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

Debanjana Kundu

Mathematics Department, 1984, Mathematics Road, University of British Columbia, Vancouver, Canada, V6T1Z2

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 totally real number field and obtain a formula for the $\mathbb{Z}_p$ co-rank of the fine Selmer group of an elliptic curve.

Keywords: Iwasawa Theory, Fine Selmer groups, Herbrand quotient
2010 MSC: 11R23

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

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

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 [20, Chapter II Theorem 5.9]. An analogue

of the above formula for algebraic number fields was proven in [8]. Kida's formula describes the change of Iwasawa λ-invariants in a p-extension in terms of the degree and the ramification index. In [6], Iwasawa proved this formula using the theory of Galois cohomology for extensions of $\mathbb{Q}$ which are not necessarily finite. More precisely,

Theorem. [6, 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

$$\lambda(\mathcal{L}) = p\lambda\left(K_{\mathrm{cyc}}\right) + \sum_{w \nmid p} \Big(e\left(w \mid v\right) - 1 \Big) + (p-1)\left(h_2 - h_1\right)$$

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 $\mathcal{L}$.

In the study of rational points of Abelian varieties, the Selmer group plays a crucial role. In [14], 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 [3], 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 [17], 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 [2], the study of the fine Selmer group was initiated. This is a subgroup of the classical Selmer group which is known to better approximate the class group (see for example [9], [10], [11], [12]). It appears that not much work has been done in understanding the λ-invariant of fine Selmer groups; this

article is a modest attempt to fill the gap. The main result is Theorem 3.1, where we use Galois cohomology to prove an analogue of Kida's formula for the fine Selmer group. The proof is similar to [3, Theorem 3.1]; but at several places the computations are significantly different. Aside from the fact that we prove a Kida-like formula for different modules, there are two other key differences between our result and that of Hachimori-Matsuno: first, we have to restrict ourselves to totally real number fields. Second, our formula is not as neat. The precise reason for both of these will become clear in §4.2.

2. Preliminaries

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

The extension F_S contains the cyclotomic $\mathbb{Z}_p$-extension F_{cyc}, and $\Gamma = \mathrm{Gal}(F_{\mathrm{cyc}}/F) \simeq \mathbb{Z}_p$ is a p-adic Lie group (of dimension 1). Denote the n-th layer of the cyclotomic tower by F_n and write $\Gamma_n = \mathrm{Gal}(F_n/F)$. 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/F, define the p^∞-fine Selmer group of A as

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

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

$$R_{p^\infty}\left(A/F_{\mathrm{cyc}}\right) := \varinjlim R_{p^\infty}\left(A/F_n\right)$$

where the inductive limit ranges over finite extensions F_n/F.

Let $T = T_pA$ denote the Tate module of an Abelian variety. It is a finitely generated $\mathbb{Z}_p$-module, endowed with a continuous action of $G_S(F)$. Define the compact G-modules as follows

$$\mathcal{Z}^i\left(A/F_{\mathrm{cyc}}\right) = \varprojlim_{F_n} H^i\left(G_S(F_n), T\right), \text{ for } i = 0,\ 1,\ 2, \tag{1}$$

where the projective limit is taken with respect to the corestriction maps. These are the i-th **Iwasawa cohomology groups** which are $\Lambda(\Gamma)$-modules.

For a discrete p-primary (resp. compact pro-p) Abelian group M, its Pontryagin dual defined as

$$M^\vee = \mathrm{Hom}_{\mathrm{cont}}(M, \mathbb{Q}_p/\mathbb{Z}_p),$$

is a compact (resp. discrete) module over the Iwasawa algebra. The Pontryagin dual of the fine Selmer group $R_{p^\infty}\left(A/F_{\mathrm{cyc}}\right)^\vee$ will be written as $Y_{p^\infty}\left(A/F_{\mathrm{cyc}}\right)$, or simply $Y_A(F)$. It is a finitely generated compact $\Lambda(\Gamma)$-module by the action of Γ on $Y_A(F)$. Let G be a profinite group and W (resp. M) be a discrete (resp. compact) G-module. The profinite cohomology groups (resp. homology groups) of W (resp. M) play an important role in the study of modules over Iwasawa algebras and are denoted $H^i(G, W)$ (resp. $H_i(G, M)$). The subgroup of elements of W fixed by G is denoted W^G, and M_G is the largest quotient of M on which G acts trivially.

