 and Equation 8 into Equation 7 and plugging this expression of $\lambda_E(L)$ into Equation 6 proves the theorem.

Acknowledgement

The author would like to thank Kumar Murty for many helpful discussions, Jim Arthur for his encouragement, past and present members of the GANITA Lab for listening to the details, Hannah Constantin, Malors Espinosa-Lara and Matthew Sunohara for being amazing sound boards, and Erick Knight for answering many questions.

References

1. Coates, J., Howson, S.: Euler characteristics and elliptic curves ii. Journal of the Mathematical Society of Japan **53**(1), 175–235 (2001)
2. Coates, J., Sujatha, R.: Galois cohomology of elliptic curves. Narosa (2000)
3. Coates, J., Sujatha, R.: Fine Selmer groups of elliptic curves over p-adic Lie extensions. Mathematische Annalen **331**(4), 809–839 (2005)
4. Hachimori, Y., Matsuno, K.: An analogue of Kida's formula for the Selmer groups of elliptic curves. J. Alg. Geom. **8**, 581–601 (1999)
5. Hachimori, Y., Venjakob, O.: Completely faithful Selmer groups over Kummer extensions. Documenta Math., Extra Volume: Kazuya Kato's Fiftieth Birthday pp. 443–478 (2003)
6. Harris, M.: p-adic representations arising from descent on abelian varieties. Compositio Mathematica **39**(2), 177–245 (1979)
7. Imai, H.: A remark on the rational points of Abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions. Proceedings of the Japan Academy **51**(1), 12–16 (1975)
8. Iwasawa, K.: Riemann-Hurwitz formula and p-adic Galois representations for number fields. Tohoku Mathematical Journal, Second Series **33**(2), 263–288 (1981)
9. Kato, K.: p-adic Hodge theory and values of zeta functions of modular forms. Astérisque **295**, 117–290 (2004)
10. Kida, Y.: ℓ-extensions of CM-fields and cyclotomic invariants. J. Number Theory **12**, 519–528 (1980)
11. Matsuno, K.: An analogue of Kida's formula for the p-adic L-functions of modular elliptic curves. Journal of Number Theory **84**(1), 80–92 (2000)
12. Mazur, B.: Rational points of Abelian varieties with values in towers of number fields. Inventiones mathematicae **18**(3-4), 183–266 (1972)
13. Pollack, R., Weston, T.: Kida's formula and congruences. Documenta Mathematica, Special **2006**, 615–630 (2006)
14. Serre, J.P.: Galois Cohomology. Springer Science & Business Media (2001)
15. Silverman, J.H.: The arithmetic of elliptic curves, vol. 106. Springer Science & Business Media (2009)