Bull. Aust. Math. Soc. **100** (2019), 245–255
doi:10.1017/S0004972719000108

ON THE SELMER GROUP OF A CERTAIN p-ADIC LIE EXTENSION

AMALA BHAVE✉ and LACHIT BORA

(Received 6 November 2018; accepted 29 December 2018; first published online 27 February 2019)

Abstract

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Let $p \geq 5$ be a prime in $\mathbb{Q}$ and suppose that E has good ordinary reduction at p. We study the dual Selmer group of E over the compositum of the GL_2 extension and the anticyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic extension as an Iwasawa module.

2010 *Mathematics subject classification*: primary 11R23; secondary 11R20, 11R34.

Keywords and phrases: elliptic curve, anticyclotomic extension, Galois group, Iwasawa module, Selmer group.

1. Introduction

Let F be an imaginary quadratic extension of $\mathbb{Q}$ and let $p \geq 5$ be a prime number. Let E be an elliptic curve over $\mathbb{Q}$ such that E has good ordinary reduction at all primes of F dividing p. Let E_{p^∞} denote the subgroup of $E(\overline{F})$ consisting of all p-power torsion points of E. We attach the coordinates of the points E_{p^∞} to F and denote the resulting extension of F by F_∞, that is, $F_\infty = F(E_{p^\infty})$. Let F^{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of F and let $\Gamma := \mathrm{Gal}(F^{\mathrm{cyc}}/F)$. Then $F^{\mathrm{cyc}} \subsetneq F_\infty$ because of the Weil pairing [10, Corollary 8.1.1]. When E does not admit complex multiplication, which we assume throughout this paper, $\mathrm{Gal}(F_\infty/F)$ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ due to a result of Serre [9]. The compositum of all $\mathbb{Z}_p$-extensions of F is the unique Galois extension K_∞ whose Galois group is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ [11, Theorem 13.4]. Let F^{anti} be the anticyclotomic $\mathbb{Z}_p$-extension of F which is the fixed field of the subgroup of $\mathrm{Gal}(K_\infty/F)$ on which the conjugation of F acts by inverse. Let L_∞ be the compositum of F_∞ and F^{anti}. Let S be a finite set of primes of F containing primes dividing p and the primes at which E has split multiplicative reduction. Let F^S be the maximal extension of F which is unramified outside S. We note that $L_\infty \subseteq F^S$ since F^{anti} is unramified outside p and the only primes ramified in F_∞ are those that divide p and

The first author acknowledges the support of DST PURSE and UPE II grants; the second author is supported by a UGC-BSR fellowship.

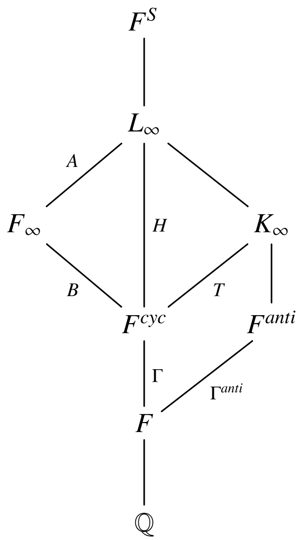

FIGURE 1. The tower of field extensions.

those at which E has bad reduction. Thus we have the tower of field extensions shown in Figure 1.

For the above tower, we denote the various Galois groups by

$$G := \mathrm{Gal}(L_\infty/F), \quad H := \mathrm{Gal}(L_\infty/F^{\mathrm{cyc}}), \quad G_\infty := \mathrm{Gal}(F_\infty/F), \quad A := \mathrm{Gal}(L_\infty/F_\infty),$$
$$B := \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}}), \quad T := \mathrm{Gal}(K_\infty/F^{\mathrm{cyc}}), \quad \Gamma := \mathrm{Gal}(F^{\mathrm{cyc}}/F), \quad \Gamma^{\mathrm{anti}} := \mathrm{Gal}(F^{\mathrm{anti}}/F).$$

Recall that G_∞ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. It is clear from the action of $\mathrm{Gal}(F/\mathbb{Q})$ on $\mathrm{Gal}(K_\infty/\mathbb{Q}) \simeq Z_p \times \mathbb{Z}_p$ that F^{cyc} and F^{anti} are mutually disjoint over F. Hence Γ and Γ^{anti} are both isomorphic to $\mathbb{Z}_p$. Next, B is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$. Hence, from basic Galois theory, T is isomorphic to $\mathbb{Z}_p$, H is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p) \times \mathbb{Z}_p$ and A is isomorphic to $\mathbb{Z}_p$. Thus L_∞/F is a compact p-adic Lie extension.

For any compact p-adic Lie group Σ, the Iwasawa algebra of Σ, denoted by $\Lambda(\Sigma)$, is defined by

$$\Lambda(\Sigma) := \varprojlim \mathbb{Z}_p[\Sigma/U],$$

where U runs over the family of open normal subgroups of Σ and the inverse limit is taken with respect to the canonical projection maps. This algebra is left and right Noetherian [7, Theorem 1]. For any algebraic extension N of F contained in F^S, the p^∞-Selmer group $\mathrm{Sel}_p(E/N)$ is defined by

$$\mathrm{Sel}_p(E/N) := \ker\Big(H^1(\mathrm{Gal}(F^S/N), E[p^\infty]) \longrightarrow \bigoplus_{v\in S} J_v(N)\Big),$$

where

$$J_v(N) = \varinjlim \bigoplus_{\omega|v} H^1(L_\omega, E)(p).$$

https://doi.org/10.1017/S0004972719000108 Published online by Cambridge University Press

Here L runs over all finite extensions of F contained in N and the limit is taken with respect to the restriction maps.

