PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 143, Number 6, June 2015, Pages 2355–2364
S 0002-9939(2015)12459-8
Article electronically published on January 21, 2015

# AN EXAMPLE OF NON-COTORSION SELMER GROUP

KING FAI LAI, IGNAZIO LONGHI, KI-SENG TAN, AND FABIEN TRIHAN

(Communicated by Matthew A. Papanikolas)

Abstract. Let $A/K$ be an elliptic curve over a global field of characteristic $p > 0$. We provide an example where the Pontrjagin dual of the Selmer group of $A$ over a $\Gamma := \mathbb{Z}_p$-extension $L/K$ is not a torsion $\mathbb{Z}_p[[\Gamma]]$-module and show that the Iwasawa Main Conjecture for $A/L$ holds nevertheless.

## 1. Setting

Let $K$ be a global field of characteristic $p > 0$ and let $A/K$ be a non-isotrivial semistable elliptic curve of analytic rank 0 with split multiplicative reduction at a place $v_0$ of $K$. Let $L/K$ be a $\Gamma = \mathbb{Z}_p$-extension and $k \subset K$ be a subfield such that $K/k$ is a separable quadratic extension with $\mathrm{Gal}(K/k) = \{1, \tau\}$. We denote for any $n$, $K_n/K$ the $\mathbb{Z}/p^n$-extension and set $\Gamma^{(n)} := \mathrm{Gal}(L/K_n)$ and $\Gamma_n = \mathrm{Gal}(K_n/K)$. We assume that $L/K$ is anticyclotomic with respect to $k$, i.e. $L/k$ is Galois and $\mathrm{Gal}(L/k)$ is dihedral in the sense that we have a decomposition

$$\mathrm{Gal}(L/k) \simeq \mathrm{Gal}(L/K) \rtimes \mathrm{Gal}(K/k)$$

such that for any $\sigma \in \mathrm{Gal}(L/K)$ we have $\tau\sigma\tau^{-1} = \sigma^{-1}$ (where $\tau$ is abusively identified with its lift to $\mathrm{Gal}(L/k)$).

Let us assume moreover that $L/K$ is totally ramified above $v_0$ and unramified elsewhere. Furthermore, $A$ is assumed to be already defined over $k$ and to have split multiplicative reduction at the restriction of $v_0$ to $k$.

*Remark* 1.0.1. There are many known instances of elliptic curves satisfying these hypotheses. For example, let $\mathbb{F}$ be a finite field of characteristic $p > 2$ and consider the function fields $k = \mathbb{F}(s)$ and $K = \mathbb{F}(t)$, with $s = t^2$. Let $A$ be defined by the Weierstrass equation

$$A : y^2 = x(x+1)(x+s) = x(x+1)(x+t^2). \tag{1}$$

This is an elliptic curve having split multiplicative reduction at $t = 0$, $t = \infty$ and (if $-1$ is a square in $\mathbb{F}$) $t = \pm 1$, and good reduction at all other places. Therefore, as a divisor of $K$ the conductor $\mathfrak{n}$ of $A/K$ is the sum of these four places. The elliptic curve $A/K$ is well known to have Hasse-Weil L-function $L(A/K, s) \equiv 1$ : one way to prove it is to observe that $A$ is associated with a modular form and apply the corollary of [Tan93, Proposition 3]; another approach (closer to the methods of [Ta66]) is explained in [Shi92].

Received by the editors August 6, 2013 and, in revised form, January 21, 2014.
2010 *Mathematics Subject Classification.* Primary 11S40; Secondary 11R23, 11R34, 11R42, 11R58, 11G05, 11G10.
*Key words and phrases.* Abelian variety, Selmer group, Frobenius, Iwasawa theory, Stickelberger element, syntomic.

Equation (1) is an instance of Beauville surface: they exist in all characteristics and always satisfy the hypotheses. See [Lan91] for a full discussion and classification.

1.1. Let $i\colon A_{p^n} \hookrightarrow A$ be the group scheme of $p^n$-torsion of $A$. The $p^n$-Selmer group $\mathrm{Sel}_{p^n}(A/K)$ is defined to be the kernel of the composition

$$\mathrm{H}^1_{\mathrm{fl}}(K, A_{p^n}) \xrightarrow{i^*} \mathrm{H}^1_{\mathrm{fl}}(K, A) \xrightarrow{loc_K} \bigoplus_v \mathrm{H}^1_{\mathrm{fl}}(K_v, A)\,, \tag{2}$$

where $\mathrm{H}^\bullet_{\mathrm{fl}}$ denotes the flat cohomology and $loc_K$ is the localization map to the direct sum of local cohomology groups over all places of $K$. The same definition works over any finite extension $F/K$. Taking the direct limit as $n \to \infty$, we get

$$\mathrm{Sel}_{p^\infty}(A/F) := \mathrm{Ker}\left(\mathrm{H}^1_{\mathrm{fl}}(F, A_{p^\infty}) \longrightarrow \bigoplus_{\text{all } v} \mathrm{H}^1_{\mathrm{fl}}(F_v, A)\right) \tag{3}$$

where $A_{p^\infty}$ is the $p$-divisible group associated with $A$. The Selmer group $\mathrm{Sel}_{p^\infty}(A/L)$ is then defined by taking the inductive limit over all finite subextensions. The Galois group $\Gamma$ acts on $\mathrm{Sel}_{p^\infty}(A/L)$ turning it into a $\Lambda := \mathbb{Z}_p[[\Gamma]]$-module. We denote

$$X_p(A/L) := \mathrm{Sel}_{p^\infty}(A/L)^\vee$$

the Pontrjagin dual of this $\Lambda$-module.

Similarly, we define for any finite extension $F/K$ the Tate-Shafarevich group of $A/F$ as

$$Ш(A/F) := \mathrm{Ker}\left(\mathrm{H}^1_{\mathrm{fl}}(F, A) \longrightarrow \bigoplus_{\text{all } v} \mathrm{H}^1_{\mathrm{fl}}(F_v, A)\right) \tag{4}$$

and $Ш(A/L)$ as the inductive limit of $Ш(A/F)$ over all finite intermediate extensions.

