IWASAWA L-FUNCTIONS OF ELLIPTIC CURVES WITH ADDITIVE REDUCTION

JOHN W. JONES

Abstract. In this paper we investigate the Iwasawa L-functions of elliptic curves with potentially multiplicative reduction and prove analogues of the conjectures of Birch and Swinnerton-Dyer for them.

Let A be an elliptic curve over a number field K, and let p be a prime number different from 2. The Iwasawa theory for an elliptic curve is best understood when A has semi-stable ordinary reduction at the places of $\mathcal{O}_K$ dividing p. The Iwasawa L-functions have been studied by Perrin Riou, Schneider, and the author (see [9, 12, 13, 1]). If A is an elliptic curve over $\mathbf{Q}$, there is a definition of the p-adic L-function and calculations to support Birch and Swinnerton-Dyer type conjectures (see [5]). Again, this is in the case of semi-stable ordinary reduction. Work has also been done in the case of good supersingular reduction (see [13, 10]).

Little is known about Iwasawa theory of elliptic curves without semi-stable reduction at primes dividing p. In the theory described above, the case of an elliptic curve with split multiplicative reduction at p provided new interest in the form of an *extra zero* in the p-adic and Iwasawa L-functions, and a new term in the first non-vanishing coefficient. This raises the question of whether any other "new" phenomena would occur in the case of additive reduction.

In this paper, we generalize the Iwasawa L-function to elliptic curves with potentially ordinary reduction at primes lying over p. We find that additional extra zeros do not occur in this case, even if the additive reduction becomes split multiplicative after a finite base change. While the final results concern elliptic curves, we set up the definitions for abelian varieties. Also, in section 4, we investigate the cokernel of the local norm map for elliptic curves with potentially multiplicative reduction and show that it is trivial.

1. Notation

Let p be an odd prime, and K a number field.

Let $A_{/K}$ be an abelian variety over K, and let A denote its Néron model over $\mathcal{O}_K$ (the ring of integers of K). The Néron model of the dual abelian variety of A_K is denoted $\tilde{A}$. If F is an extension of K, $A_{/F}$ will denote the base change of $A_{/K}$ to F.

The Tate-Shafarevich group of $A_{/K}$ is denoted by $Ш_K(A)$. The "connected component" of A will be denoted by A^0. We have the short exact sequence of sheaves for the *fpqf* site over $\mathcal{O}_K$

$$0 \to A^0 \to A \to \Phi \to 0.$$

This work was partially supported by NSF grant DMS-9100238.

The restriction of Φ to the small etale site is a skyscraper sheaf composed on each fiber by the group of connected components for the reduction of A at that place. That is, (for example, over K)

$$\Phi = \bigoplus_{v \in \mathcal{O}_K} {}_v\Phi$$

where all but finitely many of the ${}_v\Phi$ are trivial.

In writing cohomology groups, we will make the following conventions. Galois and group cohomology will be denoted by $H^i(G,-)$. Flat (*fpqf*) cohomology of $spec(R)$ where R is a ring will be denoted by $H^i(R,-)$. Relative flat cohomology will be denoted by $H^i_t(R,-)$ if t is a closed point of $spec(R)$, $H^i_T(R,-)$ if T is a closed subset, and $H^i_\cdot(R,-)$ if R is a local ring. If R'/R is an extension of rings, equivariant cohomology (in the sense of [12] or [7]) will be denoted as $H^i(R'/R,-)$. Finally, the coefficients of our coholomolgy will almost always come from the abelian variety A. It is understood that in an expression such as $H^i(\mathcal{O}_F, A^0)$ where F is an extension of K, one takes the Néron model of $A_{/F}$, and then takes the connected component.

There is a finite extension K'/K so that $A_{K'}$ has semi-stable reduction at all primes of $\mathcal{O}_{K'}$ dividing p. The extension K'/K can be taken to be Galois, and we do so denoting its Galois group by G_K.

If v is a place of K so that the reduction of A at v is an extension of an ordinary abelian variety by a torus, we say that A is ordinary at v. If $A_{K'}$ is ordinary at every place of K' dividing v, but A_K in not ordinary at v, we say that A_K is potentially ordinary at v.

Let L/K be a Γ-extension, that is, a Galois extension of K where $\mathrm{Gal}(L/K) = \Gamma \cong \mathbf{Z}_p$ (the additive group $\mathbf{Z}_p$). This isomorphism is not canonical, so we fix one by picking a topological generator γ of Γ. We further require that primes of bad reduction for A split only finitely in L.

Let Γ_n be the unique closed subgroup of Γ of index p^n, and let K_n be the fixed field of Γ_n. Let Λ denote the completed group ring $\varprojlim \mathbf{Z}_p[\Gamma/\Gamma_n]$.

The completion of K for a place v is denoted by K_v. We let L_w be the union of the completions K_{n,v_n} where each v_n is a place of K_n which w lies over.

Let $L' := K'L$. Then L'/K' is also a Γ-extension with $\Gamma' = \mathrm{Gal}(L'/K')$ canonically isomorphic to Γ_n for some n. Furthermore, $G_L := \mathrm{Gal}(L'/L)$ is naturally a subgroup of G_K.

Fix a continuous character

$$\kappa \colon \mathrm{Gal}(L/K) \to 1 + p\mathbf{Z}_p \subset \mathbf{Z}_p^*.$$

We denote Iwasawa's p-adic logarithm on $\mathbf{Z}_p^*$ by $\log_p$. (Note, we could in fact use a constant multiple of $\log_p$ here without much difficulty.) We then define a p-adic logarithm $\log_K : \mathbb{A}^*(K) \to \mathbf{Z}_p$ by $\log_K := \log_p \circ \kappa \circ rec$. Here $rec \colon \mathbb{A}^*(K) \to \mathrm{Gal}(L/K)$ is the reciprocity map from class field theory. We then induce a p-adic logarithm at the places of K dividing p by composing with the inclusion $K_v^* \to \mathbf{A}^*(K)$.

