AN ANALOGUE OF KIDA'S FORMULA FOR FINE SELMER GROUPS FOR ELLIPTIC CURVES

DEBANJANA KUNDU

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 λ-invariants of the fine Selmer group of an elliptic curve.

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. Let $\pi : R_1 \to R_2$ be an n-fold covering of compact, connected Riemann surfaces and let $g_1,\ g_2$ be their respective genus. The classical Riemann-Hurwitz formula says

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

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 (cf [Sil09, Chapter II Theorem 5.9]). An analogue of the above formula is known for algebraic number fields [Kid80]. Kida's formula describes the change of Iwasawa λ-invariants in a p-extension in terms of the degree and the ramification index. Soon after, this formula was proven using the theory of Galois cohomology for extensions of $\mathbb{Q}$ which are not necessarily finite in [Iwa81]. More precisely,

Theorem. *[Iwa81, 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 $\mathcal{L}/K$ 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 $\mathcal{L}$ and h_i is the rank of the Abelian group $H^i(\mathcal{L}/K_{\mathrm{cyc}}, E_{\mathcal{L}})$; here $E_{\mathcal{L}}$ is the group of all units of $\mathcal{L}$.

In the study of rational points of Abelian varieties (in particular, elliptic curves), the Selmer group plays a crucial role. In [Maz72], the growth of the p-primary part of the Selmer group was studied in the cyclotomic $\mathbb{Z}_p$-extension of number fields. In [HM99], they proved an analogue of Kida's formula and described the behaviour of the Selmer groups of elliptic curves in p-extensions of the cyclotomic $\mathbb{Z}_p$-extension of a number field. Recently in [CS05], the study of a certain subgroup called the fine

Date: August 12, 2019.
2010 *Mathematics Subject Classification.* Primary 11R23.
Key words and phrases. Iwasawa Theory, Fine Selmer groups, Herbrand quotient.

Selmer group was initiated. This subgroup is known to better approximate the class group than the classical Selmer group. In Theorem 3.1, we use Galois cohomology theory to prove an analogue of Kida's formula for the fine Selmer group. Finally, in Section 6 we prove an interesting corollary.

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 $G_S(K) = \mathrm{Gal}(K_S/K)$.

The cyclotomic $\mathbb{Z}_p$-extension K_{cyc}/K is contained in K_S 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 $\Lambda = \mathbb{Z}_p[[T]]$, by fixing a topological generator of Γ. This allows us to regard any $\mathbb{Z}_p[[\Gamma]]$-module as a Λ-module.

For any extension L/K, define the p^∞-Selmer group of an Abelian variety, A, as

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

When $L = K_{\mathrm{cyc}}$, for the case $p \neq 2$ one may replace $S(L)$ with $S^f(L)$, the set of primes in L above the finite primes of S. For a G_K-module, M, we use the standard notation $H^*(L_v, M)$ for the Galois cohomology of the decomposition group at v. With the setting as above, 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. Indeed, it can be seen from the exact sequence

$$0 \to R_{p^\infty}(A/L) \to \mathrm{Sel}_{p^\infty}(A/L) \to \bigoplus_{v|p} A(L_v)\otimes \mathbb{Q}_p/\mathbb{Z}_p$$

One can also write

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

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

Before proceeding, recall some definitions of invariants associated to $Y(A/K_{\mathrm{cyc}})$. Assume $Y(A/K_{\mathrm{cyc}})$ is Λ-torsion. This is conjectured to be true irrespective of the reduction type of A at the primes above p. This is the analogue of the weak Leopoldt conjecture in the Abelian variety setting. There exists a pseudo-isomorphism (ie a homomorphism with a finite kernel and cokernel)

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

where s, t, m_i, n_j are non-negative integers and $f_j(T)$ are irreducible distinguished polynomials in $\mathbb{Z}_p[T]$. The λ-invariant and the μ-invariant are defined as

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

and the characteristic polynomial is defined as

$$\mathrm{char}_\Lambda(Y(A/K_{\mathrm{cyc}})) := p^{\mu_A(K)} \prod_j f_j(T)^{n_j}.$$

It is conjectured

Conjecture. *[CS05, Conjecture A] Let E be an elliptic curve defined over the number field, K. $Y(E/K_{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module ie it is Λ-torsion and $\mu_E(K) = 0$.*

Suppose Conjecture A holds for $Y(E/K_{\mathrm{cyc}})$. Since it is a Noetherian torsion Λ-module, its $\mathbb{Z}_p$-rank is equal to $\lambda_E(K)$.