In this short note, we study the Iwasawa theory of $A/L$ as formulated by [Maz72]. According to the Iwasawa Main Conjecture (see [SU13] for the best result so far in the number field case), the characteristic ideal of the finitely generated $\Lambda$-module $X_p(A/L)$ should coincide with the ideal generated by an element of $\Lambda$ called the $p$-adic $L$-function and having the property to interpolate the values at $s = 1$ of the Hasse-Weil $L$-function of $A/K$ twisted by characters. Here we provide under our assumptions on $A$ and $L/K$, a proof of the Iwasawa Main Conjecture in the following sense: we show in §2 that $X_p(A/L)$ is a finitely generated non-torsion $\Lambda$-module with therefore a trivial characteristic ideal. In §3, we show that the $p$-adic $L$-function of $A/L$ is zero proving as a consequence the Iwasawa Main Conjecture for $A/L$.

In the following, with a slight abuse of notation we shall often use the same symbol to denote places in different fields: e.g., $L_{v_0}$ will be the completion of $L$ at the only place above $v_0$. Also, for $v$ a place of $K$ put $\Gamma_v := \mathrm{Gal}(L_v/K_v)$. Since $\Gamma_{v_0}$ can be identified with $\Gamma$, we won't distinguish between the two. Various restriction maps will be used. Among them, $\mathrm{Res}_{L/K_n}$ and $res_{L/K_n}$ are respectively the maps $\mathrm{H}^1_{\mathrm{fl}}(K_n, A_{p^\infty}) \to \mathrm{H}^1_{\mathrm{fl}}(L, A_{p^\infty})^{\Gamma^{(n)}}$ and $\mathrm{H}^1_{\mathrm{fl}}(K_n, A) \to \mathrm{H}^1_{\mathrm{fl}}(L, A)^{\Gamma^{(n)}}$.

## 2. The algebraic side

In the following, we fix a topological generator $\gamma$ of $\Gamma$ and put $T := \gamma - 1 \in \Lambda$; then $T$ is a generator of the augmentation ideal $I$. By abuse of notation, we also identify $\gamma$ with a generator of $\Gamma_n$ for all $n$.

**Lemma 2.0.1.** *The groups $A(K)$, $Ш(A/K)$ and $\mathrm{Sel}_{p^\infty}(A/K)$ are all finite.*

*Proof.* By [Ta66] (and [Mil75] for the $p$-part of Ш - see also the comments on Milne's webpage http://www.jmilne.org/math/articles/index.html for $p = 2$) it is known that analytic rank 0 implies that the full Birch and Swinnerton-Dyer conjecture holds for $A/K$. □

Since $A$ has split multiplicative reduction at $v_0$, it is a Tate curve on the completion $K_{v_0}$: we denote the local Tate period by $Q$.

**Lemma 2.0.2.** *One has $A_{tor}(K) = A_{tor}(L)$. In particular, the group $A_{tor}(L)$ is finite.*

*Proof.* To see this, first notice that the constant field does not grow in $L_{v_0}/K_{v_0}$, since it is a totally ramified extension. Besides, if a root $Q^{1/n}$ of $Q$ is not already in $K_{v_0}$, then it cannot belong to $L_{v_0}$, either because then $Q^{1/n}$ is not separable over $K_{v_0}$ (for $n$ a power of $p$) or because $L/K$ is a $p$-extension (for $(p, n) = 1$). The explicit description of the torsion points of $A(L_{v_0})$ in terms of roots of unity and of $Q$ then implies $A_{tor}(K_{v_0}) = A_{tor}(L_{v_0})$. To conclude, it suffices to observe that $L \cap K_{v_0} = K$, exploiting once again the totally ramified hypothesis. □

**Corollary 2.0.3.** *The groups $\mathrm{H}^1(\Gamma^{(m)}, A_{p^\infty}(L))$ are finite of bounded orders.*

*Proof.* By the usual Herbrad quotient argument, for every $n \geq m$,

$$|\,\mathrm{H}^1(K_n/K_m, A_{p^\infty}(K_n))| = |\hat{\mathrm{H}}^0(K_n/K_m, A_{p^\infty}(K_n))| \leq |A_{p^\infty}(K_m)| \leq |A_{p^\infty}(L)|.$$

□

2.1. If $v$ is in the $\mathrm{Gal}(K/k)$-orbit of $v_0$, then since $L/k$ is Galois, $v$ is ramified under $L/K$, and hence by our ramification hypotheses, $v = v_0$. Besides, we are assuming that $A$ is already a Tate curve over $k_{v_0}$ and thus we have $Q \in k_{v_0}^\times$.

Let $\mathcal{N} \subseteq K_{v_0}^\times$ denote the group of universal norms of the local extension $L_{v_0}/K_{v_0}$. Write rec for the reciprocity map of local class field theory: then we have $\mathrm{rec}(\tau(x)) = \tau\mathrm{rec}(x)\tau^{-1}$ for any $x \in K_{v_0}^\times$, and hence $\tau(x) \equiv x^{-1} \mod \mathcal{N}$. In particular $Q \equiv Q^{-1} \mod \mathcal{N}$, so that $Q^2 \in \mathcal{N}$. As $K_{v_0}^\times/\mathcal{N} \simeq \Gamma$ is torsion free, we deduce that $Q \in \mathcal{N}$.