The action of the Galois group on cohomology groups induces an action on the Selmer group. In this paper, we consider $\mathrm{Sel}_p(E/L_\infty)$ as a left $\Lambda(G)$-module. It is a discrete $\Lambda(G)$-module. We also consider its compact Pontryagin dual $\mathrm{Sel}_p(E/L_\infty)^\vee$, which is defined by

$$\mathrm{Sel}_p(E/L_\infty)^\vee := \mathrm{Hom}(\mathrm{Sel}_p(E/L_\infty), \mathbb{Q}_p/\mathbb{Z}_p).$$

Note that the action of G on $\mathrm{Sel}_p(E/L_\infty)^\vee$ is given by $(g\phi)(x) = \phi(g^{-1}x)$ for $g \in \mathrm{G}$, $\phi \in \mathrm{Sel}_p(E/L_\infty)^\vee$ and $x \in \mathrm{Sel}_p(E/L_\infty)$.

We study the structure of the Selmer group as a module over the Iwasawa algebra of the appropriate Galois groups. The main result in this paper is the following theorem.

THEOREM 1.1. $\mathrm{Sel}_p(E/L_\infty)^\vee$ *is a* $\Lambda(G)$*-torsion module.* □

We also compute the Euler characteristic of $\mathrm{Sel}_p(E/L_\infty)^\vee$.

THEOREM 1.2. *Let p be a rational prime such that $p \geq 5$. Further, assume that:*

(1) *E has good ordinary reduction at all places v of F dividing p; and*
(2) *$\mathrm{Sel}_p(E/F)$ is finite.*

Then we have the Euler characteristic formula

$$\chi(G, \mathrm{Sel}_p(E/L_\infty)) = \rho_p(E/F) \times \Big| \prod_v L_v(E,1) \Big|_p,$$

where

$$\rho_p(E/F) = \frac{\sharp Ш(E/F)(p) \prod_{v|p}((\sharp \widetilde{E}_v(\kappa_{F_v})(p))^2)}{(\sharp E(F)(p))^2 \prod_{v \in S} |c_v|_p}. \qquad \square$$

The definition of Euler characteristic and the terms involved in the formula are introduced at the beginning of Section 3.

2. Selmer group

In this section, we prove Theorem 1.1. To prove this theorem, we analyse the following fundamental diagram.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_p(E/L_\infty)^H \arrow[r] & \mathrm{H}^1(F^S/L_\infty, E_{p^\infty})^H \arrow[r] & \Big(\bigoplus_{v|S} J_v(L_\infty)\Big)^H & \\
0 \arrow[r] & \mathrm{Sel}_p(E/F^{\mathrm{cyc}}) \arrow[r] \arrow[u, "\alpha"] & \mathrm{H}^1(F^S/F^{\mathrm{cyc}}, E_{p^\infty}) \arrow[r, "\lambda_{F^{\mathrm{cyc}}}"] \arrow[u, "\beta"] & \bigoplus_{v|S} J_v(F^{\mathrm{cyc}}) \arrow[r] \arrow[u, "\delta = \oplus \delta_v"] & 0.
\end{tikzcd}$$

(2.1)

https://doi.org/10.1017/S0004972719000108 Published online by Cambridge University Press

The vertical maps β and δ are restriction maps and α is induced by β. Note that Mazur's conjecture states that $\mathrm{Sel}_p(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-cotorsion [8]. A theorem of Kato–Rohrlich [5, Theorem 1.5] says that $\mathrm{Sel}_p(E/F^{\mathrm{cyc}})$ is $\Lambda(\Gamma)$-cotorsion when F/Q is Abelian. Since F is imaginary quadratic, Mazur's conjecture holds in our situation and the surjectivity of the map $\lambda_{F^{\mathrm{cyc}}}$ follows from [3, Proposition 6.2]. Now we apply the snake lemma to the fundamental diagram to get the exact sequence.

$$0 \longrightarrow \ker(\alpha) \longrightarrow \ker(\beta) \longrightarrow \ker(\delta) \longrightarrow \mathrm{coker}(\alpha) \longrightarrow \mathrm{coker}(\beta) \longrightarrow \mathrm{coker}(\delta). \tag{2.2}$$

Using the five term exact cohomology sequence, we observe that

$$\ker(\beta) = H^1(L_\infty/F^{\mathrm{cyc}}, E_{p^\infty}) \quad \text{and} \quad \mathrm{coker}(\beta) \subseteq H^2(L_\infty/F^{\mathrm{cyc}}, E_{p^\infty}).$$

Lemma 2.1. *The groups* $\mathrm{H}^i(H, E_{p^\infty})$ *are finite for* $i \geq 0$. *In particular, the groups* $\ker(\beta)$ *and* $\mathrm{coker}(\beta)$ *are finite.*