The Pontryagin dual of the Selmer group (denoted $X(A/K_{\mathrm{cyc}})$) is also a finitely generated Λ-module with no assumption on the reduction type of A at the primes above p. It is conjectured that in the case of good ordinary reduction at primes above p, $X(A/K_{\mathrm{cyc}})$ is Λ-torsion [Maz72]. This conjecture of Mazur is known for elliptic curves defined over $\mathbb{Q}$ and when $K/\mathbb{Q}$ is an Abelian extension [Kat04]. There are examples of elliptic curves $E/\mathbb{Q}$, where at primes of good ordinary reduction, the μ-invariant of the dual Selmer group, $\mu(X(E/\mathbb{Q}_{\mathrm{cyc}})) > 0$.

The following lemma is due to Y. Ochi and a proof using spectral sequences is mentioned in [CS05, Lemma 3.1].

Lemma 2.1. *Let K_{cyc}/K be the cyclotomic $\mathbb{Z}_p$-extension. Then $Y(E/K_{\mathrm{cyc}})$ is Λ-torsion if and only if $H^2(G_S(K_{\mathrm{cyc}}), E[p^\infty])$ is trivial.*

3. Kida's Formula

In this section we mention 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 same proof goes through under the additional assumption that E/K is semi-stable.

3.1. Main Result.

From now on, we are interested in the special case of elliptic curves. The main theorem proved in this paper is the following.

Theorem 3.1. *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 $Y(E/K_{\mathrm{cyc}})$ is finitely generated as a $\mathbb{Z}_p$-module. Then $Y(E/L_{\mathrm{cyc}})$ is finitely generated as a $\mathbb{Z}_p$-module. Also,*

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

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

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

The fact that E has good ordinary reduction at primes above p is used only in proving Lemma 4.3.

Set the notation $G = \mathrm{Gal}(L_{\mathrm{cyc}}/K_{\mathrm{cyc}})$. The first step in proving this theorem 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 3.2. *[Mat00] Let $K \subset L \subset M$ be number fields such that M/K is a Galois p-extension. If Theorem 3.1 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 3.3. *Assume Conjecture A holds for $Y(E/K_{\mathrm{cyc}})$. Then Conjecture A holds for $Y(E/L_{\mathrm{cyc}})$.*

Proof. Consider the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & R_{p^\infty}(A/K_{\mathrm{cyc}}) & \longrightarrow & H^1(G_S(K_{\mathrm{cyc}}), E[p^\infty]) & \longrightarrow & \bigoplus_{v\in S^f(K_{\mathrm{cyc}})} H^1(K_{\mathrm{cyc},v}, E[p^\infty]) \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} \\ 0 & \longrightarrow & R_{p^\infty}(A/L_{\mathrm{cyc}})^G & \longrightarrow & H^1(G_S(L_{\mathrm{cyc}}), E[p^\infty])^G & \longrightarrow & \left(\bigoplus_{w\in S^f(L_{\mathrm{cyc}})} H^1(L_{\mathrm{cyc},w}, E[p^\infty])\right)^G \end{array}$$

Here, $\ker(\beta) = H^1(G, E(L_{\mathrm{cyc}})[p^\infty])$ and $\mathrm{coker}(\beta) = H^2(G, E(L_{\mathrm{cyc}})[p^\infty])$. Both are finite because for any $\mathbb{Z}_p[G]$-module M of cofinite type, $H^i(G, M)$ is finite for $i = 1, 2$.