**Lemma 2.1.1.** *Let $v$ be a place of $K$. Then*

$$\mathrm{H}^1(\Gamma_v, A(L_v)) \simeq \begin{cases} 0 & \text{if } v \text{ is a place of good reduction;} \\ \text{a finite group} & \text{if } v \text{ is an unramified place of bad reduction;} \\ \mathbb{Q}_p/\mathbb{Z}_p & \text{if } v = v_0. \end{cases}$$

*Proof.* For unramified places, this is a consequence of [Mil86a, I, Proposition 3.8]. As for $v_0$, observe that for any $n$ we have $A(K_{n,v_0}) \simeq K_{n,v_0}^\times/Q^{\mathbb{Z}}$. We deduce the exact sequence

$$\mathrm{H}^1(\Gamma_n, K_{n,v_0}^\times) \longrightarrow \mathrm{H}^1(\Gamma_n, A(K_{n,v_0})) \longrightarrow \mathrm{H}^2(\Gamma_n, Q^{\mathbb{Z}}) \longrightarrow \mathrm{H}^2(\Gamma_n, K_{n,v_0}^\times)\,,$$

that we can rewrite

$$0 \longrightarrow \mathrm{H}^1(\Gamma_n, A(K_{n,v_0})) \longrightarrow Q^{\mathbb{Z}}/Q^{p^n\mathbb{Z}} \longrightarrow K_{v_0}^\times/N_{K_{n,v_0}/K_{v_0}}(K_{n,v_0}^\times)\,. \tag{5}$$

Since $Q \in \mathcal{N}$, the map $Q^{\mathbb{Z}} \to K_{v_0}^\times/N_{K_{n,v_0}/K_{v_0}}(K_{n,v_0}^\times)$ is trivial. Thus we obtain

$$\mathrm{H}^1(\Gamma_n, A(K_{n,v_0})) \simeq p^{-n}\mathbb{Z}/\mathbb{Z}\,. \tag{6}$$

As $n$ varies, this isomorphism is compatible with the inflation maps on the left and the canonical inclusions on the right, thereby proving the assertion. □

**Corollary 2.1.2.** *The group* $\mathrm{Sel}_{p^\infty}(A/L)^\Gamma$ *is cofinitely generated over* $\mathbb{Z}_p$ *of corank at most one. The* $\Lambda$*-module* $X_L$ *is finitely generated.*

*Proof.* Applying the snake lemma and the Hochschild-Serre spectral sequence ([Mil80, III, 2.21]) to the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}_{p^\infty}(A/K) & \longrightarrow & \mathrm{H}^1_{\mathrm{fl}}(K, A_{p^\infty}) & \longrightarrow & \bigoplus_v \mathrm{H}^1_{\mathrm{fl}}(K_v, A) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Sel}_{p^\infty}(A/L)^\Gamma & \longrightarrow & \mathrm{H}^1_{\mathrm{fl}}(L, A_{p^\infty})^\Gamma & \longrightarrow & \bigoplus_v \mathrm{H}^1_{\mathrm{fl}}(L_v, A)^{\Gamma_v} \end{array}$$

we get an exact sequence

$$\mathrm{H}^1(\Gamma, A_{p^\infty}(L)) \longrightarrow H \longrightarrow \mathrm{Sel}_{p^\infty}(A/L)^\Gamma / \mathrm{Sel}_{p^\infty}(A/K) \longrightarrow \mathrm{H}^2(\Gamma, A_{p^\infty}(L)) = 0,$$

where $H$ is a subgroup of $\oplus_v \mathrm{H}^1(\Gamma_v, A(L_v))$ and the equality on the right comes from the fact that $\Gamma$ has cohomological dimension 1. The claim follows from Lemma 2.1.1, since $A_{p^\infty}(L)$ and $\mathrm{Sel}_{p^\infty}(A/K)$ are finite groups thanks to Lemmas 2.0.2 and 2.0.1. The second assertion is a consequence of the first by the usual topological Nakayama Lemma. □

*Remark* 2.1.3. The group $G := \mathrm{Gal}(K/k)$ acts on $\mathrm{H}^1_{\mathrm{fl}}(K, A)$ and the other cohomology groups appearing in the above discussion. In particular, since $v_0$ does not split in $K/k$, $G$ acts on $\mathrm{H}^1(\Gamma, A(L_{v_0}))$. The connecting homomorphism in (5) is a map of $G$-modules and so is the isomorphism (6), because $Q \in k_v$. Therefore we have

$$\mathrm{H}^1(\Gamma, A(L_{v_0})) = \mathrm{H}^1(\Gamma, A(L_{v_0}))^G .$$

2.2. Consider the localization map:

$$loc_K \colon \mathrm{H}^1_{\mathrm{fl}}(K, A) \longrightarrow \bigoplus_v \mathrm{H}^1_{\mathrm{fl}}(K_v, A).$$

The generalized Cassels-Tate dual exact sequence of [GT07, Main Theorem] identifies, for any integer $m$, the cokernel of $loc_K$ with the Pontryagin dual of

$$T_m \mathrm{Sel}(A^t/K) := \varprojlim \mathrm{Sel}_{m^n}(A^t/K) .$$

In our case $A$ is an elliptic curve, so $A = A^t$. Taking the inverse limit of the sequence

$$0 \longrightarrow A(K)/m^n A(K) \longrightarrow \mathrm{Sel}_{m^n}(A/K) \longrightarrow Ш(A/K)[m^n] \longrightarrow 0$$

we see that $T_m \mathrm{Sel}(A/K)$ is always finite, and trivial for almost every $m$, because so are $A(K)$ and $Ш(A/K)$. Hence $loc_K$ has finite cokernel and, by the inclusions

$$\mathrm{H}^1(\Gamma, A(L_{v_0})) \subseteq \mathrm{H}^1_{\mathrm{fl}}(K_{v_0}, A) \subseteq \bigoplus_v \mathrm{H}^1_{\mathrm{fl}}(K_v, A) ,$$

it follows that

$$\mathcal{H} := \mathrm{H}^1(\Gamma, A(L_{v_0})) \cap loc_K\big(\mathrm{H}^1_{\mathrm{fl}}(K, A)\big)$$

has finite index in $\mathrm{H}^1(\Gamma, A(L_{v_0}))$. Since the latter is $p$-divisible, we must have

$$\mathcal{H} = \mathrm{H}^1(\Gamma, A(L_{v_0})) \subseteq loc_K\big(\mathrm{H}^1_{\mathrm{fl}}(K, A)\big). \tag{7}$$

Write $E := loc_K^{-1}\big(\mathrm{H}^1(\Gamma, A(L_{v_0}))\big)$. We have an exact sequence

$$0 \longrightarrow Ш(A/K) \longrightarrow E \xrightarrow{loc_K} \mathrm{H}^1(\Gamma, A(L_{v_0})) \longrightarrow 0. \tag{8}$$

It follows that $loc_L(res_{L/K}(E)) = 0$, because restriction and localization commute and $\mathrm{H}^1(\Gamma, A(L_{v_0}))$ has trivial image in $\oplus_v \mathrm{H}^1_{\mathrm{fl}}(L_v, A)$.