Proof. Note that $E_{p^\infty}(F_\infty) = E_{p^\infty}(L_\infty) = E_{p^\infty}$ because all the p-primary torsion points of E are defined over F_∞. Clearly, A is isomorphic to a subgroup of $T \simeq \mathbb{Z}_p$. Hence the p-cohomological dimension of A is one ($A \simeq \mathbb{Z}_p$) and

$$\mathrm{H}^j(A, E_{p^\infty}) = 0 \quad \text{for } j \geq 2. \tag{2.3}$$

Further, the group A acts trivially on E_{p^∞}, so $\mathrm{H}^0(A, E_{p^\infty}) = E_{p^\infty}$ and $\mathrm{H}^1(A, E_{p^\infty}) = \mathrm{Hom}(A, E_{p^\infty})$. Since A is Abelian, the Galois group B acts on A by conjugation and we have a homomorphism $\tau : B \longrightarrow \mathbb{Z}_p^\times = \mathrm{Aut}(A)$. But B is an open subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ and their Lie algebras coincide. As the Lie algebra of $\mathrm{SL}_2(\mathbb{Z}_p)$ is simple, this implies that there exists a subgroup B' of B such that (i) B' is open in B and (ii) B' acts trivially on A. Now consider $W = F_\infty \cap K_\infty$, which is a finite extension of F^{cyc} [2, Lemma 1]. The group $B' = \mathrm{Gal}(F_\infty/W)$ satisfies both (i) and (ii). We claim that

$$\mathrm{Hom}(A, E_{p^\infty}) \simeq E_{p^\infty}, \tag{2.4}$$

considered as B'-modules. Indeed, for a fixed topological generator γ of A, since any homomorphism $f \in \mathrm{Hom}(A, E_{p^\infty})$ is determined by its image on γ, it follows that $f \mapsto f(\gamma)$ gives a B'-isomorphism. Here recall that the natural action of B' on $\mathrm{Hom}(A, E_p^\infty)$ is given by $(\beta \cdot f)(\gamma) = \beta \cdot f(\tau(\beta^{-1})(\gamma))$ for every $\beta \in B'$.

This, therefore, implies that $\mathrm{H}^i(B', \mathrm{H}^1(A, E_{p^\infty})) \simeq \mathrm{H}^i(B', E_{p^\infty})$ and by [4] the groups $\mathrm{H}^i(B, E_{p^\infty})$ and $\mathrm{H}^i(B', E_{p^\infty})$ are finite for $i = 1, 2$. Also $\mathrm{H}^0(B, \mathrm{H}^1(A, E_{p^\infty})) = E_{p^\infty}(F^{\mathrm{cyc}})$ which is finite by Imai's theorem [6]. Thus the Hochschild–Serre spectral sequence along with (2.3) and (2.4) implies that the $\mathrm{H}^i(H, E_{p^\infty})$ are finite for $i \geq 0$. This completes the proof of the lemma. □

We now study the maps $\delta = \bigoplus \delta_v$. Figure 2 is obtained by completing the fields at a compatible set of primes, that is, $u \mid w$, $u \mid w'$, $w \mid v$ and $w' \mid v$. The Galois groups are the corresponding decomposition subgroups of the Galois groups occurring in Figure 1. Let $H_u := \mathrm{Gal}(L_{\infty,u}/F_v^{\mathrm{cyc}})$, $\Gamma_v := \mathrm{Gal}(F_v^{\mathrm{cyc}}/F_v)$, $W_v := F_{\infty,w} \cap K_{\infty,w'}$ and $G_u := \mathrm{Gal}(L_{\infty,u}/F_v)$. When $v \nmid p$, the extension $K_{\infty,w'}$ is unramified over F_v. But the

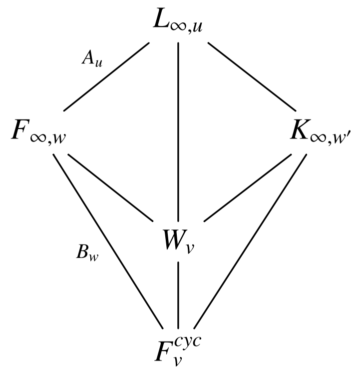

Figure 2. The tower of local field extensions.

maximal unramified extension of F_v is contained in F_v^{cyc}. Hence $K_{\infty,w'} = F_v^{\mathrm{cyc}}$, which implies that the Galois group A_u is trivial by basic Galois theory. Further, if E has good reduction at v, then $w \mid v$ is unramified in F_∞. Hence, by the same argument, B_w and H_u are trivial. However, if v is a prime of bad reduction, then B_w has dimension one ([3, Lemma 5.1]). Thus $G_u = \mathrm{Gal}(L_{\infty,u}/F_v) = \mathrm{Gal}(F_{\infty,w}/F_v)$ has dimension two and H_u has dimension one by [3, Lemma 5.1]. When $v \mid p$, by [3, Lemma 5.1], G_u has dimension at most four and H_u has dimension at most three.

Lemma 2.2. *The $\mathbb{Z}_p$-corank of* $\ker(\delta)$ *is equal to the number of primes in F^{cyc} at which E has split multiplicative reduction.*

Proof. We consider two cases.