For each v, $\ker(\gamma_v) = \oplus_{w|v} H^1(G_v, E(L_{\mathrm{cyc},w})[p^\infty])$. Here, $G_v = \mathrm{Gal}(L_{\mathrm{cyc},w}/K_{\mathrm{cyc},v})$ is the decomposition group. The dual of $E(L_{\mathrm{cyc}})[p^\infty]$ and $E(L_{\mathrm{cyc},w})[p^\infty]$ are finitely generated over $\mathbb{Z}_p$ and hence over $\Lambda(G)$ and $\Lambda(G_v)$ respectively. The dual of the map α gives rise to

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

where the kernel and cokernel are finitely generated $\mathbb{Z}_p$-modules. Since $Y(E/L_{\mathrm{cyc}})$ is compact, it is finitely generated as a $\mathbb{Z}_p[G]$-module by Nakayama lemma for compact local rings. But G is finite, so $Y(E/L_{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module. □

With this the proof of the first part of the main theorem is complete.

3.2. **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 $Y(E/K_{\mathrm{cyc}})$ (and hence $Y(E/L_{\mathrm{cyc}})$) is a finitely generated $\mathbb{Z}_p$-module, we have

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

The last equality is not obvious. It requires the restriction map, α to have a finite kernel and cokernel. From the proof of Proposition 3.3 above, we know that $\ker(\beta)$ and $\mathrm{coker}(\beta)$ are finite. We are yet to show that $\ker(\gamma)$ is finite. When $v \nmid p$, it is obvious. When $v \mid p$, it will follow from [Ser79, Cor 2, page 130]. This can also be seen from the proof of Lemma 4.3.

Before we proceed, we recall some classical theory of $\mathbb{Z}_p$-modules. The rest of this section is similar to [Iwa81, section 9].

Let G be a cyclic group of order p and M be a divisible $\mathbb{Z}_p[G]$-module of cofinite type. Write

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

where each M_i is indecomposable and defined as

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

$I(\mathbb{Z}_p[G])$ is the notation for the augmentation ideal and $(-)^\vee = \mathrm{Hom}_{\mathbb{Z}_p}(-, \mathbb{Q}_p/\mathbb{Z}_p)$ denotes the Pontryagin dual. Note that $\mathbb{Z}_p = \mathbb{Z}_p[G]/I(\mathbb{Z}_p[G])$.

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

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

Then $T \mapsto V(T)$ 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

$$\pi_p = \pi_1 \oplus \pi_{p-1} = \pi_G \tag{2}$$

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

For the representation π of G on the space $V(M)$, we get the following from Equation 1.

$$\pi = a\pi_1 \oplus b\pi_{p-1} \oplus c\pi_p. \tag{3}$$

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. One can check the ranks $r_{n,i}$ of the Abelian groups $H^n(G, M_i)$. We have

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

Combining this with Equation 1, one obtains

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

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 Equation 1 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 Equation 3 as

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

The second equation follows from Equation 2. Now, comparing the degrees of the representations,

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

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

$$\lambda_E(L) = p\lambda_E(K) + (p-1)\operatorname{ord}_p\left(h_G(R_{p^\infty}(E/L_{\mathrm{cyc}}))\right). \tag{4}$$

4. Herbrand Quotient Calculation

The goal of this section is calculate $h_G(R_{p^\infty}(E/L_{\mathrm{cyc}}))$ obtained in Equation 4. From the definition of fine Selmer groups and an elementary property of Herbrand quotients we have

$$h_G\left(R_{p^\infty}(E/L_{\mathrm{cyc}})\right) = \frac{h_G\left(H^1(G_S(L_{\mathrm{cyc}}), E[p^\infty])\right)}{h_G\left(\bigoplus_w H^1(L_{\mathrm{cyc},w}, E[p^\infty])\right)} \tag{5}$$

4.1. Simplify the Numerator.

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

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

Proof. Observe: the first equality follows, if for $i = 1,\ 2$ we can prove

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

By assumption, Conjecture A holds for $Y(E/L_{\mathrm{cyc}})$ equivalently by Lemma 2.1, $H^2(G_S(L_{\mathrm{cyc}}), E[p^\infty]) = 0$. $G_S(L_{\mathrm{cyc}})$ (and hence $G_S(K_{\mathrm{cyc}})$) has p-cohomological dimension 2, ie $H^i(G_S(L_{\mathrm{cyc}}), E[p^\infty]) = H^i(G_S(K_{\mathrm{cyc}}), E[p^\infty]) = 0$ for $i \geq 2$ [Ser01].