Let $D$ be the divisible part of $E$: then $D \simeq \mathbb{Q}_p/\mathbb{Z}_p$, since $Ш(A/K)$ is a finite group. By construction $D$ is a subgroup of $\mathrm{H}^1_{\mathrm{fl}}(K, A)$, killed by $loc_L \circ res_{L/K}$: that is,

$$res_{L/K}(D) \subset Ш_{p^\infty}(A/L)^\Gamma. \tag{9}$$

2.3. For the proof that $X_p(A/L)$ is not torsion, we are going to reason by contradiction. Thus in the following we assume that $X_p(A/L)$ is torsion.

For each $n$, let $Ш_{p^\infty}(A/K_n)_{div}$ and $\mathrm{Sel}_{p^\infty}(A/K_n)_{div}$ respectively denote the $p$-divisible part of $Ш_{p^\infty}(A/K_n)$ and $\mathrm{Sel}_{p^\infty}(A/K_n)$. Denote

$$\mathfrak{b}_n = Ш_{p^\infty}(A/K_n)/Ш_{p^\infty}(A/K_n)_{div} = \mathrm{Sel}_{p^\infty}(A/K_n)/\mathrm{Sel}_{p^\infty}(A/K_n)_{div}.$$

Let $\mathfrak{r}^n_m : \mathfrak{b}_m \to \mathfrak{b}_n$ and $\mathfrak{k}^n_m : \mathfrak{b}_n \to \mathfrak{b}_m$ be the morphisms induced respectively from the restriction

$$\mathrm{H}^1_{\mathrm{fl}}(K_m, A) \longrightarrow \mathrm{H}^1_{\mathrm{fl}}(K_n, A)$$

and the co-restriction

$$\mathrm{H}^1_{\mathrm{fl}}(K_n, A) \longrightarrow \mathrm{H}^1_{\mathrm{fl}}(K_m, A).$$

The Cassels-Tate pairing induces, for every $n$, a perfect alternating pairing:

$$\langle\,,\rangle_n \colon \mathfrak{b}_n \times \mathfrak{b}_n \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p\,.$$

Then the module $\mathfrak{b}_\infty := \varinjlim \mathfrak{b}_m$ is identified with the Pontryagin dual of $\mathfrak{b} := \varprojlim_n \mathfrak{b}_n$. Set

$$\mathrm{Sel}_{div}(A/L) := \varinjlim_n \mathrm{Sel}_{p^\infty}(A/K_n)_{div}\,,$$

$$Y_p(A/K_n) := (\mathrm{Sel}_{p^\infty}(A/K_n)_{div})^\vee,$$

and

$$Y_p(A/L) := \varprojlim_n Y_p(A/K_n) = \mathrm{Sel}_{div}(A/L)^\vee.$$

Again, the notation $\bullet^\vee$ denotes the Pontryagin dual of $\bullet$. We have the following short exact sequence:

$$0 \longrightarrow \mathfrak{b} \longrightarrow X_p(A/L) \longrightarrow Y_p(A/L) \longrightarrow 0. \tag{10}$$

In particular, if $X_p(A/L)$ is a finitely generated torsion $\Lambda$-module, so are the modules $\mathfrak{b}$ and $Y_p(A/L)$.

**Definition 2.3.1.** An element $f \in \Lambda(\Gamma)$ is simple if there exist $\gamma \in \Gamma - \Gamma^p$ and $\zeta \in \boldsymbol{\mu}_{p^\infty}$ such that

$$f = f_{\gamma,\zeta} := \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)} (\gamma - \sigma(\zeta)).$$

The following result was proved in [Tan12, Theorem 5],

**Theorem 2.3.1.** *Suppose $X_p(A/L)$ is a torsion $\Lambda$-module. Then there exist pairwise relatively prime simple elements $f_1, ..., f_m$ $(m \geq 1)$ such that*

$$f_1 \cdots f_m \cdot \mathrm{Sel}_{div}(A/L) = 0.$$

We will also need the following two lemmas:

**Lemma 2.3.2.** *For $n \geq m$ the restriction map*

$$\mathrm{Sel}_{p^\infty}(A/K_m)_{div} \longrightarrow (\mathrm{Sel}_{p^\infty}(A/K_n)^{\Gamma^{(m)}})_{div}$$

*is surjective.*

*Proof.* The commutative diagram of exact sequences

$$\begin{array}{ccccccc}
\mathrm{Sel}_{p^\infty}(A/K_m)_{div} & = & \mathrm{Sel}_{p^\infty}(A/K_m)_{div} & \hookrightarrow & \mathrm{Sel}_{p^\infty}(A/K_m) & \twoheadrightarrow & \mathfrak{b}_m \\
\downarrow{\scriptstyle j'} & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \mathfrak{r}_m^n} \\
(\mathrm{Sel}_{p^\infty}(A/K_n)^{\Gamma^{(m)}})_{div} & \subset & (\mathrm{Sel}_{p^\infty}(A/K_n)_{div})^{\Gamma^{(m)}} & \hookrightarrow & \mathrm{Sel}_{p^\infty}(A/K_n)^{\Gamma^{(m)}} & \longrightarrow & \mathfrak{b}_n^{\Gamma^{(m)}}
\end{array}$$

induces the exact sequence

$$\mathrm{Ker}(\mathfrak{r}_m^n) \longrightarrow \mathrm{Coker}(j) \longrightarrow \mathrm{Coker}(i).$$