Case 1. Let $v \nmid p$. In this case, it follows from Kummer theory that

$$H^1(F_v^{\mathrm{cyc}}, E)(p) \simeq H^1(F_v^{\mathrm{cyc}}, E_{p^\infty}) \quad \text{and} \quad H^1(F_{\infty,\omega}, E)(p) \simeq H^1(F_{\infty,\omega}, E_{p^\infty}).$$

Therefore, by the Hochschild–Serre spectral sequence,

$$\ker(\delta_v) = H^1(H_u, E_{p^\infty}) \quad \text{and} \quad \mathrm{coker}(\delta_v) \subseteq H^2(H_u, E_{p^\infty}).$$

If E has good reduction at v, then all of w, w' and u are unramified primes. But the maximal unramified extension of F_v is contained in F_v^{cyc}. This implies that $F_{\infty,w} = L_{\infty,u} = K_{\infty,w'} = F_v^{\mathrm{cyc}}$. So it follows that the $H^i(H_u, E_{p^\infty})$ are zero for $i \geq 1$. This means that $\ker(\delta_v) = \mathrm{coker}(\delta_v) = 0$.

Suppose E has bad reduction at v. Then $K_{\infty,w'}$ is unramified and again $K_{\infty,w'} = F_v^{\mathrm{cyc}}$, as explained above, that is, $B_w = H_u$. Now using the argument from [3, Lemma 5.4], $J_v(L_\infty) = 0$, which implies that $\mathrm{coker}(\delta_v) = 0$. Note that $\ker(\delta_v) = H^1(H_u, E_{p^\infty}) = H^1(B_w, E_{p^\infty})$, which has $\mathbb{Z}_p$-corank one when E has split multiplicative reduction at v by [3, Lemma 5.13].

Case 2. Let $v \mid p$. As in [3, Lemma 2.8], $\ker(\delta_v) = \mathrm{H}^1(\mathrm{H}_u, E(L_{\infty,u}))(p)$ and $\mathrm{coker}(\delta_v) = \mathrm{H}^2(\mathrm{H}_u, E(L_{\infty,u}))(p)$. For their computation, we need some further notation and repeated use of the Hochschild–Serre spectral sequence.

https://doi.org/10.1017/S0004972719000108 Published online by Cambridge University Press

Consider the extensions $W_v = F_{\infty,w} \cap K_{\infty,w'}$, $M_v = F_v(\mu_{p^\infty})$, $N_v = M_v \cdot W_v$ and $K' = M_v \cdot K_{\infty,w'}$ of F_v^{cyc} contained in $L_{\infty,u}$. Denote the corresponding Galois groups $R := \mathrm{Gal}(L_{\infty,u}/N_v)$, $Q := \mathrm{Gal}(K'/N_v)$ and $P := \mathrm{Gal}(L_{\infty,u}/K')$. Clearly, M_v is a finite extension of F_v^{cyc} and K' is a finite extension of $K_{\infty,w'}$. Moreover, W_v is a finite Galois extension of F_v^{cyc} [2, Lemma 6]. Therefore N_v is a finite Galois extension of F_v^{cyc}. Hence it is enough to prove that $\mathrm{H}^i(R, E(L_{\infty,u}))(p)$ is finite for $i \geq 1$. Now $L_{\infty,u}$ and N_v are deeply ramified extensions of F_v [3, Section 5.2]. Also E has good reduction at v so the reduced curve $\widetilde{E}_v$ is nonsingular. Hence, from [3, Proposition 5.15],

$$H^1(N_v, E)(p) \simeq H^1(N_v, \widetilde{E}_{v,p^\infty}) \quad \text{and} \quad H^1(L_{\infty,u}, E)(p) \simeq H^1(L_{\infty,u}, \widetilde{E}_{v,p^\infty}).$$

Since the p-cohomological dimension of Q is one, applying the Hochschild–Serre spectral sequence to the extensions $N_v \subset K' \subset L_{\infty,u}$, gives, for all $i \geq 1$,

$$0 \longrightarrow \mathrm{H}^1(Q, \mathrm{H}^{i-1}(P, \widetilde{E}_{v,p^\infty})) \longrightarrow \mathrm{H}^i(R, \widetilde{E}_{v,p^\infty}) \longrightarrow \mathrm{H}^0(Q, \mathrm{H}^i(P, \widetilde{E}_{v,p^\infty})) \longrightarrow 0.$$

We claim that $\mathrm{H}^i(R, \widetilde{E}_{v,p^\infty})$ is finite for all $i \geq 1$. It is sufficient to show that $\mathrm{H}^i(P, \widetilde{E}_{v,p^\infty})$ is finite for all $i \geq 1$. Let $\mathrm{Gal}(F_{\infty,w}/N_v) = B'_w$. Now $P \simeq B'_w$ and their actions on $\widetilde{E}_{v,p^\infty}$ are the same as $F_{\infty,w} \cap K' = N_v$. Hence it is enough to show that $\mathrm{H}^i(B'_w, \widetilde{E}_{v,p^\infty})$ is finite for all $i \geq 1$, which is indeed true from [3, Lemma 5.25]. Hence we conclude that $\ker(\delta_v)$ and $\mathrm{coker}(\delta_v)$ are finite when $v \mid p$.