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

(6)

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

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.

The second equality follows from a result in [Ima75]. He proved that $E(L_{\mathrm{cyc}})[p^\infty]$ is finite; hence the $h_G(E(L_{\mathrm{cyc}})[p^\infty]) = 1$ [Ser79, Proposition 8, page 134]. □

4.2. **Simplify the Denominator.** To simplify the denominator of Equation 5, we divide it into two cases, when $v \nmid p$ and when $v \mid p$.

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

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

Proof. We divide it into two cases. First when $w \mid v$ is totally split. We have

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

The right hand side is cohomologically trivial.

Now consider the non-split case. Recall that the p-part of the Brauer group, $\mathrm{Br}(L_{\mathrm{cyc},w})[p^\infty] = 0$ [Ser01, 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. An application of Hochschild-Serre spectral sequence gives a diagram similar to Equation 6. From this we conclude

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

□

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

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

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

The absolute Galois group of $K_{\mathrm{cyc},v}$ and $L_{\mathrm{cyc},w}$ have p-cohomological dimension 2. Further, by Tate duality, $H^2(L_{\mathrm{cyc},w}, E[p^\infty]) = H^2(K_{\mathrm{cyc},v}, E[p^\infty])) = 0$ [CS00, Proof of Theorem 1.12]. Using the Hochschild-Serre spectral sequence argument we arrive at the following isomorphism for $i = 1, 2$,

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

Observe 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 by the same argument as in Lemma 4.1.

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 proof of the claim is identical to that of [HV03, Proposition 3.12, Page 459]. It crucially uses a theorem of Imai, wherein he proves $L_{\mathrm{cyc},w} \cap L_w(\mathcal{F}[p^\infty])$ is a finite extension of L_w.

□

4.3. **Putting it Together.** The series of lemmas above simplifies Equation 5 to

$$h_G(R_{p^\infty}(E/L_{\mathrm{cyc}})) = \frac{1}{\bigoplus_{w\in S'(L_{\mathrm{cyc}})} h_G(E(L_{\mathrm{cyc},w})[p^\infty])}. \tag{7}$$

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 $L_{\mathrm{cyc}}/K_{\mathrm{cyc}}$. Set $H_w = \mathrm{ord}_p(h_G(E(L_{\mathrm{cyc},w})[p^\infty]))$. Rewrite Equation 4 as

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

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

5. Calculating H_w

Calculation of H_w is similar to that of [HM99]. We need to study the p-primary torsion points of E on the unramified $\mathbb{Z}_p$-extension of an ℓ-adic field. Computations in Section 4 allows us to focus only on the case $p \neq \ell$. We prove

Proposition 5.1. *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 3.1.

The proof of the above written proposition follows from the next lemma.

Lemma 5.2. *[HM99, Proposition 5.1] Let p, ℓ be distinct primes. Let $k/\mathbb{Q}_\ell$ be a finite extension and $k \supseteq \mu_p$. Set $k_\infty = k(\mu_{p^\infty})$ and E be defined over k.*

(1) If E has good reduction over k_∞, then

$$E(k_\infty)[p^\infty] \simeq \begin{cases} E[p^\infty] & \text{if } E(k)[p] \neq 0 \\ 0 & \text{if } E(k)[p] = 0 \end{cases}$$

(2) If E has split multiplicative reduction over k_∞, there exists an element $q \in k^\times$ and a non-negative integer m such that $E(k_\infty)[p^\infty]$ is isomorphic to the subgroup of $k_\infty^\times/q^{\mathbb{Z}}$ generated by μ_{p^∞} and q^{1/p^m} as a $\mathrm{Gal}(k_\infty/k_1)$-module.

(3) If E has non-split multiplicative reduction or additive reduction over k_∞, then $E(k_\infty)[p^\infty]$ is finite.

Proof. Since k is an ℓ-adic field, k_∞/k is unramified at primes above p and therefore the reduction type of E does not change since $p \geq 5$.