Since $\mathrm{Ker}(\mathfrak{r}_m^n)$ is finite while $\mathrm{Coker}(j')$ is $p$-divisible, it is sufficient to show that $\mathrm{Coker}(i)$ is annihilated by some positive integer. Consider the commutative diagram of exact sequences

$$\begin{array}{ccccc}
\mathrm{Sel}_{p^\infty}(A/K_m) & \hookrightarrow & \mathrm{H}^1_{\mathrm{fl}}(K_m, A_{p^\infty}) & \xrightarrow{loc_m} & \prod_{\mathrm{all}\ v} \mathrm{H}^1_{\mathrm{fl}}(K_{mv}, A) \\
\downarrow{\scriptstyle i} & & \downarrow{\scriptstyle res_m^n} & & \downarrow{\scriptstyle r_m^n} \\
\mathrm{Sel}_{p^\infty}(A/K_n)^{\Gamma^{(m)}} & \hookrightarrow & \mathrm{H}^1_{\mathrm{fl}}(K_n, A_{p^\infty})^{\Gamma^{(m)}} & \xrightarrow{loc_n} & \prod_{\mathrm{all}\ w} \mathrm{H}^1_{\mathrm{fl}}(K_{nw}, A)^{\Gamma^{(m)}_w}
\end{array}$$

that induces the exact sequence

$$\mathrm{Ker}\left(\ \mathrm{Im}(loc_m) \xrightarrow{r_m^n} \mathrm{Im}(loc_n)\ \right) \longrightarrow\ \mathrm{Coker}(i) \longrightarrow\ \mathrm{Coker}(res_m^n)\,.$$

By the Hochschild-Serre spectral sequence, the right-hand term $\mathrm{Coker}(res_m^n)$ is a subgroup of $\mathrm{H}^2(K_n/K_m, A_{p^\infty}(K_n))$, and hence is annihilated by $p^{d(n-m)} = [K_n : K_m]$. Similarly, the left-hand term, being a subgroup of $\prod_v \mathrm{H}^1(K_{nv}/K_{mv}, A(K_{nv}))$, is also annihilated by $[K_n : K_m]$. □

**Lemma 2.3.3.** *If $X_p(A/L)$ is a torsion $\Lambda$-module, then there exists some $N$ such that*

$$\mathrm{Sel}_{p^\infty}(A/K_n)_{div} = (\mathrm{Sel}_{p^\infty}(A/K_n)_{div})^{\Gamma^{(m)}} = (\mathrm{Sel}_{p^\infty}(A/K_n)^{\Gamma^{(m)}})_{div}$$

*holds for all $n \geq m \geq N$.*

*Proof.* The second equality is an easy consequence of the first one. The assumption $\Gamma = \gamma^{\mathbb{Z}_p}$ implies that if $f \in \Lambda$ is simple, then $f$ divides $\gamma^{p^m} - 1$ for some $m$. Therefore, by Theorem 2.3.1, there exists an integer $N$ such that $(\gamma^{p^N} - 1)\,\mathrm{Sel}_{div}(A/L)^{\Gamma^{(n)}} = 0$ for every $n$. The kernel of the map $\mathrm{Sel}_{p^\infty}(A/K_n)_{div} \to \mathrm{Sel}_{div}(A/L)^{\Gamma^{(n)}}$ is finite since $A_{p^\infty}(L)$ is finite. This implies that $(\gamma^{p^N} - 1)\,\mathrm{Sel}_{p^\infty}(A/K_n)_{div}$ must be trivial, because it is both finite and $p$-divisible. □

**Proposition 2.3.4.** *The $\mathbb{Z}_p$-rank of $\mathfrak{b}/T\mathfrak{b}$ equals* 1.

*Proof.* First, note that, by Lemma 2.3.2, the finiteness of $\mathrm{Sel}_{p^\infty}(A/K)$ implies $\mathrm{Sel}_{p^\infty}(A/K_n)^\Gamma$ is finite for every $n \geq 0$. Then Lemma 2.3.2 and Lemma 2.3.3 imply that for $n \gg 0$,

$$\mathrm{Sel}_{div}(A/L)^\Gamma = (\mathrm{Sel}_{div}(A/L)^{\Gamma^{(n)}})^\Gamma = (\mathrm{Sel}_{p^\infty}(A/K_n)_{div})^\Gamma \subset \mathrm{Sel}_{p^\infty}(A/K_n)^\Gamma$$

is also finite. By duality, the $\mathbb{Z}_p$-module $Y_p(A/L)/TY_p(A/L)$ is finite. This means the characteristic ideal of $Y_p(A/L)$ is relatively prime to $(T)$. Hence, there is some $\xi \in \Lambda$, relatively prime to $T$ such that $\xi \cdot Y_p(A/L)$ is pseudo-null (finite). Replacing $\xi$ by some suitable $p^m\xi$, we can assert that $\xi \cdot Y_p(A/L) = 0$. Then $Y_p(A/L)[T]$, being annihilated by $T$ and $\xi$, is also finite (hence trivial, because $Y_p(A/L)$, as a submodule of the $\mathbb{Z}_p$-free part of $X_p(A/L)$, is a free $\mathbb{Z}_p$-module of finite rank). Since (10) and the snake lemma yield the exact sequence

$$Y_p(A/L)[T] \longrightarrow \mathfrak{b}/T\mathfrak{b} \longrightarrow X_p(A/L)/TX_p(A/L) \longrightarrow Y_p(A/L)/TY_p(A/L)\,,$$

it follows from Corollary 2.1.2 that the $\mathbb{Z}_p$-rank of $\mathfrak{b}/T\mathfrak{b}$ is at most 1.