This logarithm will induce one for K' as follows. Since the extension L'/K' is the base change of L/K, we have the following commutative diagram

$$\begin{array}{ccc} \mathbb{A}^*(K') & \xrightarrow{rec} & \Gamma' \\ \mathbf{N}\big\downarrow & & \big\downarrow \\ \mathbb{A}^*(K) & \xrightarrow{rec} & \Gamma \end{array}$$

where $\mathbf{N}$ is the norm map on ideles. We then define κ for L'/K' by composing $\Gamma' \hookrightarrow \Gamma \xrightarrow{\kappa} \mathbf{Z}_p^*$. Then $\log_{K'} = \log_K \circ \mathbf{N}_{K'/K}$.

A *quasi-isomorphism* is a group homomorphism with finite kernel and cokernel. A group H_1 is quasi-isomorphic to H_2 if there is a quasi-isomorphism $H_1 \to H_2$. We denote this by $H_1 \sim H_2$. (Note that this is not an equivalence relation in general, but it is for the category of torsion Λ-modules.)

The order of a finite abelian group H is denoted by $|H|$, or simply by H. If H is an abelian group, we let $H^* = \mathrm{Hom}(H, \mathbf{Q}/\mathbf{Z})$ denote the Pontryagin dual of H. A $\mathbf{Z}_p$-module, M, is cofinitely generated if M^* is a finitely generated $\mathbf{Z}_p$-module. The $\mathbf{Z}_p$-corank of M is then the $\mathbf{Z}_p$-rank of M^*.

Finally, if H is an abelian group, an abelian group scheme or a sheaf of abelian groups, H_n will denote the kernel of multiplication by n on H. We then let $H_{p^\infty} := \varinjlim H_{p^m}$.

2. Defining the Iwasawa L-function

In order to define an Iwasawa L-function, we need an appropriate choice of Selmer group S for A over L. The Pontryagin dual of this group should be a compact finitely generated Λ-module, whose characteristic polynomial (for γ) we denote by $F_S(T)$. The Iwasawa L-function is then $L(S;x) = F_S(\kappa(\gamma)^{1-x} - 1)$. For questions regarding the basic theory of Λ-modules and their characteristic polynomials, see [14].

There are several choices for the Selmer group in this situation. Two we consider here are $H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^{G_L}$ and $H^1(\mathcal{O}_{L'}/\mathcal{O}_L, A^0_{p^\infty})$. These selections were motivated by the success of $H^1(\mathcal{O}_L, A^0_{p^\infty})$ in the ordinary case (see [1]). We first show that these two groups are quasi-isomorphic, hence would give rise to the same Iwasawa L-function.

Proposition 1. *There is a quasi-isomorphism* $H^1(\mathcal{O}_{L'}/\mathcal{O}_L, A^0_{p^\infty}) \to H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^{G_L}$. *If the order of* G_L *is prime to* p, *this map is an isomorphism.*

Proof: By the spectral sequence (see [7])

$$H^p(G_L, H^q(\mathcal{O}_{L'}, A^0_{p^\infty})) \Rightarrow H^{p+q}(\mathcal{O}_{L'}/\mathcal{O}_L, A^0_{p^\infty})$$

we get the following exact sequence of the low order terms.

$$0 \to H^1(G_L, A^0_{p^\infty}(\mathcal{O}_{L'})) \to H^1(\mathcal{O}_{L'}/\mathcal{O}_L, A^0_{p^\infty}) \to H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^{G_L} \to H^2(G_L, A^0_{p^\infty}(\mathcal{O}_{L'})).$$

In general, the groups $H^i(G_L, A^0_{p^\infty}(\mathcal{O}_{L'}))$ are finite for $i > 0$ (see Lemma 2.2 below), and we get the quasi-isomorphism from $H^1(\mathcal{O}_{L'}/\mathcal{O}_L, A^0_{p^\infty})$ to $H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^{G_L}$. If the order of G_L is prime to p, $H^i(G_L, A^0_{p^\infty}(\mathcal{O}_{L'})) = 0$ for $i > 0$ and we get $H^1(\mathcal{O}_{L'}/\mathcal{O}_L, A^0_{p^\infty}) = H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^{G_L}$. □

We will use $H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^{G_L}$ then for defining the Iwasawa L-function throughout.

In our definition, there is a choice made in the field K' (Galois over K, for which A is semi-stable at the primes dividing p). We prove that the corresponding Iwasawa L-function is independent of the choice of K'.

Theorem 2.1. *Let K' and K'' be finite Galois extensions of K so that A is semi-stable for each prime of K' and K'' dividing p. If $L' = K'L$ and $L'' = K''L$, then $H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^{G_{L'/L}}$ and $H^1(\mathcal{O}_{L''}, A^0_{p^\infty})^{G_{L''/L}}$ give rise to the same Iwasawa L-function.*

Proof: It is sufficient to show that the two cohomology groups are quasi-isomorphic to a common Λ-module. Furthermore, by comparing the groups for L' and L'' with the corresponding group for the composite $L'L''$, we reduce to the case where L'' contains L'.