Compiling all the cases for δ_v, we conclude that $\ker(\delta)$ has $\mathbb{Z}_p$-corank equal to the number of primes v in F^{cyc} at which E has split multiplicative reduction. □

Proof of Theorem 1.1. From Equation (2.2) and the two preceding lemmas, we see that $\mathrm{coker}(\alpha)$ and $\ker(\delta)$ have the same $\mathbb{Z}_p$-corank. Consider the left vertical exact sequence in the fundamental diagram (2.1), namely,

$$0 \longrightarrow \ker(\alpha) \longrightarrow \mathrm{Sel}_p(E/F^{\mathrm{cyc}}) \longrightarrow \mathrm{Sel}_p(E/L_\infty)^H \longrightarrow \mathrm{coker}(\alpha) \longrightarrow 0.$$

By definition, the $\mathbb{Z}_p$-corank of $\mathrm{Sel}(E/F^{\mathrm{cyc}}) = \lambda$, which is the Iwasawa λ-invariant of E over F^{cyc}. Hence the Pontryagin dual of $\mathrm{Sel}_p(E/L_\infty)^H$ is a finitely generated $\mathbb{Z}_p$-module of rank $\lambda + r$, where r is the number of primes of F^{cyc} at which E has split multiplicative reduction. By the Nakayama lemma [1], the dual of $\mathrm{Sel}_p(E/L_\infty)$ is a finitely generated $\Lambda(H)$-module of rank $\lambda + r$. Hence $\mathrm{Sel}_p(E/L_\infty)$ is a $\Lambda(G)$-cotorsion module. □

3. Euler characteristic

For a p-adic Lie group Σ and a discrete Σ-module M, the *Euler characteristic* $\chi(\Sigma, M)$ is defined as

$$\chi(\Sigma, M) := \prod_{i \geq 0} \sharp \mathrm{H}^i(\Sigma, M)^{(-1)^i},$$

whenever it is defined [3]. In our case, the Euler characteristic is defined under the hypotheses of Theorem 1.2. Now we introduce the terms which appear in the formula of the G-Euler characteristic of $\mathrm{Sel}_p(E/L_\infty)$:

- $Ш(E/F)$ is the Tate–Shafarevich group of E over F;
- $c_v = |E(F_v) : E_0(F_v)|$ denotes the local Tamagawa factor at a prime v, where $E_0(F_v)$ is the subgroup of $E(F_v)$ consisting of the points with nonsingular reduction at v;
- $L_v(E, 1)$ denotes the Euler factor of E at v;
- κ_{F_v} is the residue field of F at v;
- when E has good reduction at v, $\widetilde{E}_v$ is reduction of E over F_v; and
- S_1 is the set of primes of F at which E has bad reduction.

We need the following lemmas.

Lemma 3.1. *We have* $\chi(G, E_{p^\infty}) = 1$.

Proof. Since $\mathrm{cd}_p(\Gamma) = 1$, the Hochschild–Serre spectral sequence takes the form

$$0 \longrightarrow H^1(\Gamma, H^{i-1}(H, E_{p^\infty})) \longrightarrow H^i(G, E_{p^\infty}) \twoheadrightarrow H^0(\Gamma, H^i(H, E_{p^\infty})), \tag{3.1}$$

for all $i \geq 1$. The $H^i(H, E_{p^\infty})$ are finite for all $i \geq 0$ by Lemma 2.1. When M is a finite Γ-module, the cardinality of $H^1(\Gamma, M)$ and $H^0(\Gamma, M)$ are equal. Let

$$h_i = \sharp\mathrm{H}^1(\Gamma, H^{i-1}(H, E_{p^\infty})) = \sharp\mathrm{H}^0(\Gamma, H^{i-1}(H, E_{p^\infty})).$$

Then, by (3.1),

$$\sharp\mathrm{H}^1(G, E_{p^\infty}) = h_{i-1}h_i.$$

Now $H^6(G, E_{p^\infty}) = 0$, which implies that $h_5 = 1$. Hence

$$\chi(G, E_{p^\infty}) = h_0(h_o h_1)^{-1} \cdots (h_4 h_5)^{-1} = 1.$$

□

We state the following lemma which follows exactly as for Lemma 3.1 above.

Lemma 3.2. *When* $v \mid p$, *we have* $\chi(G_u, \widetilde{E_{v,p^\infty}}) = 1$, *where* $G_u \simeq \mathrm{Gal}(L_{\infty,u}/F_v)$.