For the other inequality, consider the composition

$$\pi\colon\ D \xrightarrow{res_{L/K}} Ш_{p^\infty}(A/L)^\Gamma \longrightarrow \mathfrak{b}_\infty^\Gamma\ . \tag{11}$$

Let Æ denote the preimage of $D$ under the natural surjection from $\mathrm{H}^1(K, A_{p^\infty})$ to the $p$-primary part of $\mathrm{H}^1(K, A)$. Because $A(K)$ is finite, the exact sequence

$$0 \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \otimes A(K) \longrightarrow Æ \longrightarrow D \longrightarrow 0$$

implies that $Æ \simeq D$ is of corank 1 over $\mathbb{Z}_p$. It follows that $\mathrm{Res}_{L/K}(Æ) \subset \mathrm{Sel}_{p^\infty}(A/L)^\Gamma$ is also of corank 1 over $\mathbb{Z}_p$, since $\mathrm{Ker}(\mathrm{Res}_{L/K}) = \mathrm{H}^1(\Gamma, A_{p^\infty}(L))$ is of finite order, by Corollary 2.0.3. If the image of $\pi$ were finite (and thus trivial, since $D$ is $p$-divisible), then $\mathrm{Res}_{L/K}(Æ)$ would be contained in $\mathrm{Sel}_{div}(A/L)^\Gamma$, which has just been shown to be finite. This is absurd. Therefore, the corank of $\mathfrak{b}_\infty^\Gamma$ is at least 1, and the desired inequality followed by the duality. □

Proposition 2.3.4 implies that there exist some $r \geq 1$ and $\xi_i \in \Lambda$, $i = 1, ..., s$, coprime to $T$ such that $\mathfrak{b}$ is pseudo-isomorphic to $[\mathfrak{b}] := \Lambda/T^r\Lambda \oplus \bigoplus_i^s \Lambda/\xi_i\Lambda$. Since $[\mathfrak{b}]$ contains no non-trivial pseudo-null submodule, we actually have a short exact sequence

$$0 \longrightarrow \Lambda/T^r\Lambda \oplus \bigoplus_i^s \Lambda/\xi_i\Lambda \longrightarrow \mathfrak{b} \longrightarrow N \longrightarrow 0, \tag{12}$$

with $N$ pseudo-null. For each $n$, let $\mathfrak{r}_n : \mathfrak{b}_n \to \mathfrak{b}_\infty$ and $\mathfrak{k}_n : \mathfrak{b} \to \mathfrak{n}_n$ be the natural maps associated to the injective and projective limits. They are dual to each other.

**Lemma 2.3.5.** *The kernel of $\mathfrak{r}_n$ and the cokernel of $\mathfrak{k}_n$ are of bounded orders as $n$ varies.*

*Proof.* Suppose the natural projection $\mathrm{Sel}_{p^\infty}(A/K_n) \twoheadrightarrow \mathfrak{b}_n$ sends each $x$ to $\bar{x}$. Assume that $\bar{x} \in \mathrm{Ker}(\mathfrak{r}_n)$. Then $\mathrm{Res}_{L/K_n}(x) \in \mathrm{Sel}_{div}(A/L)$. Consider the restriction map

$$\mathrm{R}_n : \mathrm{Sel}_{p^\infty}(A/K_n)_{div} \longrightarrow \mathrm{Sel}_{div}(A/L).$$

Since $\mathrm{Sel}_{p^\infty}(A/L)$ is cotorsion over $\Lambda$, the divisible subgroup $\mathrm{Sel}_{div}(A/L)$ must be cofinitely generated over $\mathbb{Z}_p$. Thus for $n$ sufficiently large, $\mathrm{R}_n$ is surjective. For such $n$, there exists $y \in \mathrm{Sel}_{p^\infty}(A/K_n)_{div}$ such that $\mathrm{Res}_{L/K_n}(y) = \mathrm{Res}_{L/K_n}(x)$.

Since $\overline{x-y} = \bar{x}$ and $x - y$ is contained in $\mathrm{Ker}(\mathrm{Res}_{L/K_n}(x)) = \mathrm{H}^1(\Gamma^{(n)}, A_{p^\infty}(L))$, by Corollary 2.0.3, the order of $\mathrm{Ker}(\mathfrak{r}_n)$ is bounded. □

**Lemma 2.3.6.** *Let $r$ be as in* (12). *Then the indexes of the subgroups $\mathfrak{k}_n(\mathfrak{b}[T^r]) \subset \mathfrak{b}_n[T^r]$ are bounded as $n$ varies.*

*Proof.* Lemma 2.3.5 implies that $\mathfrak{b}_n[T^r]/\mathfrak{k}_n(\mathfrak{b}) \cap \mathfrak{b}_n[T^r]$, embedded as a subgroup of $\mathfrak{b}_n/\mathfrak{k}_n(\mathfrak{b})$, is of bounded order. It is sufficient to show that $\mathfrak{e}_n := \mathfrak{k}_n(\mathfrak{b}) \cap \mathfrak{b}_n[T^r]/\mathfrak{k}_n(\mathfrak{b}[T^r])$ is also of bounded order. Denote $\mathfrak{f}_n := \mathfrak{k}_n(\mathfrak{b})/\mathfrak{k}_n(\mathfrak{b}[T^r])$. Then $\mathfrak{e}_n \subset \mathfrak{f}_n[T^r]$. Suppose the pseudo-null $N$ in (12) is annihilated by some $\eta$ coprime to $T$. Then $g = \eta \cdot \xi_1 \cdot \cdots \cdot \xi_s$ is also coprime to $T$ and we have $g \cdot \mathfrak{b} \in [\mathfrak{b}][T^r] \subset \mathfrak{b}[T^r]$. This implies $g \cdot \mathfrak{f}_n = 0$, and hence $\mathfrak{e}_n$ is annihilated by some $p$-power $p^c \in (T^r, g) \subset \Lambda$. Since $\mathfrak{b}$ is $\Lambda$-torsion, it is a finitely generated $\mathbb{Z}_p$-module. We have the composition of surjective homomorphisms $\mathbb{Z}_p^l \to \mathfrak{b} \to \mathfrak{k}_n(\mathfrak{b}) \to \mathfrak{f}_n$ for some $l$. Then $\varrho^{-1}(\mathfrak{e}_n)$ is a free $\mathbb{Z}_p$-module of rank at most $l$ and we have a surjective homomorphism $\varrho^{-1}(\mathfrak{e}_n) \to \mathfrak{e}_n$. Therefore, $\mathfrak{e}_n$ can be generated by a subset of cardinality at most $l$. Hence its order is bounded by $p^{lc}$. □