(1) From Nakayama lemma, it follows that $E(k)[p] = 0$ implies $E(k_\infty)[p^\infty] = 0$. When $E(k)[p] \neq 0$, by Weil pairing we know $k(E[p])/k$ is a p-extension because $k \supseteq \mu_p$. $k(E[p^\infty])/k$ is therefore a pro-p extension. Since E has good ordinary reduction, $k(E[p^\infty])/k$ is unramified. k_∞ is the maximal unramified pro-p extension of k, thus $k(E[p^\infty]) \subseteq k_\infty$. This gives the necessary isomorphism, $E(k_\infty)[p^\infty] \simeq E[p^\infty]$.

(2) E is isomorphic to a Tate curve over k_1 with Tate period $q \in k^\times$ [Sil09, Theorem C14.1]. As $\mathrm{Gal}(k_\infty/k_1)$-modules, $E(k_\infty) \simeq k_\infty^\times/q^{\mathbb{Z}}$. Let q_n be the p^n-th root of q. Then, $q_n^p = q_{n-1}$. Since, q is a unit in an ℓ-adic field, $\mathrm{ord}_\ell(q) > 0$; there is an integer m such that $q_m \in k_\infty$ but $q_{m+1} \notin k_\infty$. By assumption, $\mu_{p^\infty} \subset k_\infty$, we get the desired assertion.

(3) Let $\widetilde{k_n}$ be the residue field of k_n and $\widetilde{E_{ns}}(\widetilde{k_n})$ be the group of non-singular points of the reduction of E on $\widetilde{k_n}$. There exists a short exact sequence of Abelian groups

$$0 \to E_1(k_n) \to E_0(k_n) \xrightarrow{\text{red}} \widetilde{E_{ns}}(\widetilde{k_n}) \to 0$$

where $E_0(k_n)$ is the subgroup of $E(k_n)$ consisting of points with non-singular reduction and $E_1(k_n)$ is the kernel of red [Sil09, VII.2.1].

By assumption, $k \supseteq \mu_p$ so $|\widetilde{k_n}| \equiv 1 \mod p$, and $(|\widetilde{E_{ns}}(\widetilde{k_n})|, p) = 1$ [Sil09, Prop II.2.5]. Since $\ell \neq p$, the subgroup $E_1(k_n)$ has no non-trivial points of of order p [Sil09, Prop VII.3.1]. The above exact sequence implies $E_0(k_n)[p^\infty]$ is trivial. To finish the proof, we need to show $E(k_n)/E_0(k_n)$ is bounded. By the Kodaira-Neron theorem [Sil09, Theorem VII.6.1], $E(k_n)/E_0(k_n)$ is finite and independent of n. It has order at most 4. Thus, $E(k_n)[p^\infty]$ must be bounded independent of n for all n. This gives the desired result.

□

Proof. (of Proposition 5.1) Recall the notation, $v = w\,|_{K_{\mathrm{cyc}}}$ and $v \nmid p$ and v does not split in $L_{\mathrm{cyc}}/K_{\mathrm{cyc}}$. $L_{\mathrm{cyc},w}/K_{\mathrm{cyc},v}$ is a degree p Galois extension and using local class field theory, it is in fact a unique ramified extension. Furthermore, $K_{\mathrm{cyc},v} \supset \mu_{p^\infty}$.

- When E has good reduction at w, and there is no point of order p, ie

$$E(L_{\mathrm{cyc},w})[p] = E(K_{\mathrm{cyc},v})[p] = 0,$$

there is nothing to prove. When $w \in P_2$, the above proposition gives

$$E(L_{\mathrm{cyc},w})[p^\infty] = E(K_{\mathrm{cyc},w})[p^\infty] = E[p^\infty] \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^2.$$

Now note that

$$H_w = \mathrm{ord}_p\left(\frac{\#H^2(G, E(L_{\mathrm{cyc},w})[p^\infty])}{\#H^1(G, E(L_{\mathrm{cyc},w})[p^\infty])}\right) = \mathrm{ord}_p\left(\frac{\#\{0\}}{\#(\mathbb{Z}/p)^2}\right) = -2$$

- When E has split multiplicative reduction at w, $w \in P_1$. There is an exact sequence

$$0 \to \mu_{p^\infty} \to E(L_{\mathrm{cyc},w})[p^\infty] \to F \to 0$$

where F is a finite group. Action of G on μ_{p^∞} is trivial and hence

$$H_w = \mathrm{ord}_p\, h_G(\mu_{p^\infty}) = -1.$$

- When E has non-split or additive reduction at w, $w \notin P_1 \cup P_2$. From above, $E(L_{\mathrm{cyc},w})[p^\infty]$ is finite and hence $H_w = 0$.