We will analyse the following fundamental diagram.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_p(E/L_\infty)^G \arrow[r] & \mathrm{H}^1(F^S/L_\infty, E_{p^\infty})^G \arrow[r, "\psi_{L_\infty}"] & \left(\bigoplus_{v|S} J_v(L_\infty)\right)^G \\
0 \arrow[r] & \mathrm{Sel}_p(E/F) \arrow[r] \arrow[u, "\alpha 1"] & \mathrm{H}^1(F^S/F, E_{p^\infty}) \arrow[r, "\lambda_F"] \arrow[u, "\beta 1"] & \bigoplus_{v|S} J_v(F). \arrow[u, "\delta 1 = \bigoplus \delta 1_v"]
\end{tikzcd} \tag{3.2}$$

Lemma 3.3. *In diagram (3.2),* $\ker(\beta 1)$ *and* $\mathrm{coker}(\beta 1)$ *are finite.*

Proof. Using the Hochschild–Serre spectral sequence, we have $\ker(\beta 1) = \mathrm{H}^1(G, E_{p^\infty})$ and $\mathrm{coker}(\beta 1) \subseteq \mathrm{H}^2(G, E_{p^\infty})$. Now $G/H \simeq \mathbb{Z}_p$, that is, $\mathrm{cd}_p(G/H) = 1$. The Hochschild–Serre spectral sequence gives the exact sequence

$$0 \longrightarrow \mathrm{H}^1(G/H, \mathrm{H}^{n-1}(H, E_{p^\infty})) \longrightarrow \mathrm{H}^n(G, E_{p^\infty}) \longrightarrow \mathrm{H}^n(H, E_{p^\infty})^{G/H} \longrightarrow 0\,.$$

Hence, from Lemma 2.1, $\ker(\beta 1)$ and $\mathrm{coker}(\beta 1)$ are finite. □

https://doi.org/10.1017/S0004972719000108 Published online by Cambridge University Press

Lemma 3.4. *In the fundamental diagram (3.2),* $\ker(\delta 1)$ *and* $\operatorname{coker}(\delta 1)$ *are finite.*

Proof. Considering the vertical map $\delta 1$, we note that $\ker(\delta 1_v) \simeq \mathrm{H}^1(G_u, E(L_{\infty,u}))(p)$ and $\operatorname{coker}(\delta 1_v) \simeq \mathrm{H}^2(G_u, E(L_{\infty,u}))(p)$. First we consider the case $v \mid p$. We let $\hat{E}$ be the formal group of E defined over F_v. Let $\mathcal{M}$ and $\mathcal{M}(L_{\infty,u})$ be the maximal ideals of the rings of integers of F_v and $L_{\infty,u}$, respectively. Then we have the exact sequence

$$0 \longrightarrow \hat{E}(\mathcal{M}(L_{\infty,u})) \longrightarrow E(L_{\infty,u}) \longrightarrow \tilde{E}_{v,p^\infty} \longrightarrow 0. \tag{3.3}$$

By following [3, Lemma 5.18],

$$\mathrm{H}^i(G_u, \hat{E}(\mathcal{M}(L_{\infty,u}))) \simeq \mathrm{H}^i(F_v, \hat{E}(\mathcal{M})) \quad \text{for all } i \geq 1, \tag{3.4}$$

$$\mathrm{H}^i(F_v, \hat{E}(\mathcal{M})) = 0 \quad \text{for all } i \geq 2. \tag{3.5}$$

Applying G_u-cohomology to the exact sequence (3.3), and using equations (3.4) and (3.5), we conclude that

$$\sharp \operatorname{coker}(\delta 1_v) = \sharp \mathrm{H}^2(G_u, \widetilde{E}_{v,p^\infty}).$$

Moreover, from [3, Lemmas 5.18 and 5.19],

$$\sharp \ker(\delta 1_v) = \sharp \widetilde{E}_v(\kappa_{F_v})(p) \times \sharp \mathrm{H}^1(G_u, \widetilde{E}_{v,p^\infty}).$$

Now $L_{\infty,u}$ contains $F_v(\mu_{p^\infty})$. So, from [3, Lemma 5.4], when E has bad reduction at v, it follows that $J_v(L_\infty) = 0$, that is, $\operatorname{coker}(\delta 1_v) = 0$. In this case, from [3, Lemma 5.6], $\ker(\delta 1_v) = |L_v(E, 1)/c_v|_p$. Here $|\cdot|_p$ denotes the p-adic absolute value. Suppose $v \nmid p$ and E has good reduction at v. Then v is unramified in $L_{\infty,u}$. Hence $G_u = \Gamma_v$ has p-cohomological dimension one. This implies that $\operatorname{coker}(\delta 1_v) = 0$. In addition, $\ker(\delta 1_v) = 0$ from [3, Lemma 5.10]. □

In the following, we assume that $\mathrm{Sel}_p(E/F)$ is finite. Note the following lemma from [3].

Lemma 3.5 [3, Lemma 2.7]. *If p is an odd prime and* $\mathrm{Sel}_p(E/F)$ *is finite, then* $\operatorname{coker}(\lambda_F) \simeq E\widehat{(F)}(p)$.