Assume $Y_A(F)$ is $\Lambda(\Gamma)$-torsion. This is conjectured to be always true. The Structure Theorm of (torsion) $\Lambda(\Gamma)$-modules guarantees that there exists a pseudo-isomorphism

$$Y_A(F) \to \bigoplus_{i=1}^{s} \Lambda/(p^{m_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{n_j})$$

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

$$\lambda_Y(F) := \sum_j n_j \deg(f_j(T)), \quad \mu_Y(F) := \sum_i m_j.$$

The following conjecture was made in [2].

Conjecture A. Let E be an elliptic curve over a number field F. The dual fine Selmer group, $Y_E(F)$ is a finitely generated $\mathbb{Z}_p$-module, i.e., it is $\Lambda(\Gamma)$-torsion with $\mu_Y(F) = 0$.

In [7], Kato proved $\Lambda(\Gamma)$-torsion-ness of the fine Selmer group for elliptic curves over $\mathbb{Q}$ and when $F/\mathbb{Q}$ is an Abelian extension. Suppose Conjecture A holds for $Y_E(F)$. Since it is a Noetherian torsion $\Lambda(\Gamma)$-module, its $\mathbb{Z}_p$-rank is equal to $\lambda_Y(F)$.

It is for this reason that we restrict ourselves to stating and proving our main result for elliptic curves. However, under appropriate assumptions an analogous statement should hold for Abelian varieties in general.

We record here two technical lemmas.

Lemma 2.1. *[16, Proposition 1.3.2] Let F_{cyc}/F be the cyclotomic $\mathbb{Z}_p$-extension. Then $Y_E(F)$ is $\Lambda(\Gamma)$-torsion if and only if $H^2\left(G_S\left(F_{\mathrm{cyc}}\right), E[p^\infty]\right)$ is trivial.*

Lemma 2.2. *Let M be a G-module and N a normal subgroup of G. Assume $H^i(G,M)$ and $H^i(N,M)$ vanish for all $i \geq 2$. Then*

$$H^i\left(G/N, H^1\left(N,M\right)\right) \simeq H^{i+2}\left(G/N, M\right),$$

via the transgression map.

3. Kida's Formula

We begin this section by stating the main result in [3].

Theorem. *Let $p > 2$ be a prime. Let E/F be an elliptic curve with good ordinary reduction at p. Further assume that the elliptic curve is semi-stable if $p = 3$. Let L/F be a Galois extension of degree a power of p. Assume that the Pontryagin dual of the classical Selmer group over F_{cyc}, written $X(E/F_{\mathrm{cyc}})$, is $\Lambda(\Gamma)$-torsion with $\mu_X(F) = 0$. Then, $X(E/L_{\mathrm{cyc}})$ is also $\Lambda(\Gamma)$-torsion with $\mu_X(L) = 0$. Furthermore, the λ-invariants of these modules, $\lambda_X(F)$ and $\lambda_X(L)$, satisfy the following formula:*

$$\lambda_X(L) = [L_{\mathrm{cyc}} : F_{\mathrm{cyc}}]\lambda_X(F) + \sum_{w \in P_1(L)} \big(e(w) - 1\big) + 2 \sum_{w \in P_2(L)} \big(e(w) - 1\big)$$

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

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

We remark that in the above theorem, the hypothesis on the reduction type at primes above p is crucial. We are now in a position to state the main theorem of this article, and reduce the proof to the calculation of Herbrand quotients. Throughout this section we assume that Conjecture A holds for $Y_E(F)$, i.e., $Y_E(F)$ is a finitely generated $\mathbb{Z}_p$-module. In particular, the elliptic curve analogue of the Weak Leopoldt Conjecture (WLC) holds, i.e.,

$$H^2\left(G_S\left(F_{\mathrm{cyc}}\right),\ E[p^\infty]\right) = 0.$$

Since the dual fine Selmer group is a Noetherian torsion $\Lambda(\Gamma)$-module, its $\mathbb{Z}_p$-rank is equal to $\lambda_Y(F)$.

3.1. Statement of the Theorem and a Reduction Step

The main theorem proved in this article is the following.