□

6. Applications

In this section, we record an interesting corollary.

Set up: Let K be a number field, E be an elliptic curve defined over K and p be any prime. Set the notation, $K_n = K(E[p^{n+1}])$, ie the field obtained by adjoining the p^{n+1}-torsion points of E to K. Set $\mathcal{K}_\infty$ to be the field obtained by adjoining all the p-power torsion points on E to K. Let $G_\infty = \mathrm{Gal}(\mathcal{K}_\infty/K)$. When E has CM by an an imaginary quadratic, upon performing a finite base change, $G_\infty \simeq \mathbb{Z}_p^2$ and when E does not have CM, G_∞ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. In the second case, 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 $R_{p^\infty}(E/K_n^{cyc})$ is finitely generated as a $\mathbb{Z}_p$-module, the $\mathrm{corank}_{\mathbb{Z}_p}(R_{p^\infty}(E/K_n^{cyc})) = O(p^{3n})$ as $n \to \infty$. In the CM case, under the same assumptions as above, $\mathrm{corank}_{\mathbb{Z}_p}(R_{p^\infty}(E/K_n^{cyc})) = O(p^n)$ as $n \to \infty$. These would follow from asymptotic results proved in [Har00, Lemma 3.4.1]. We get more precise results using Theorem 3.1. The following result is in the spirit of [CH01, Proposition 6.9].

We prove the result in the non-CM case. The proof in the CM case is identical.

Proposition 6.1. *Assume the following:*

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

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

Then, for $n \geq m$,

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

Proof. By hypothesis, Theorem 3.1 gives the formula

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

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

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

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

Acknowledgement

The author would like to thank Kumar Murty for many helpful discussions, Jim Arthur for his encouragement, all 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

[CH01] JH Coates and Susan Howson. Euler characteristics and elliptic curves ii. *Journal of the Mathematical Society of Japan*, 53(1):175–235, 2001.

[CS00] John Coates and Ramdorai Sujatha. *Galois cohomology of elliptic curves*. Narosa, 2000.

[CS05] John Coates and Ramdorai Sujatha. Fine Selmer groups of elliptic curves over p-adic Lie extensions. *Mathematische Annalen*, 331(4):809–839, 2005.

[Har00] Michael Harris. Correction to p-adic representations arising from descent on Abelian varieties. *Compositio Mathematica*, 121(1):105–108, 2000.

[HM99] Yoshitaka Hachimori and Kazuo Matsuno. An analogue of Kida's formula for the Selmer groups of elliptic curves. *J. Alg. Geom.*, 8:581–601, 1999.

[HV03] Yoshitaka Hachimori and Otmar Venjakob. Completely faithful Selmer groups over Kummer extensions. *Documenta Math., Extra Volume: Kazuya Kato's Fiftieth Birthday*, pages 443–478, 2003.

[Ima75] Hideo 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.

[Iwa81] Kenkichi Iwasawa. Riemann-Hurwitz formula and p-adic Galois representations for number fields. *Tohoku Mathematical Journal, Second Series*, 33(2):263–288, 1981.

[Kat04] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004.

[Kid80] Yûji Kida. ℓ-extensions of CM-fields and cyclotomic invariants. *J. Number Theory*, 12:519–528, 1980.

[Mat00] Kazuo 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.

[Maz72] Barry Mazur. Rational points of abelian varieties with values in towers of number fields. *Inventiones mathematicae*, 18(3-4):183–266, 1972.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67. Springer, 1979.

[Ser01] Jean-Pierre Serre. *Galois Cohomology*. Springer Science & Business Media, 2001.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

Department of Mathematics, University of Toronto, Bahen Centre, 40 St. George St., Room 6290, Toronto, Ontario, Canada, M5S 2E4

Email address: dkundu@math.utoronto.ca