To show that $H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^{G_{L'/L}} \rightarrow H^1(\mathcal{O}_{L''}, A^0_{p^\infty})^{G_{L''/L}}$ is a quasi-isomorphism, it suffices to show that $H^1(\mathcal{O}_{L'}, A^0_{p^\infty}) \rightarrow H^1(\mathcal{O}_{L''}, A^0_{p^\infty})^{G_{L''/L'}}$ is a quasi-isomorphism. One then takes $G_{L'/L}$ invariants to get the result.

Let T' be the places of L' ramifying in L''/L' and let T'' be the places of L'' lying above T'. From the relative cohomology sequence we get the following diagram.

$$\begin{array}{ccccccc}
H^1_{T'}(\mathcal{O}_{L'}, A^0_{p^\infty}) & \rightarrow & H^1(\mathcal{O}_{L'}, A^0_{p^\infty}) & \rightarrow & H^1(\mathcal{O}_{L'} - T', A^0_{p^\infty}) & \rightarrow & H^2_{T'}(\mathcal{O}_{L'}, A^0_{p^\infty}) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
H^1_{T''}(\mathcal{O}_{L''}, A^0_{p^\infty}) & \rightarrow & H^1(\mathcal{O}_{L''}, A^0_{p^\infty}) & \rightarrow & H^1(\mathcal{O}_{L''} - T'', A^0_{p^\infty}) & \rightarrow & H^2_{T''}(\mathcal{O}_{L''}, A^0_{p^\infty})
\end{array}$$

The kernel of the first horizontal map in the top row is $A^0_{p^\infty}(\mathcal{O}_{L'} - T')/A^0_{p^\infty}(\mathcal{O}_{L'})$. This group is bounded by the group $A_{p^\infty}(L')/A^0_{p^\infty}(\mathcal{O}_{L'})$, which is finite by Lemma 3.3 of [1]. Similarly, the first map in the bottom row has a finite kernel.

To show that $H^1(\mathcal{O}_{L'}, A^0_{p^\infty}) \rightarrow H^1(\mathcal{O}_{L''}, A^0_{p^\infty})^{G_{L''/L'}}$ is a quasi-isomorphism, we break the above horizontal sequences into short exact sequences, and take $G_{L''/L'}$-invariants. It then suffices to show that

$$H^1_{T'}(\mathcal{O}_{L'}, A^0_{p^\infty}) \rightarrow H^1_{T''}(\mathcal{O}_{L''}, A^0_{p^\infty})^{G_{L''/L'}} \tag{1}$$

$$H^1(\mathcal{O}_{L'} - T', A^0_{p^\infty}) \rightarrow H^1(\mathcal{O}_{L''} - T', A^0_{p^\infty})^{G_{L''/L'}} \tag{2}$$

are quasi-isomorphisms and that

$$H^2_{T'}(\mathcal{O}_{L'}, A^0_{p^\infty}) \rightarrow H^2_{T''}(\mathcal{O}_{L''}, A^0_{p^\infty})^{G_{L''/L'}} \tag{3}$$

has finite kernel.

Looking at map 1, we can replace $H^1_{T'}(\mathcal{O}_{L'}, A^0_{p^\infty})$ by $\bigoplus_{t \in T'} H^1_{\cdot}(\mathcal{O}_{L'_t}, A^0_{p^\infty}) = \bigoplus_{t \in T'} H^1(\mathcal{O}_{L'_t}, \Phi_{p^\infty})$ (and similarly over L''). The final equality comes from Lemma 3.1 of [2] at the finite levels of the Γ-extension and taking the limit up the tower. For each $t' \in T'$, pick a place $t'' \in T''$ lying over it and let D be the corresponding decomposition group. The kernel and cokernel of $H^1(\mathcal{O}_{L'_{t'}}, \Phi_{p^\infty}) \rightarrow (\bigoplus_{t''|t'} H^1(\mathcal{O}_{L''_{t''}}, \Phi_{p^\infty}))^{G_{L''/L'}}$ is the same as for $H^1(\mathcal{O}_{L'_{t'}}, \Phi_{p^\infty}) \rightarrow H^1(\mathcal{O}_{L''_{t''}}, \Phi_{p^\infty})^D$. By devissage, we then consider just the cases where the extension is either unramified or totally ramified.

For the totally ramified case, note $H^1(\mathcal{O}_{L'_{t'}}, \Phi_{p^\infty}) = H^1(k', \Phi(\mathcal{O}_{L'_{t'}})_{p^\infty})$ where k' is the residue field for $\mathcal{O}_{L'_{t'}}$ (see Lemma 5.1 of [3]). The $\mathbf{Z}_p$-corank of this group is the dimension of the maximal split subtorus in the reduction of A over $\mathcal{O}_{K'}$. This dimension does not change after a totally ramified extension (i.e., to L''). Since map

1 is induced by inclusion, the same is true over the residue fields. Since $k'' = k'$, the map is a quasi-isomorphism.

In the unramified case, we have $H^1(\mathcal{O}_{L'_{t'}}, \Phi_{p^\infty}) = H^1(k', \Phi(\mathcal{O}_{L'_{t'}})_{p^\infty})$ as above. Hence, we reduce to the map $H^1(k', \Phi(\mathcal{O}_{L'_{t'}})_{p^\infty}) \to H^1(k'', \Phi(\mathcal{O}_{L''_{t''}})_{p^\infty})^D$ where now $D = \mathrm{G}_{k''/k'}$. We can now apply the Hochshild-Serre spectral sequence to see that the kernel and cokernel are given by $H^i(\mathrm{G}_{k''/k'}, \Phi(k'')_{p^\infty})$ for $i = 1$ and 2 respectively. These are finite by the Lemma 2.2 below.