Theorem 3.1. *Let F be a totally real number field. Let $p > 2$ be a prime and E/F be an elliptic curve with good ordinary reduction at all primes above p. Further assume that the elliptic curve is semi-stable if $p = 3$. Let L/F be a finite Galois p-extension which is also totally real. If the dual fine Selmer group $Y_E(F)$ is finitely generated as a $\mathbb{Z}_p$-module then $Y_E(L)$ is also finitely generated as a $\mathbb{Z}_p$-module. Moreover,*

$$\lambda_Y(L) - \lambda_{\mathcal{Z}^1}(L) = [L_{\mathrm{cyc}} : F_{\mathrm{cyc}}] \left(\lambda_Y(F) - \lambda_{\mathcal{Z}^1}(F)\right) + \sum_{w \in P_1(L)} \big(e(w) - 1\big) + 2 \sum_{w \in P_2(L)} \big(e(w) - 1\big)$$

where $\mathcal{Z}^1(E/F_{\mathrm{cyc}})$ and $\mathcal{Z}^1(E/L_{\mathrm{cyc}})$ are the compact Iwasawa cohomology groups, $e(w) = e_{L_{\mathrm{cyc}}/F_{\mathrm{cyc}}}(w)$ is the ramification index of w in $L_{\mathrm{cyc}}/F_{\mathrm{cyc}}$, and $P_1(L)$, $P_2(L)$ are sets of primes in L_{cyc} defined as

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

The fact that E has good ordinary reduction at primes above p is used only in proving Lemma 4.3. Since the statement of Conjecture A is independent of the reduction type of the elliptic curve at p, we believe it might be possible to prove a result similar to the one above *without* assuming that E has good ordinary reduction at p.

Set the notation $G = \mathrm{Gal}(L_{\mathrm{cyc}}/F_{\mathrm{cyc}})$. The first step in proving this theorem is a reduction step. The reduction to cyclic groups of order p work because p-groups are nilpotent.

Lemma 3.2. *[13] Let $F \subset L \subset M$ be number fields such that M/F is a Galois p-extension. If Theorem 3.1 is true for any two extensions M/L, M/F, L/F it is true for the third one.*

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

$$\left[M_{\text{cyc}} : L_{\text{cyc}}\right]\left(e_{L_{\text{cyc}}/F_{\text{cyc}}}(v) - 1\right) = \sum_{w}\left(e_{M_{\text{cyc}}/F_{\text{cyc}}}(w) - e_{M_{\text{cyc}}/L_{\text{cyc}}}(w)\right).$$

This proves the lemma. □

From here on, we will assume $G = \text{Gal}(L_{\text{cyc}}/F_{\text{cyc}}) = \mathbb{Z}/p\mathbb{Z}$. Since the definition of the p-primary fine Selmer group is independent of S, we can choose it to include all primes of F that are ramified in L/F. Therefore, by our choice of S the maximal extension of L unramified outside $S(L)$ is F_S.

The next proposition is the fine Selmer variant of a well-known result of Iwasawa [5, Theorem 2]. This will finish the proof of the first part of the main theorem.

Proposition 3.3. *Assume that Conjecture A holds for $Y_E(F)$. Then Conjecture A holds for $Y_E(L)$.*

Proof. Consider the following commutative diagram:

$$\begin{array}{ccccc} 0 \longrightarrow R(E/F_{\text{cyc}}) & \longrightarrow & H^1(G_S(F_{\text{cyc}}), E[p^\infty]) & \longrightarrow & \bigoplus_{v\in S(F_{\text{cyc}})} H^1\left(F_{\text{cyc},v}, E[p^\infty]\right) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\ 0 \to R(E/L_{\text{cyc}})^G & \longrightarrow & H^1(G_S(L_{\text{cyc}}), E[p^\infty])^G & \longrightarrow & \left(\bigoplus_{w\in S(L_{\text{cyc}})} H^1\left(L_{\text{cyc},w}, E[p^\infty]\right)\right)^G \end{array}$$

Here, β, γ are the natural restriction maps. By the inflation-restriction sequence, $\ker(\beta) = H^1\left(G, E\left(L_{\text{cyc}}\right)[p^\infty]\right)$ and $\text{coker}(\beta) = H^2\left(G, E\left(L_{\text{cyc}}\right)[p^\infty]\right)$. Both $\ker(\beta)$ and $\text{coker}(\beta)$ are finite; indeed, if M is a $\mathbb{Z}_p[G]$-module of cofinite type, $H^i(G, M)$ is finite for $i = 1, 2$.