Lemma 3.6. *If* $\mathrm{Sel}_p(E/F)$ *is finite and if E has good ordinary reduction at all primes v of F that divides p and $p \geq 5$, then* $H^0(G, \mathrm{Sel}_p(E/L_\infty))$ *and* $\operatorname{coker}(\psi_{L^\infty})$ *are finite.*

Proof. We consider the following diagram

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{im}(\psi_{L_\infty}) \arrow[r] & \left(\bigoplus_{v|S} J_v(L_\infty)\right)^G \arrow[r] & \operatorname{coker}(\psi_{L_\infty}) \arrow[r] & 0 \\
0 \arrow[r] & \operatorname{im}(\lambda_F) \arrow[r] \arrow[u, "\delta 2"] & \bigoplus_{v\in S} \mathrm{H}^1(F_v, E)(p) \arrow[r] \arrow[u, "\delta 1"] & \operatorname{coker}(\lambda_F) \arrow[r] \arrow[u, "\eta"] & 0.
\end{tikzcd} \tag{3.6}$$

https://doi.org/10.1017/S0004972719000108 Published online by Cambridge University Press

Here $\ker(\delta 2) = \ker(\delta 1) \cap \operatorname{im}(\lambda_F)$ and $\operatorname{coker}(\delta 2) = \operatorname{im}(\psi_{L_\infty})/\delta 1(\operatorname{im}(\lambda_F))$. By applying the snake lemma to the fundamental diagram (3.2), we get the exact sequence

$$0 \longrightarrow \ker(\alpha 1) \longrightarrow \ker(\beta 1) \longrightarrow \ker(\delta 1) \cap \operatorname{im}(\lambda_F) \tag{3.7}$$

$$\longrightarrow \operatorname{coker}(\alpha 1) \longrightarrow \operatorname{coker}(\beta 1) \longrightarrow \operatorname{im}(\psi_{L_\infty})/\delta 1(\operatorname{im}(\lambda_F)) \longrightarrow 0.$$

Now, using Lemmas 3.3 and 3.4, the terms $\ker(\alpha 1)$ and $\operatorname{coker}(\alpha 1)$ in the exact sequence (3.7) are finite. Hence we consider the vertical map $\alpha 1$. By assumption, $\mathrm{Sel}_p(E/F)$ is finite, so $H^0(G, \mathrm{Sel}_p(E/L_\infty))$ is finite. Applying the snake lemma to the diagram (3.6) and using Lemma 3.4, it follows that $\operatorname{coker}(\eta)$ is finite. Also, from Lemma 3.5, $\operatorname{coker}(\lambda_F) = \widehat{E(F)}(p)$. The latter is finite, which, in turn, implies that $\ker(\eta)$ is finite. So considering the vertical map η, we conclude that $\operatorname{coker}(\psi_{L_\infty})$ is finite. □

Lemma 3.7. *The map λ_{L_∞} in the following exact sequence is surjective.*

$$0 \longrightarrow \mathrm{Sel}_p(E/L_\infty) \longrightarrow \mathrm{H}^1(F^S/L_\infty, E_{p^\infty}) \xrightarrow{\lambda_{L_\infty}} \Big(\bigoplus_{v|S} J_v(L_\infty)\Big). \tag{3.8}$$

Proof. The proof of this lemma is the same as that of [2, Lemma 12]. □

Applying G-cohomology to the exact sequence (3.8) gives the long exact sequence

$$0 \longrightarrow \mathrm{Sel}_p(E/L_\infty)^G \longrightarrow \mathrm{H}^1(F^S/L_\infty, E_{p^\infty})^G \xrightarrow{\psi_{L_\infty}} \Big(\bigoplus_{v|S} J_v(L_\infty)\Big)^G.$$

$$\longrightarrow \mathrm{H}^1(G, \mathrm{Sel}_p(E/L_\infty)) \longrightarrow \mathrm{H}^1(G, \mathrm{H}^1(F^S/L_\infty, E_{p^\infty}))$$

From this exact sequence,

$$0 \longrightarrow \operatorname{coker}(\psi_{L_\infty}) \longrightarrow \mathrm{H}^1(G, \mathrm{Sel}_p(E/L_\infty)) \longrightarrow \mathrm{H}^1(G, \mathrm{H}^1(F^S/L_\infty, E_{p^\infty})). \tag{3.9}$$

Lemma 3.8. *For $i \geq 1$,*

$$\mathrm{H}^i(G, \mathrm{H}^1(F^S/L_\infty, E_{p^\infty})) \simeq \mathrm{H}^{i+2}(G, E_{p^\infty}).$$

Proof. From [3, Theorem 2.10], $\mathrm{H}^2(F^S/F_\infty, E_{p^\infty}) = 0$ and $\mathrm{H}^2(F^S/L_\infty, E_{p^\infty}) = 0$. Thus, using the Hochschild–Serre sequence in group cohomology and following [3, Lemmas 4.3 and 4.4], we conclude that, for $i \geq 1$,

$$\mathrm{H}^i(G, \mathrm{H}^1(F^S/L_\infty, E_{p^\infty})) \simeq \mathrm{H}^{i+2}(G, E_{p^\infty}).$$ □

Lemma 3.9. *For $i \geq 1$,*

$$\mathrm{H}^i(G, J_v(L_\infty)) \simeq \mathrm{H}^{i+2}(G_u, \widetilde{E}_{v,p^\infty}) \quad \text{for } v \mid p, \qquad \mathrm{H}^i(G, J_v(L_\infty)) \simeq 0 \quad \text{for } v \nmid p.$$

https://doi.org/10.1017/S0004972719000108 Published online by Cambridge University Press

Proof. For $v \nmid p$, the argument is the same as in [3, Lemmas 5.4 and 5.5]. Similarly, for the proof in the other case, we argue as in Case 2 of Lemma 2.2 and [3, Lemma 5.16] to get the required result. □