In map 2, we can apply the Hochshild-Serre spectral sequence. The kernel and cokernel are bounded by the groups $H^i(G_{L'/L}, A^0_{p^\infty}(\mathcal{O}_{L''} - T''))$ for $i = 1$ and 2 resectively. These groups are also finite by Lemma 2.2 below.

Finally in map 3, the group

$$\begin{aligned} H^2_{T'}(\mathcal{O}_{L'}, A^0_{p^\infty}) &= \bigoplus_{t \in T'} H^2_t(\mathcal{O}_{L'}, A^0_{p^\infty}) \\ &= \bigoplus_{t \in T'} H^2_t(\mathcal{O}_{L'}, A^0)_{p^\infty} \quad \text{by the Kummer sequence} \\ &= \bigoplus_{t \in T'} H^1(L'_t, A)_{p^\infty} \quad \text{by the relative cohomology sequence} \end{aligned}$$

and similarly over L''. The kernel of the map $H^1(L'_t, A)_{p^\infty} \to \bigoplus_{v|t} H^1(L''_v, A)_{p^\infty}$ is given by $H^1(G_{L''_v/L'_t}, A(L''_v))_{p^\infty}$ by the Hochshild-Serre spectral sequence (for some place $v|t$). We write this final group a direct limit over the finite levels of the Γ-extensions.

$$H^1(G_{L''_v/L'_t}, A(L''_v))_{p^\infty} = \varinjlim H^1(G_{K''_{n,v}/K'_{n,t}}, A(K''_{n,v}))_{p^\infty}$$

so the problem becomes to show that the orders of the latter groups is bounded as n goes to infinity.

The group $H^1(G_{K''_{n,v}/K'_{n,t}}, A(K''_{n,v}))_{p^\infty}$ is dual to the cokernel of the norm map $\tilde{A}(K''_{n,v}) \to \tilde{A}(K'_{n,t})$. We now use the following exact diagram

$$\begin{array}{ccccccccc} 0 & \to & \tilde{A}^0(\mathcal{O}_{K''_{n,v}}) & \to & \tilde{A}(K''_{n,v}) & \to & \Phi(\mathcal{O}_{K''_{n,v}}) & \to & 0 \\ & & \downarrow \mathbf{N} & & \downarrow \mathbf{N} & & \downarrow \mathbf{N} & & \\ 0 & \to & \tilde{A}^0(\mathcal{O}_{K'_{n,t}}) & \to & \tilde{A}(K'_{n,t}) & \to & \Phi(\mathcal{O}_{K'_{n,t}}) & \to & 0 \end{array}$$

Since $\tilde{A}$ is semi-stable and ordinary over K', it is over $K'_{n,t}$ and $K''_{n,v}$, so the cokernel in the first column is uniformly bounded by Corollary 4.30 of [3] (in fact, it is bounded by $(G(n,t)_{\mathrm{ab}})^d$ where d is the dimension of the Abelian variety $\tilde{A}$, and $G(n,t)_{\mathrm{ab}}$ denotes the order of the abelianization of the Galois group $\mathrm{Gal}(K''_{n,v}/K'_{n,t})$, which in turn are bounded by the order of $\mathrm{Gal}(L''/L')$). The order of the cokernel in the right column is bounded by $\varinjlim \Phi(K'_n)/|G|$ (which is bounded because the group of connected components in the limit is of cofinite type). This completes the theorem. □

We now state the lemma referred to in the theorem above.

Lemma 2.2. *Let M be a cofinitely generated $\mathbf{Z}_p$-module which is also a G-module for a finite group G. Then $H^i(G, M)$ are finite for $i \geq 1$.*

Proof: The proof is elementary. The key point is that the divisible subgroup of M is of finite index by the assumption that it is cofinitely generated, and the cohomology of a divisible group is trivial. □

3. Heights

A central term on the "right hand side" of the Birch and Swinnerton-Dyer formula is the height pairing determinant. Although p-adic heights for abelian varieties which are not semi-stable at p has not been well developed, it is not difficult to extend the existing theory.

Note that if A has ordinary reduction modulo the primes dividing p of a field E, then there are several descriptions of p-adic height pairings $<,>_E: A(E)\times \hat{A}(E)\to \mathbf{Q}_p$ (see [11, 2, 4]). In each case, if E' is a finite extension of E of degree d, then

$$d < P,Q >_E = < P,Q >_{E'} \qquad \forall P\in A(E), Q\in \hat{A}(E).$$

Let $\langle\ ,\ \rangle_{p,K'}$ be the pairing defined in [2] for the field K' (this is recalled below). We can then define $\langle\ ,\ \rangle_{p,K}: A(K)\times \hat{A}(K)\to \mathbf{Q}_p$ by

$$\langle P,Q\rangle_{p,K} = \frac{1}{[K':K]}\langle P,Q\rangle_{p,K'}.$$

This definition is independent of the choice of field K' for which A is semi-stable at the primes dividing p (if K'' is another such field, compare with the value of the height pairing for the composite $K'K''$). Moreover, if this extension is carried out for different heights (say Schneider's analytic height or Mazur-Tate canonical height), the same comparison theorems hold for $\langle\ ,\ \rangle_{p,K}$.