By Shapiro's Lemma, $\ker(\gamma_v) = \oplus_{w|v} H^1\left(G_v, E\left(L_{\mathrm{cyc},w}\right)[p^\infty]\right)$, for each v. Here, $G_v = \mathrm{Gal}(L_{\mathrm{cyc},w}/F_{\mathrm{cyc},v})$ is the decomposition group of G. The dual of $E\left(L_{\mathrm{cyc}}\right)[p^\infty]$ (resp. $E\left(L_{\mathrm{cyc},w}\right)[p^\infty]$) are finitely generated over $\mathbb{Z}_p$ and hence over $\Lambda(G)$ (resp. $\Lambda(G_v)$). The dual of the map α gives rise to the following map

$$Y_E(L)_G \xrightarrow{\alpha^\vee} Y_E(F)$$

where the kernel and cokernel are finitely generated $\mathbb{Z}_p$-modules. Since $Y_E(L)$ is compact, by the Nakayama's lemma for compact local rings it is finitely generated as a $\mathbb{Z}_p[G]$-module. But G is finite, so $Y_E(L)$ is a finitely generated $\mathbb{Z}_p$-module. Equivalently, Conjecture A holds for $Y_E(L)$. □

4. Proof via Calculation of Herbrand Quotients

In this section we will prove the remainder of the main theorem. We emphasize that even though the idea behind the proof is very similar to that of [3], the details are significantly different, specially in the simplification of the Herbrand quotient.

4.1. Reduction to Calculation of Herbrand Quotients

The next step is to reduce the proof to the calculation of the Herbrand quotient. Since we are assuming that $Y_E(F)$ (and hence $Y_E(L)$) is a finitely generated $\mathbb{Z}_p$-module, we have

$$\begin{aligned}
\lambda_Y(L) &= \mathrm{corank}_{\mathbb{Z}_p}\left(R\left(E/L_{\mathrm{cyc}}\right)\right); \\
\lambda_Y(F) &= \mathrm{corank}_{\mathbb{Z}_p}\left(R\left(E/F_{\mathrm{cyc}}\right)\right) \\
&= \mathrm{corank}_{\mathbb{Z}_p}\left(R\left(E/L_{\mathrm{cyc}}\right)^G\right)
\end{aligned}$$

The last equality is not obvious. It requires the restriction map, α to have a finite kernel and cokernel. This follows from an application of the Snake Lemma once we know $\ker(\beta)$, $\ker(\gamma)$ and $\mathrm{coker}(\beta)$ are finite. From

the proof of Proposition 3.3 above, we have $\ker(\beta)$ and $\operatorname{coker}(\beta)$ are finite. We are yet to show that $\ker(\gamma)$ is finite. When $v \nmid p$, it is obvious. When $v \mid p$, it follows from [18, Cor 2, page 130]. This can also be seen from the proof of Lemma 4.3.

Since we are assuming that both F and L are totally real number fields, the compact Iwasawa cohomology groups $\mathcal{Z}^1\left(E/F_{\text{cyc}}\right)$ and $\mathcal{Z}^1\left(E/L_{\text{cyc}}\right)$ are finitely generated $\mathbb{Z}_p$-modules [15, Page 30]. Now by similar arguments as above, we have

$$\begin{aligned}
\lambda_{\mathcal{Z}^1}(L) &= \operatorname{corank}_{\mathbb{Z}_p}\left(\mathcal{Z}^1\left(E/L_{\text{cyc}}\right)^\vee\right); \\
\lambda_{\mathcal{Z}^1}(F) &= \operatorname{corank}_{\mathbb{Z}_p}\left(\mathcal{Z}^1\left(E/F_{\text{cyc}}\right)^\vee\right) \\
&= \operatorname{corank}_{\mathbb{Z}_p}\left(\left(\mathcal{Z}^1\left(E/L_{\text{cyc}}\right)^\vee\right)^G\right).
\end{aligned}$$