2.4. In order to exploit the anticyclotomic assumption, we now consider the action of $G := \mathrm{Gal}(K/k) = \langle \tau \rangle$ on $\mathfrak{b}$. We lift $G$ to a subgroup of $\mathrm{Gal}(L/k)$. Note that the maps $loc_K$ of (8) and $\pi$ of (11) are both compatible with the action of $G$.

**Lemma 2.4.1.** *There exists $x \in \mathfrak{b}[T^r]^G$ such that $[\mathfrak{b}[T^r] : \Lambda\, x] < \infty$.*

*Proof.* Remark 2.1.3 yields that $(1-\tau)D$ is contained in $\mathrm{Ker}(loc_K) = Ш(A/K)$ and hence is trivial (because $D$ is divisible). Thus we have $\pi(D) = \pi(D_G) = \pi(D)_G$ and by duality (see the proof of Proposition 2.3.4) it follows that $(\mathfrak{b}/T\mathfrak{b})^G$ has rank 1 over $\mathbb{Z}_p$. Also the image of $\mathfrak{b}[T^r]$ in $\mathfrak{b}/T\mathfrak{b}$ is of $\mathbb{Z}_p$-rank 1, by (12), so there must be $y \in \mathfrak{b}[T^r]$ such that $y \bmod T\mathfrak{b}$ is $G$-invariant and has infinite order. Choose $x := (1+\tau)y$. Then $x \in \mathfrak{b}[T^r]^G$ and $\Lambda\, x$ has finite index in $\mathfrak{b}[T^r] \sim \Lambda/T^r\Lambda$ since $x \equiv 2y \pmod{T\mathfrak{b}}$ generates a free $\mathbb{Z}_p$-module in $\mathfrak{b}/T\mathfrak{b}$. □

Let $\mathfrak{c} := \Lambda\, x$ and $\mathfrak{c}_n := \mathfrak{k}_n(\mathfrak{c})$.

**Lemma 2.4.2.** *As $n$ varies, the orders of the cokernels of the maps $\mathfrak{c}_n \to \mathfrak{b}_n[T^r]$ and $\mathfrak{c}_n \to \mathfrak{b}_n \to \mathfrak{b}_n/T^r\mathfrak{b}_n$ are bounded.*

*Proof.* By (12) the cokernel of $\mathfrak{b}[T^r] \to \mathfrak{b} \to \mathfrak{b}/T^r\mathfrak{b}$ is finite. Then apply Lemma 2.3.6 and Lemma 2.4.1. □

**Lemma 2.4.3.** *We have*

$$\langle \mathfrak{c}_n, \mathfrak{c}_n \rangle_n \subset (\mathbb{Q}_p/\mathbb{Z}_p)[2].$$

So $\langle \mathfrak{c}_n, \mathfrak{c}_n \rangle_n$ has at most 2 elements and it is trivial if $p \neq 2$. Let $^\# : \Lambda \to \Lambda$ denote the $\mathbb{Z}_p$-algebra isomorphism induced by $\gamma \mapsto \gamma^{-1}$, $\gamma \in \Gamma$.

*Proof.* Write $x_n := \mathfrak{k}_n(x)$. For any $\lambda \in \Lambda$ we have

$$\langle x_n, \lambda x_n \rangle_n = -\langle \lambda x_n, x_n \rangle_n = -\langle x_n, \lambda^\# x_n \rangle_n\,, \tag{13}$$

using first the fact that $\langle\ ,\ \rangle_n$ is alternating and then its $\Gamma$-equivariance. On the other hand, the pairing is also $G$-invariant and $x = \tau x$ implies

$$\langle x_n, \lambda x_n \rangle_n = \langle \tau x_n, \tau(\lambda x_n) \rangle_n = \langle x_n, \lambda^\# x_n \rangle_n\,, \tag{14}$$

because $\tau(\lambda x) = (\tau\lambda\tau^{-1})\tau x$ and the action of $\tau$ on $\Lambda$ is precisely $\lambda \mapsto \lambda^{\#}$, by the anticyclotomic hypothesis. Equalities (13) and (14) together prove

$$2\langle x_n, \lambda^{\#} x_n\rangle_n = 0$$

and this suffices, since $\mathfrak{c}_n = \Lambda\, x_n$. □

2.5. Now we can finally obtain a contradiction. The Cassels-Tate pairing makes $\mathfrak{b}_n[T^r]$ and $\mathfrak{b}_n/T^r\mathfrak{b}_n$ dual to each other . Lemma 2.4.2 implies that the subgroup

$$\langle \mathfrak{c}_n, \mathfrak{c}_n\rangle_n \subseteq \langle \mathfrak{b}_n[T^r], \mathfrak{b}_n/T^r\mathfrak{b}_n\rangle_n$$

has bounded index as $n$ varies. Since $\pi(D) \subseteq \mathfrak{b}_\infty[T] \subseteq \mathfrak{b}_\infty[T^r] = \varinjlim_n \mathfrak{b}_n[T^r]$ is infinite, we must have

$$\bigcup_n \langle \mathfrak{c}_n, \mathfrak{c}_n\rangle_n = \mathbb{Q}_p/\mathbb{Z}_p\,,$$

a contradiction to Lemma 2.4.3.