We now recall the definition of $\langle\ ,\ \rangle_{p,K'}$. We start with the pairing $\langle\ ,\ \rangle_{\gamma,K'}$, which is induced by the following diagram.

$$\begin{tikzcd}
\tilde{A}^0(\mathcal{O}_{K'})\otimes \mathbf{Z}_p \arrow[d] & \mathrm{Hom}_{\mathbf{Z}_p}(A^0(\mathcal{O}_{K'})\otimes \mathbf{Z}_p, \mathbf{Z}_p) \\
H^2(\mathcal{O}_{K'}, A_{p^\infty})^* \arrow[d, "\varphi_2^*"] & (H^1(\mathcal{O}_{K'}, A^0_{p^\infty})^*)_{\mathrm{Tor}} \arrow[u] \\
H^2(\mathcal{O}_{K'}, A^0_{p^\infty})^* & H^1(\mathcal{O}_{K'}, A^0_{p^\infty})^* \arrow[u] \\
{[H^2(\mathcal{O}_{L'}/\mathcal{O}_{K'}, A^0_{p^\infty})/H^1_T(\mathcal{O}_{L'}/\mathcal{O}_{K'})]^*} \arrow[u, "\theta^*"] \arrow[d, "\mu^*"] & \mathcal{S}^* \arrow[u, "i^*"] \\
{[H^1(\mathcal{O}_{L'}, A^0_{p^\infty})_\Gamma/H^1_T(\mathcal{O}_{L'})]^*} \arrow[d, equal] & \\
H^1(\Gamma, \mathcal{S}_\infty)^* \arrow[r, "g^*"] & H^0(\Gamma, \mathcal{S}_\infty)^* \arrow[uu, "\alpha^*"]
\end{tikzcd} \tag{4}$$

We will not need the details of the definitions of the groups and maps here. They can be found in [2]. It is furthermore shown in [2] that, provided $III_K(A)_{p^\infty}$ is finite, all of the maps used in the definition are quasi-isomorphisms except for possibly μ^* and g^*, but μ^* is surjective.

This definition depends on our choice of generator γ of Γ. To remedy this we set

$$\langle\ ,\ \rangle_{p,K'} := \langle\ ,\ \rangle_{\gamma,K'} \log_p \kappa(\gamma).$$

4. The Cokernel of the Local Norm Map

A term needed for the next section, as well as an interesting invariant in its own right, is the cokernel of the local norm mapping. In this section, we calculate it for elliptic curves with potentially multiplicative reduction.

Let A be an elliptic curve, K_v be a finite extension of $\mathbf{Q}_p$, and L_v/K_v a Γ-extension.

If E is a finite Galois extension of K_v, the norms

$$\mathbf{N}_{E/K_v}A := \{ \sum_{g\in \mathrm{Gal}(E/K_v)} g\,x \quad \text{for} \quad x \in A(E)\}$$

where the sum is taken under the group law of A. The *universal norms* for the Γ-extension L_v/K_v are formed by the intersection of the groups of norms from each finite subextension E

$$\mathbf{N}A(L_v) := \bigcap_{K_v\subset E\subset L_v} \mathbf{N}_{E/K_v}H.$$

We would like to study the behavior of the cokernel of the norm map under quadratic twists.

4.1. **Quadratic Twists.**

In general, given a quadratic extension K'/K, the Galois group G_K is cyclic of order 2. The natural map $G_L \to G_K$ is an isomorphism because $p \neq 2$. To simplify the notation, we identify G_K and G_L via this map and denote them by G. Similarly, Γ' is naturally isomorphic to Γ, and so we identify them. In particular, $\mathrm{Gal}(L'/K) \cong G \times \Gamma$.

Let $A_{(v)/K}$ be the twist of $A_{/K}$ for the quadratic extension K'/K. There are natural actions of G on $A_{/K'}$ and on $A_{(v)/K'}$ by viewing them as base changes of $A_{/K}$ and $A_{(v)/K}$. Since $A_{(v)/K'} \cong A_{/K'}$, there are two actions on this elliptic curve. They differ by a twist by -1 (inversion). Hence, when looking at the action of G on $A(K)$ (or some a related cohomology group), the + eigenspace is the set of invariants for the action of G coming from $A_{/K}$ and the - eigenspace is the set of invariants for the action of G coming from $A_{(v)}$.

So, $H^1(\mathcal{O}_{K'}, A^0_{p^\infty}) = H^1(\mathcal{O}_{K'}, A^0_{p^\infty})^+ \oplus H^1(\mathcal{O}_{K'}, A^0_{p^\infty})^- = H^1(\mathcal{O}_{K'}, A^0_{p^\infty})^G \oplus H^1(\mathcal{O}_{K'}, (A^0_{(v)})_{p^\infty})^G$, a direct sum of its plus and minus components (using here $p \neq 2$). Naturally, the analogous statement holds for L'/L, or in the local situation of the next section.

4.2. **Cokernels.**

We return now to the local situation.

Lemma 4.1. *If K'_v is a quadratic extension of K_v,*

$$A(K'_v)/\mathbf{N}A(L'_v) \cong A(K_v)/\mathbf{N}A(L_v) \times A_{(v)}(K_v)/\mathbf{N}A_{(v)}(L_v)$$

and

$$|A(K'_v)/\mathbf{N}A(L'_v)| = |A(K_v)/\mathbf{N}A(L_v)| \cdot |A_{(v)}(K_v)/\mathbf{N}A_{(v)}(L_v)|$$

where the equality implies that if two of the terms are finite, then so is the third.

Proof: Clearly the isomorphism implies the equality on the orders. By Proposition 4.2 of [3], the group $A(K_v)/NA(L_v)$ is dual to $H^1(\Gamma, A(L_v))$ (we do not distinguish between A and its dual since A since we assume here that A is an elliptic curve). Consider $H^1(\Gamma, A(L'_v))$. Since it is a p-group with $p \neq 2$,

$$\begin{aligned} H^1(\Gamma, A(L'_v)) &= H^1(\Gamma, A(L'_v))^+ \oplus H^1(\Gamma, A(L'_v))^- \\ &= H^1(\Gamma, A(L'_v))^G \oplus H^1(\Gamma, A_{(v)}(L'_v))^G \end{aligned}$$

from the discussion above.