4.1.1. Classical Theory of $\mathbb{Z}_p$-Modules

We recall some classical theory of $\mathbb{Z}_p$-modules (see [6, section 9]). Let G be a cyclic group of order p and M be a divisible $\mathbb{Z}_p[G]$-module of co-finite type. Write

$$M \simeq M_1^a \oplus M_{p-1}^b \oplus M_p^c \tag{2}$$

where each M_i is indecomposable and defined as

$$M_1 = \mathbb{Z}_p^\vee = \mathbb{Q}_p/\mathbb{Z}_p, \qquad M_{p-1} = I\left(\mathbb{Z}_p[G]\right)^\vee, \qquad M_p = \mathbb{Z}_p[G]^\vee.$$

We use the notation $I\left(\mathbb{Z}_p[G]\right)$ for the augmentation ideal. Note that $\mathbb{Z}_p = \mathbb{Z}_p[G]/I\left(\mathbb{Z}_p[G]\right)$.

For each torsion $\mathbb{Z}_p$-module T, define

$$\begin{aligned}
V(T) &:= \operatorname{Hom}_{\mathbb{Z}_p}\left(T, \mathbb{Q}_p/\mathbb{Z}_p\right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \\
&= T^\vee \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.
\end{aligned}$$

The map $T \mapsto V(T)$ is an exact contravariant functor from torsion $\mathbb{Z}_p$-modules into vector spaces over $\mathbb{Q}_p$. With this definition in hand, set

$$V_i = V(M_i), \qquad \pi_i : G \to \mathrm{GL}(V_i) \quad \text{for } i = 1,\ p-1,\ p.$$

Here π_1 is the *trivial representation* of G over $\mathbb{Q}_p$, π_{p-1} is the unique *faithful irreducible representation* of G over $\mathbb{Q}_p$, and

$$\pi_p = \pi_1 \oplus \pi_{p-1} = \pi_G \tag{3}$$

where π_G is the *regular representation* of G over $\mathbb{Q}_p$.

For the representation π of G on the space $V(M)$, from (2) we get

$$\pi = a\pi_1 \oplus b\pi_{p-1} \oplus c\pi_p. \tag{4}$$

The task is to compute the integers $a,\ b,\ c$.

Since G is cyclic of order p, the cohomology groups of G are Abelian groups of exponent p. The ranks $r_{n,i}$ of the Abelian groups $H^n(G, M_i)$ are

$$\begin{aligned} r_{1,1} = 1, \quad r_{1,p-1} = 0, \quad r_{1,p} = 0, \\ r_{2,1} = 0, \quad r_{2,p-1} = 1, \quad r_{2,p} = 0. \end{aligned}$$

Combining this with (2), one obtains

$$r\left(H^1(G, M)\right) = a, \qquad r\left(H^2(G, M)\right) = b.$$

The first and second cohomology groups of M are finite. Thus, the **Herbrand quotient** defined as follows

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

exists and equals p^{b-a}. Since (2) implies

$$M^G \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{a+c} \oplus (\mathbb{Z}/p\mathbb{Z})^b,$$

the $\operatorname{corank}_{\mathbb{Z}_p}(M^G) = a + c$. Rewrite (4) as

$$\begin{aligned}\pi &= a\pi_1 \oplus b\pi_{p-1} \oplus c\pi_p \\ &= (a+c)\pi_p \oplus (b-a)\pi_{p-1} \\ &= \operatorname{corank}_{\mathbb{Z}_p}(M^G)\pi_G \oplus \operatorname{ord}_p\left(h_G(M)\right)\pi_{p-1}.\end{aligned}$$

The second equality follows from (3). Now, comparing the degrees of the representations,

$$\operatorname{corank}_{\mathbb{Z}_p}(M) = p\operatorname{corank}_{\mathbb{Z}_p}(M^G) + (p-1)\operatorname{ord}_p\left(h_G\left(M\right)\right). \tag{5}$$

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

$$\lambda_Y(L) = p\lambda_Y(F) + (p-1)\operatorname{ord}_p\left(h_G\left(R\left(E/L_{\text{cyc}}\right)\right)\right). \tag{6}$$