## 3. The analytic side

In this example $X_p(A/L)$ is non-torsion, whence its characteristic ideal is trivial. In the spirit of the Iwasawa Main Conjecture one expects that the corresponding $p$-adic $L$-function should be 0. Here we verify this.

In the function field setting, non-isotrivial elliptic curves are known to be modular: that is, there is a cuspidal automorphic function $f$ associated with $A$; its level is $\mathfrak{n}$, the conductor of $A/K$ (as a divisor of $K$). For any $n \geq 0$, let $\mathfrak{d}_n$ denote the divisor $nv_0$ and let $K(\mathfrak{d}_n)/K$ be the corresponding ray class field. It is shown in [Tan93] how to construct a modular element $\Theta_{\mathfrak{d}_n,f} \in \mathbb{Z}_p[\mathrm{Gal}(K(\mathfrak{d}_n)/K)]$, such that for each $\omega \in \mathrm{Gal}(K(\mathfrak{d}_n)/K)^\vee$ one has

$$\omega(\Theta_{\mathfrak{d}_n,f}) = \tau_\omega \cdot L(A, \omega, 1)\,, \tag{15}$$

where $\tau_\omega$ is a Gauss sum.

By [Tan93, Proposition 2, 2.(d)], the maps

$$\mathbb{Z}_p[\mathrm{Gal}(K(\mathfrak{d}_{n+1})/K)] \longrightarrow \mathbb{Z}_p[\mathrm{Gal}(K(\mathfrak{d}_n)/K)]$$

send the modular elements $\Theta_{\mathfrak{d}_n,f}$ into each other, so that one can take their limit $\tilde{\Theta}$. Any abelian extension of $K$ totally ramified above $v_0$ and unramified elsewhere is contained in $\cup K(\mathfrak{d}_n)$: in particular this holds for our $L$. Let $\Theta$ be the image of $\tilde{\Theta}$ under the projection

$$\varprojlim \mathbb{Z}_p[\mathrm{Gal}(K(\mathfrak{d}_n)/K)] \longrightarrow \Lambda\,.$$

Equation (15) shows that $\Theta$ satisfies the interpolation property required for the $p$-adic $L$-function. Observe that $\Theta_{\mathfrak{d}_n,f}$ is invariant under the action of $\mathrm{Gal}(K/k)$, since the modular elements are already defined above $k$. Thus, as elements of $\mathbb{Z}_p[[\mathrm{Gal}(L/k)]]$,

$$\Theta = \tau \cdot \Theta \cdot \tau^{-1} = \Theta^{\#}.$$

On the other hand, by [Tan93, Proposition 3] we have

$$\Theta_{\mathfrak{d}_n,f} = -\Theta^{\#}_{\mathfrak{d}_n,f} \cdot \eta,$$

where $\eta \in \mathrm{Gal}(K(\mathfrak{d}_n)/K)$ corresponds to the divisor $\mathfrak{n}' = \mathfrak{n} - v_0$. This implies that $\Theta = 0$.

## References


[GT07] Cristian D. González-Avilés and Ki-Seng Tan, *A generalization of the Cassels-Tate dual exact sequence*, Math. Res. Lett. **14** (2007), no. 2, 295–302, DOI 10.4310/MRL.2007.v14.n2.a11. MR2318626 (2008k:11067)

[Lan91] William E. Lang, *Extremal rational elliptic surfaces in characteristic p. I. Beauville surfaces*, Math. Z. **207** (1991), no. 3, 429–437, DOI 10.1007/BF02571400. MR1115175 (92f:14032)

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266. MR0444670 (56 #3020)

[Mil75] J. S. Milne, *On a conjecture of Artin and Tate*, Ann. of Math. (2) **102** (1975), no. 3, 517–533. MR0414558 (54 #2659)

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. MR559531 (81j:14002)

[Mil86a] J. S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press Inc., Boston, MA, 1986. MR881804 (88e:14028)

[Shi92] Tetsuji Shioda, *Some remarks on elliptic curves over function fields*, Astérisque **209** (1992), 12, 99–114. Journées Arithmétiques, 1991 (Geneva). MR1211006 (94d:11046)

[SU13] Christopher Skinner and Eric Urban, *The Iwasawa Main Conjectures for $GL_2$*, Invent. Math. **195** (2014), no. 1, 1–277, DOI 10.1007/s00222-013-0448-1. MR3148103

[Tan93] Ki-Seng Tan, *Modular elements over function fields*, J. Number Theory **45** (1993), no. 3, 295–311, DOI 10.1006/jnth.1993.1079. MR1247386 (95d:11158)

[Tan12] Ki-Seng Tan, *Selmer groups over $\mathbb{Z}_p^d$-extensions*, Math. Ann. **359** (2014), no. 3-4, 1025–1075, DOI 10.1007/s00208-014-1023-9. MR3231024

[Ta66] John Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 306, 415–440. MR1610977



School of Mathematical Sciences, Capital Normal University, Beijing 100048, People's Republic of China

*E-mail address*: kinglaihonkon@gmail.com

Department of Mathematics, National Taiwan University. Taipei 10764, Taiwan

*Current address*: Department of Mathematical Sciences, Xi'an Jiaotong-Liverpool University, No. 111 Ren'ai Road, Dushu Lake Higher Education Town, Suzhou Industrial Park, Suzhou 215123 Jiangsu, People's Republic of China.

*E-mail address*: longhi@math.ntu.edu.tw

Department of Mathematics, National Taiwan University, Taipei 10764, Taiwan

*E-mail address*: tan@math.ntu.edu.tw

College of Engineering, Mathematics and Physical Sciences, University of Exeter, North Park Road, Exeter, United Kingdom

*Current address*: Department of Information and Communication Sciences, Faculty of Science and Technology, Sophia University, 4 Yonbancho, Chiyoda-ku, Tokyo 102-0081 Japan

*E-mail address*: f-trihan-52m@sophia.ac.jp