We now apply the Hochshild-Serre spectral sequence for the extension L'_v/K_v (breaking it up both with G as the subgroup and with Γ as the subgroup). From the exact sequences of low order terms we get

$$0 \to H^1(G, A(K'_v)) \to H^1(G \times \Gamma, A(L'_v)) \to H^1(\Gamma, A(L'_v))^G \to H^2(G, A(K'_v))$$

and

$$0 \to H^1(\Gamma, A(L_v)) \to H^1(G \times \Gamma, A(L'_v)) \to H^1(G, A(L'_v))^\Gamma$$

In the first sequence, $H^i(G, A(K'_v))_{p^\infty} = 0$ for $i > 0$ since $|G|$ is prime to p. Similarly, in the second, $H^1(G, A(L'_v))^\Gamma_{p^\infty} = 0$. Hence,

$$H^1(\Gamma, A(L'_v))^G = H^1(G \times \Gamma, A(L'_v))_{p^\infty} = H^1(\Gamma, A(L_v))$$

One has the analogous result of $A_{(v)}$, and so

$$H^1(\Gamma, A(L'_v)) = H^1(\Gamma, A(L_v)) \oplus H^1(\Gamma, A_{(v)}(L_v)).$$

□

Note that this proposition gives information on the orders of groups of connected components on A and $A_{(v)}$ by applying it to the unramified Γ-extension by Proposition 4.3 of [3].

We now concentrate on the case of potentially multiplicative reduction. In general, if A has additive reduction at the place v of K_v which is multiplicative in an extension of K_v, we see from looking at Weierstrass equations that A has multiplicative reduction over $K' := K(\sqrt{\pi_v})$ where π_v is a local uniformizer at a place v.

Lemma 4.2. *If v is a place of $\mathcal{O}_K$ for which A has potentially multiplicative reduction, then $A_{(v)}$ has multiplicative reduction at v.*

Proof: This is clear from a calculation with a Weierstrass equation for A which is minimal at v. □

Now, the main proposition of this section.

Proposition 2. *If A has potentially multiplicative reduction at the unique prime of K_v, then $A(K_v)/\mathbf{N}A(L_v)$ is the trivial group.*

Proof: Let K'_v be a quadratic ramified extension of K_v so that A has multiplicative reduction. Let $A_{(v)/K}$ be the twist of $A_{/K}$ for this extension K'_v/K_v, and let $L'_v := K'_v L_v$.

We can now make use of the results of [8] on the cokernel of the local norm map for elliptic curves with multiplicative reduction. We know that $A_{(v)}$ has multiplicative reduction over K_v and K'_v. This extension is necessarily ramified since A has additive reduction over K_v and multiplicative reduction over K'_v. Hence, if $A_{(v)}$ has non-split multiplicative reduction over K_v, it has non-split reduction over K'_v and both $H^1(\Gamma, A_{(v)}(L_v))$ and $H^1(\Gamma, A_{(v)}(L'_v)) = H^1(\Gamma, A(L'_v))$ are trivial.

If $A_{(v)}$ has split multiplicative reduction over K_v and K'_v, there are two cases to consider. Let q be the Tate-q parameter for $A_{(v)}$, and $\log_v$ a p-adic log for

L_v/K_v. From the methods of [8], if $\log_v(q) = 0$, both groups $H^1(\Gamma, A_{(v)}(L_v))$ and $H^1(\Gamma, A_{(v)}(L'_v))$ are isomorphic to $\mathbf{Z}_p$, so again $H^1(\Gamma, A(L_v))$ is trivial.

Finally, if $\log_v q \neq 0$, $H^1(\Gamma, A_{(v)}(L_v))$ and $H^1(\Gamma, A_{(v)}(L'_v))$ have order given by the index of the norm residue symbol of q for the extensions L_v/K_v and L'_v/K'_v. Since one extension is gotten from the other by "translating" by a group of order 2, these indexes are the same. $\square$

5. Elliptic Curves with Potentially Multiplicative Reduction

In this section, $A_{/K}$ will denote an elliptic curve over K. As before, we define the Iwasawa L-function of A for a Γ-extension L/K as

$$L_p(L/K, A; x) := F_H(\kappa(\gamma)^{1-x} - 1). \tag{5}$$

$F_H(T)$ is the characteristic polynomial of γ for a Λ-module H^* gotten as follows. Let K' be a finite Galois extension of K such that the reduction of A at primes of K' dividing p is semi-stable. Furthermore, let $L' = K'L$ and $G = \mathrm{Gal}(K'/K) = \mathrm{Gal}(L'/L)$. Then, $H = H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^G$.

We denote the order of vanishing of $L_p(L/K, A; x)$ at $x = 1$ by $\mathrm{ord}_{\,x=1} L_p(L/K, A; x)$. Note that by equation 5, this is the same as the order of vanishing of $F_H(T)$ at $T = 0$. We furthermore define for any non-negative integer ρ,

$$L_p^{(\rho)}(L/K, A; x) = \frac{1}{\rho!}\frac{d^\rho}{dx^\rho} L_p(L/K, A; x)$$

For each place v of K, let e_v equal 1 if v is a place of split multiplicative reduction, and 0 otherwise. Let $e := \sum_{v \in T} e_v$. For each place v of split multiplicative reduction, let q_v be the local Tate-q. Denote the rank of $A(K)$ by r. Finally, for two elements a and b of a field with a non-archimedian valuation, we write $a \approx b$ to denote that a and b have the same valuation.