4.2. Herbrand Quotient Calculation

We need to calculate $h_G\left(R\left(E/L_{\text{cyc}}\right)\right)$ that appeared in (6). Consider the following exact sequence obtained by Tate duality and the assumption that the elliptic curve analogue of the WLC holds.

$$0 \to R(E/L_{\text{cyc}}) \to H^1\left(G_S\left(L_{\text{cyc}}\right), E[p^\infty]\right) \to \bigoplus_w H^1\left(L_{\text{cyc},w}, E[p^\infty]\right) \to \mathcal{Z}^1\left(E/L_{\text{cyc}}\right)^\vee \to 0.$$

From the definition of fine Selmer groups and an elementary property of Herbrand quotients we have the following equality

$$h_G\left(R\left(E/L_{\text{cyc}}\right)\right) = \frac{h_G\left(H^1\left(G_S\left(L_{\text{cyc}}\right), E[p^\infty]\right)\right) \cdot h_G\left(\mathcal{Z}^1\left(E/L_{\text{cyc}}\right)^\vee\right)}{h_G\left(\bigoplus_w H^1\left(L_{\text{cyc},w}, E[p^\infty]\right)\right)}. \tag{7}$$

Unfortunately, it appears that even for specific examples evaluating the Herbrand quotient of $\mathcal{Z}^1\left(E/L_{\text{cyc}}\right)^\vee$ is hard. In our setting, $\mathcal{Z}^1\left(E/F_{\text{cyc}}\right)$ and $\mathcal{Z}^1\left(E/L_{\text{cyc}}\right)$ are finitely generated $\mathbb{Z}_p$-modules; it follows from (5) that

$$\frac{\lambda_{\mathcal{Z}^1}(L) - p\lambda_{\mathcal{Z}^1}(F)}{p-1} = \text{ord}_p\left(h_G\left(\mathcal{Z}^1\left(E/L_{\text{cyc}}\right)^\vee\right)\right). \tag{8}$$

4.2.1. Partially Simplifying the Numerator of (7)

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

Lemma 4.1. $h_G\left(H^1\left(G_S\left(L_{\text{cyc}}\right), E[p^\infty]\right)\right) = h_G\left(E\left(L_{\text{cyc}}\right)[p^\infty]\right) = 1.$

Proof. Note that the first equality will follow, if for $i = 1,\ 2$ we can prove

$$H^i\left(G, H^1\left(G_S\left(L_{\text{cyc}}\right), E[p^\infty]\right)\right) \simeq H^i\left(G, E\left(L_{\text{cyc}}\right)[p^\infty]\right). \tag{9}$$

Recall that we are assuming Conjecture A holds for $Y_E(F)$ (hence also for $Y_E(L)$). In particular, the dual fine Selmer group is $\Lambda(\Gamma)$-torsion. Equivalently, the analogue of the weak Leopoldt Conjecture holds, i.e.,

$$H^2\left(G_S\left(F_{\text{cyc}}\right), E[p^\infty]\right) = H^2\left(G_S\left(L_{\text{cyc}}\right), E[p^\infty]\right) = 0.$$

We know that $G_S\left(L_{\text{cyc}}\right)$ and $G_S\left(F_{\text{cyc}}\right)$ have p-cohomological dimension less than equal to 2, i.e.,

$$H^i\left(G_S\left(L_{\text{cyc}}\right), E[p^\infty]\right) = H^i\left(G_S\left(F_{\text{cyc}}\right), E[p^\infty]\right) = 0 \qquad \text{for } i \geq 3.$$

Now by Hochschild-Serre spectral sequences, we obtain the following exact sequence

$$\begin{array}{llll} \cdots & \to H^2\left(G_S\left(F_{\text{cyc}}\right), E[p^\infty]\right) & \to H^1\left(G, H^1\left(G_S\left(L_{\text{cyc}}\right), E[p^\infty]\right)\right) & \xrightarrow{f_1} \quad H^3\left(G, E\left(L_{\text{cyc}}\right)[p^\infty]\right) \\ & \to H^3\left(G_S\left(F_{\text{cyc}}\right), E[p^\infty]\right) & \to H^2\left(G, H^1\left(G_S\left(L_{\text{cyc}}\right), E[p^\infty]\right)\right) & \xrightarrow{f_2} \quad H^4\left(G, E\left(L_{\text{cyc}}\right)[p^\infty]\right) \\ & \to H^4\left(G_S\left(F_{\text{cyc}}\right), E[p^\infty]\right) & \to \cdots & \end{array} \tag{10}$$

From the above discussion, both $f_1,\ f_2$ are isomorphisms. Since G is cyclic we have $H^i\left(G, E\left(L_{\text{cyc}}\right)[p^\infty]\right) = H^{i+2}\left(G, E\left(L_{\text{cyc}}\right)[p^\infty]\right)$. Therefore, (9) follows, giving the first equality.