We define the local $\mathcal{L}_v$-invariant of an elliptic curve A with respect to the Γ-extension L/K at a place v of K which is ramified in L as

$$\mathcal{L}_v(A) := \frac{A(K_v)/\mathbf{N}A(L_v)}{\Phi(\mathcal{O}_{K_v}) \ \ |\log_p \kappa(\gamma)|_p^{e_v}}.$$

As pointed out in [1],

$$\mathcal{L}_v(A) \approx \begin{cases} \frac{\log_K q_v}{\mathrm{ord}_{\,p} q_v} & \text{if } v \text{ is split multiplicave} \\ 1 & \text{if } v \text{ is non-split multiplicative} \\ A(k_v)^2 & \text{if } v \text{ is good ordinary} \end{cases}$$

For our new case, where v is potentially multiplicative, $\mathcal{L}_v(A) \approx 1$. This comes by combining Proposition 2 above with the fact that for an elliptic curve with potentially multiplicative reduction at v, $\Phi(\mathcal{O}_{K_v})$ has order dividing 4, hence is prime to p.

Let $v_1, \ldots, v_j$ be the places of K ramifying in L where A has potentially multiplicative reduction. Using Artin's approximation theorem, one can find an element $x \in K$ which is a local uniformizer for each of the v_i. Then, A has multiplicative reduction over the field $K' = K(\sqrt{x})$ for the places of K' lying over each v_i. We will now fix K'.

We now state our main theorem. In the following statements, we denote the number of connected components for the reduction at a place v by m_v.

Theorem 5.1.

$$\mathrm{ord}_{\,x=1} L_p(L/K, A; x) \geq r + e.$$

If the height pairing $\langle\ ,\ \rangle_{p,K'}$ is non-degenerate, $\log_p(q_v) \neq 0$ for each $v \in T$ where A has split multiplicative reduction, and $\text{Ш}_{K'}(A)_{p^\infty}$ is finite, then

$$\mathrm{ord}_{\,x=1} L_p(L/K, A; x) = r + e$$

and

$$L_p^{(r+e)}(L/K, A; x) \approx \prod_{t \in T} L_t(A)\, \frac{\mathrm{Det}\langle\ ,\ \rangle_{p,K}\ \text{Ш}_K(A)_{p^\infty}}{A_{p^\infty}(K)^2} \prod_{v \not\mid \infty} m_v.$$

Proof: From the basic theory of Λ-modules, we can obtain a lower bound for the order of vanishing of the Iwasawa L-function by looking at the $\mathbf{Z}_p$-corank of $(H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^G)^\Gamma$.

From Lemma 3.2 and Proposition 3.4 of [1], $H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^\Gamma \sim H^1(\mathcal{O}_{K'}, A^0_{p^\infty}) \oplus (\bigoplus_{t \in T_{L'}}\ {}_t\Phi_{p^\infty})^\Gamma$. The terms of this direct sum are finite with the exception of those $t \in T_{L'}$ lying over places of K' of split multiplicative reduction. For each such place, $({}_t\Phi_{p^\infty})^\Gamma \cong \mathbf{Q}_p/\mathbf{Z}_p$. Letting e' be the number of places of K' ramifying in L' for which A has split multiplicative reduction, we have

$$H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^\Gamma \sim H^1(\mathcal{O}_{K'}, A^0_{p^\infty}) \oplus (\mathbf{Q}_p/\mathbf{Z}_p)^{e'} \tag{6}$$

So the corank of $(H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^\Gamma)^G$ is the sum of the coranks of $H^1(\mathcal{O}_{K'}, A^0_{p^\infty})^G$ and $((\mathbf{Q}_p/\mathbf{Z}_p)^{e'})^G$.

For the first, we use the Kummer sequence

$$0 \to A^0(\mathcal{O}_{K'}) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to H^1(\mathcal{O}_{K'}, A^0_{p^\infty}) \to H^1(\mathcal{O}_{K'}, A^0) \to 0. \tag{7}$$

The group $(A^0(\mathcal{O}_{K'}) \otimes \mathbf{Q}_p/\mathbf{Z}_p)^G$ naturally contains a subgroup isomorphic to $(\mathbf{Q}_p/\mathbf{Z}_p)^r$, namely the image of $A^0(\mathcal{O}_K) \otimes \mathbf{Q}_p/\mathbf{Z}_p$,

In the group $((\mathbf{Q}_p/\mathbf{Z}_p)^{e'})^G$, we get a subgroup of corank e coming from the e places of K of split multiplicative reduction. Thus, we get the inequality on the order of vanishing.

Now, since

$$\begin{aligned} H^1(\mathcal{O}_{L'}, A^0_{p^\infty}) &= H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^+ \oplus H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^- \\ &= H^1(\mathcal{O}_{L'}, A^0_{p^\infty})^G \oplus H^1(\mathcal{O}_{L'}, (A^0_{(v)})_{p^\infty})^G, \end{aligned}$$

we have that the characteristic polynomials multiply and hence

$$L_p(L'/K', A; s) = L_p(L/K, A; s) L_p(L/K, A_{(v)}; s).$$

Since A over K' and $A_{(v)}$ each have either multiplicative reduction, or good ordinary reduction for each place ramifying in L'/K' the order of vanishing and first non-vanishing coefficient (up to p-unit) are understood by [1]. We let

$$\begin{aligned} \rho &= \mathrm{ord}_{\,s=1} L_p(L/K, A; s), \\ \rho' &= \mathrm{ord}_{\,s=1} L_p(L'/K', A; s), \\ \rho_{(v)} &= \mathrm{ord}_{\,s=1} L_p(L/K, A_{(v)}; s), \end{aligned}$$

and similarly for r and e. Thus,

$$\rho' = \rho + \rho_{(v)}$$

and

$$L_p^{(\rho')}(L'/K', A; 1) = L_p^{(\rho)}(L/K, A; 1) \cdot L_p^{(\rho_{(v)})}(L/K, A_{(v)}; 1).$$

To get the equality for order of vanishing, we note that the equality is now known for $A_{/K'}$ and $A_{(v)/K}$. So, we just need to show that $r' = r + r_{(v)}$ and $e' = e + e_{(v)}$. This follows by decomposing equation 6 into $\pm$ eigenspaces for G. The decomposition into $\pm$-eigenspaces

$$(\mathbf{Q}_p/\mathbf{Z}_p)^{e'} \sim (\bigoplus_{t\in T_{L'}} {}_t\Phi_{p^\infty})^{\Gamma} = (\bigoplus_{t\in T_{L'}} {}_t\Phi_{p^\infty})^{G\times\Gamma} \oplus (\bigoplus_{t\in T_{L'}} {}_t(\Phi_{(v)})_{p^\infty})^{G\times\Gamma}$$
$$\sim (\mathbf{Q}_p/\mathbf{Z}_p)^{e} \oplus (\mathbf{Q}_p/\mathbf{Z}_p)^{e(v)}$$

gives the equality for e' immediately (use the Tate parameterization to look at the group of connected components for places of multiplicative reduction and consider separately whether a place of K is split, inert, and ramified in K').

The $H^1(\mathcal{O}_{K'}, A^0_{p^\infty})$ term can be decomposed as before in sequence 7. For the Mordell-Weil groups, note that breaking $A(K')$ into its $\pm$ eigenspaces shows that $A(K)$ and $A_{(v)}(K)$ are independent sublattices which together generate a subgroup with index a power of 2. Hence the $r' = r + r_{(v)}$.

We now compare the expressions on the right side of the formula in the theorem term by term to see that the product of the corresponding terms for $A_{/K}$ and $A_{(v)/K}$ is that of $A_{/K'}$. By the previous paragraph (and since p is odd), we find that up to a p-adic unit:

$$\langle\ ,\ \rangle_{p,K'}(A) \approx \langle\ ,\ \rangle_{p,K}(A) \quad\cdot\quad \langle\ ,\ \rangle_{p,K}(A_v)$$

(Note: the factor of $1/[K' : K]$ which appears when changing base field is not significant here since it is prime to p.)

For the order and finiteness of $Ш$, note that $Ш_{K'}(A) = Ш_{K'}(A)^+ \oplus Ш_{K'}(A)^- = Ш_{K'}(A)^G \oplus Ш_{K'}(A_{(v)})^G$. A simple descent then shows that $Ш_{K'}(A)^G_{p^\infty} = Ш_K(A)_{p^\infty}$ and that $Ш_{K'}(A_{(v)})^G_{p^\infty} = Ш_K(A_{(v)})_{p^\infty}$ (using that the order of G is prime to p). So, $Ш_{K'}(A) = Ш_K(A)_{p^\infty} \oplus Ш_K(A_{(v)})_{p^\infty}$. Note that the argument for the $A_{p^\infty}(K)$ term on the right side of the formula is similar, but easier.

The $\mathcal{L}_v$-invariants and the orders of the groups of connected components $\prod m_v$ can be treated together. The product of the two terms is equal to

$$\frac{\prod_{v\not|\infty} A(K_v)/\mathbf{N}A(L_v)}{|\log_p \kappa(\gamma)|_p^e}$$

The denominators multiply since $e' = e + e_{(v)}$. The numerators multiply by Lemma 4.1. $\square$

References

[1] Jones, J.: Iwasawa L-functions of multiplicative Abelian varieties. Duke Math. J. **59**, 399-420 (1989)

[2] Jones, J.: p-adic heights for semi-stable Abelian varieties. Comp. Math. **73**, 31-56 (1990)

[3] Mazur, B.: Rational points on abelian varieties with values in towers of number fields. Invent. math. **18**, 183-266 (1972)

[4] Mazur, B., Tate, J.: "Canonical heights via biextensions", in Arithmetic and Geometry, vol I, Birkhäuser, 195-238 (1983)

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

[6] McCallum, W.: Duality theorems for Neŕon models. Duke Math. J. **53**, 1093-1124 (1986)

[7] McCallum, W.: Equivariant Cohomology, unpublished notes.

[8] Nasybullin, A.: Elliptic Tate curves over local Γ-extensions. Math. Notes of U.S.S.R. **13** 322-327 (1973)

[9] Perrin-Riou, B.: Descente infinie et hauteur p-adique sur les courbes elliptiques á multiplication complexe. Invent. math. **70**, 369-398 (1982)

[10] Perrin-Riou, B.: Théorie d'Iwasawa p-adique locale et global. Invent. math. **99**, 247-292 (1990)

[11] Schneider, P.: p-adic height pairings I. Invent. math. **69**, 401-409 (1982)

[12] Schneider, P.: Iwasawa L-functions of varieties over algebraic number fields. A first approach. Invent. math. **71**, 251-293 (1983)

[13] Schneider, P.: p-adic height pairings II. Invent. math. **79**, 329-374 (1985)

[14] Washington, L.: Introduction to Cyclotomic Fields. GTM **83**. Berlin-Heidelberg-New York:Springer (1982)

Department of Mathematics, Arizona State University, Tempe, AZ 85287