The second equality in the statement of the lemma follows from a well-known result of Imai which implies that $E(L_{\text{cyc}})[p^\infty]$ is finite (see [4]). Hence, the Herbrand quotient $h_G\left(E\left(L_{\text{cyc}}\right)[p^\infty]\right) = 1$ [18, Proposition 8, page 134]. □

4.2.2. Simplifying the Denominator of (7)

To simplify the denominator of (7), we divide it into two cases: when $v \nmid p$ and when $v \mid p$. First rewrite

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

Lemma 4.2. *Let $v \in S(F_{\mathrm{cyc}})$ be a prime not above p. For $i = 1, 2$, we have*

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

Proof. We divide the proof into two cases. When $w \mid v$ is *totally split*,

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

The right hand side is cohomologically trivial.

Consider the *non-split* case. Recall that the p-primary part of the Brauer group $\mathrm{Br}(L_{\mathrm{cyc},w})(p) = 0$ [19, 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 $F_{\mathrm{cyc},v}$ is also 1. An application of Hochschild-Serre spectral sequence gives a diagram similar to (10). From this we conclude

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

This finishes the proof of the lemma. □

When $v \mid p$, we have the following lemma.

Lemma 4.3. *Let $v \in S(F_{\mathrm{cyc}})$ be a prime lying above p. Then for $i = 1, 2$, the Herbrand quotient $h_G\left(\bigoplus_{w|v} H^1\left(L_{\mathrm{cyc},w}, E[p^\infty]\right)\right) = 1$*

Proof. When v *splits* completely in $L_{\mathrm{cyc}}/F_{\mathrm{cyc}}$, $H^i\left(G, \bigoplus_{w|v} H^1\left(L_{\mathrm{cyc},w}, E[p^\infty]\right)\right)$ is trivial using the same argument as above. We need to study the case when v *does not split* in the extension $L_{\mathrm{cyc}}/F_{\mathrm{cyc}}$.

The absolute Galois group of $F_{\mathrm{cyc},v}$ and $L_{\mathrm{cyc},w}$ have p-cohomological dimension at most 2. By Tate duality, $H^2(L_{\mathrm{cyc},w}, E[p^\infty]) = H^2(F_{\mathrm{cyc},v}, E[p^\infty])) =$

0 (see [1, Proof of Theorem 1.12]). Using the Hochschild-Serre spectral sequence argument we arrive at the following isomorphism for $i = 1, 2$,

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

Observe it is enough to show that $E(L_{\mathrm{cyc},w})[p^\infty]$ is finite. This is true by the main result in [4]. Therefore, the required Herbrand quotient is 1 by the same argument as in Lemma 4.1. □

4.2.3. Putting it Together

The series of lemmas above simplifies (7) to

$$h_G\left(R\left(E/L_{\mathrm{cyc}}\right)\right) = \frac{h_G\left(\mathcal{Z}^1\left(E/L_{\mathrm{cyc}}\right)^\vee\right)}{\bigoplus_{w\in S'(L_{\mathrm{cyc}})} h_G\left(E\left(L_{\mathrm{cyc},w}\right)[p^\infty]\right)}. \tag{11}$$

In the above equation, w runs over those primes of $S(L_{\mathrm{cyc}})$ which are not above p and which do not split in the extension $L_{\mathrm{cyc}}/F_{\mathrm{cyc}}$. For ease of notation, set $H_w = \mathrm{ord}_p\left(h_G\left(E\left(L_{\mathrm{cyc},w}\right)[p^\infty]\right)\right)$. We rewrite (6) as

$$\lambda_Y(L) = [L_{\mathrm{cyc}} : F_{\mathrm{cyc}}]\lambda_Y(F) + (p-1)\left(\mathrm{ord}_p\left(h_G\left(\mathcal{Z}^1\left(E/L_{\mathrm{cyc}}\right)^\vee\right)\right) - \sum_w H_w\right).$$

In view of (8), the above equation becomes

$$\lambda_Y(L) - \lambda_{\mathcal{Z}^1}(L) = [L_{\mathrm{cyc}} : F_{\mathrm{cyc}}]\left(\lambda_Y(F) - \lambda_{\mathcal{Z}^1}(F)\right) - (p-1)\sum_w H_w.$$

The final task to finish the proof of Theorem 3.1 is to explicitly solve for H_w.

4.2.4. Calculating H_w

The calculation of H_w is exactly as done in the paper of Hachimori and Matsuno [3, Section 5]. We need to study the p-primary torsion points of E in the unramified $\mathbb{Z}_p$-extension of an ℓ-adic field. By the computations we have done so far, we can focus only on the case $p \neq \ell$. We have the following result

Proposition 4.4. *[3, Corollary 5.2] Suppose that $p \geq 5$ or $p = 3$ and E is a semi-stable elliptic curve. For $w \in S'(L_{\mathrm{cyc}})$, we have*

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

where $P_1(L)$, $P_2(L)$ were defined in Theorem 3.1.

With this, the proof of the theorem is complete.

Acknowledgement

The author would like to thank Kumar Murty for many helpful discussions, Stephen Kudla and Jim Arthur for their 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. She is currently supported by the PIMS Postdoctoral fellowship and also thanks CRM Montreal for their hospitality. Finally, thanks are also due to the anonymous referee for their comments which helped improve the exposition.

References

[1] J. Coates and R. Sujatha. *Galois cohomology of elliptic curves.* Narosa, 2000.

[2] J. Coates and R. Sujatha. Fine Selmer groups of elliptic curves over p-adic Lie extensions. *Mathematische Annalen*, 331(4):809–839, 2005.

[3] Y. Hachimori and K. Matsuno. An analogue of Kida's formula for the Selmer groups of elliptic curves. *J. Alg. Geom.*, 8:581–601, 1999.

[4] H. Imai. 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.

[5] K. Iwasawa. On the μ-invariants of $\mathbb{Z}_\ell$-extensions, number theory. *Algebraic Geometry and Commutative Algebra*, pages 1–11, 1973.

[6] K. Iwasawa. Riemann-Hurwitz formula and p-adic Galois representations for number fields. *Tohoku Mathematical Journal, Second Series*, 33(2):263–288, 1981.

[7] K. Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004.

[8] Y. Kida. ℓ-extensions of CM-fields and cyclotomic invariants. *J. Number Theory*, 12:519–528, 1980.

[9] D. Kundu. Growth of fine Selmer groups in infinite towers. *Canadian Mathematical Bulletin*, pages 1–15, 2020.

[10] D. Kundu. Growth of Selmer groups and fine Selmer groups in uniform pro-p extensions. *Annales mathématiques du Québec*, pages 1–16, 2020.

[11] D. Kundu. Growth of p-fine Selmer groups and p-fine Shafarevich-Tate groups in $\mathbb{Z}/p\mathbb{Z}$ extensions. *J. Ramanujan Math. Soc*, to appear.

[12] M. F. Lim and V. K. Murty. The growth of fine Selmer groups. *arXiv preprint arXiv:1504.02522*, 2015.

[13] K. Matsuno. 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.

[14] B. Mazur. Rational points of Abelian varieties with values in towers of number fields. *Inventiones mathematicae*, 18(3-4):183–266, 1972.

[15] Y. Ochi and O. Venjakob. On the ranks of Iwasawa modules over p-adic Lie extensions. In *Math. Proc. Camb. Philos. Soc*, volume 135, pages 25–43. Cambridge University Press, 2003.

[16] B. Perrin-Riou. *Fonctions L p-adiques des représentations p-adiques*. Société mathématique de France, 1995.

[17] R. Pollack and T. Weston. Kida's formula and congruences. *Documenta Mathematica, Special*, 2006:615–630, 2006.

[18] J.-P. Serre. *Local fields*, volume 67 of *GTM*. Springer, 1979.

[19] J.-P. Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer, 2013.

[20] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *GTM*. Springer, 2009.