Now, from Lemmas 3.8 and 3.9, we see that all the terms of the exact sequence (3.9) are finite. Also G has p-cohomological dimension less than or equal to five. Hence, from the exact sequence (3.9),

$$\sharp\,\mathrm{coker}(\psi_{L_\infty}) = \frac{\prod_{3\le i\le 5} \sharp \mathrm{H}^i(G, E_{p^\infty})^{(-1)^i}}{\prod_{1\le i\le 5} \sharp \mathrm{H}^i(G, \mathrm{Sel}_p(E/L_\infty))^{(-1)^i} \prod_{v|p}\big(\prod_{3\le i\le 5} \sharp \mathrm{H}^i(G_u, \widetilde{E}_{v,p^\infty})^{(-1)^i}\big)}. \tag{3.10}$$

Proof of Theorem 1.2. Applying the snake lemma to diagram (3.6),

$$\frac{\sharp\,\ker(\delta 2)}{\sharp\,\mathrm{coker}(\delta 2)} = \frac{\sharp\,\ker(\delta 1)}{\sharp\,\mathrm{coker}(\delta 1)} \times \frac{\sharp\,\mathrm{coker}(\psi_{L_\infty})}{\sharp\,\mathrm{coker}(\lambda_F)}. \tag{3.11}$$

Now, taking alternating products along the exact sequence (3.7) and using (3.11),

$$\sharp \mathrm{H}^0(G, \mathrm{Sel}_p(E/L_\infty)) = \frac{\sharp\,\ker(\delta 1)}{\sharp\,\mathrm{coker}(\delta 1)} \times \frac{\sharp\,\mathrm{coker}(\psi_{L_\infty})}{\sharp\,\mathrm{coker}(\lambda_F)} \times \frac{\sharp\,\mathrm{coker}(\beta 1)}{\sharp\,\ker(\beta 1)} \times \sharp\,\mathrm{Sel}_p(E/F).$$

Consider the vertical map $\beta 1$. The inflation restriction cohomology sequence gives $\ker(\beta 1) = \mathrm{H}^1(G, E_{p_\infty})$. Also, from [3, Lemma 4.3], $\mathrm{H}^2(F^S/F, E_{p_\infty}) = 0$. Hence $\mathrm{coker}(\beta 1) = \mathrm{H}^2(G, E_{p_\infty})$. Now we note that $\sharp\,\mathrm{Sel}_p(E/F) = \sharp Ш_p(E/F)$ and $\mathrm{coker}(\lambda_F) = \widehat{E(F)}(p)$ [3, Lemma 2.7]. Thus,

$$\sharp \mathrm{H}^0(G, \mathrm{Sel}_p(E/L_\infty)) = \frac{\sharp\,\ker(\delta 1)}{\sharp\,\mathrm{coker}(\delta 1)} \times \frac{\sharp\,\mathrm{coker}(\psi_{L_\infty})}{\sharp \widehat{E(F)}(p)} \times \frac{\sharp \mathrm{H}^2(G, E_{p_\infty})}{\sharp \mathrm{H}^1(G, E_{p_\infty})} \times \sharp Ш_p(E/F). \tag{3.12}$$

From Lemma 3.4 , it follows that

$$\frac{\sharp\,\ker(\delta 1)}{\sharp\,\mathrm{coker}(\delta 1)} = \prod_{v\in S_1} \left|\frac{L_v(E,1)}{c_v}\right|_p \times \frac{\sharp \widetilde{E}_v(\kappa_{F_v})(p)}{\prod_{v|p}\big(\prod_{1\le i\le 2} \sharp \mathrm{H}^i(G_u, \widetilde{E}_{v,p^\infty})^{(-1)^i}\big)}. \tag{3.13}$$

Finally, combining (3.10), (3.12), (3.13) and using Lemmas 3.1 and 3.2,

$$\begin{aligned}\chi(G, \mathrm{Sel}_p(E/L_\infty)) &= \frac{\sharp Ш(E/F)(p) \prod_{v|p}((\sharp \widetilde{E}_v(\kappa_{F_v})(p))^2)}{(\sharp ! E(F)(p))^2 \prod_{v\in S} |c_v|_p} \times \Big|\prod_v L_v(E,1)\Big|_p \\ &= \rho_p(E/F) \times \Big|\prod_v L_v(E,1)\Big|_p,\end{aligned}$$

as desired. □

https://doi.org/10.1017/S0004972719000108 Published online by Cambridge University Press

References

[1] P. N. Balister and S. Howson, 'Note on Nakayama's lemma for compact Λ-modules', *Asian. J. Math.* **1**(2) (1997), 224–229.

[2] A. Bhave, 'Analogue of Kida's formula for certain strongly admissible extensions', *J. Number Theory* **122** (2007), 100–120.

[3] J. H. Coates and S. Howson, 'Euler characteristics and elliptic curves II', *J. Math. Soc. Japan* **53**(1) (2001), 175–235.

[4] J. H. Coates and R. Sujatha, *Galois Cohomology of Elliptic Curves*, Tata Institute of Fundamental Research, Lectures on Mathematics, 88 (Narosa Publishing House, New Delhi, 2000).

[5] R. Greenberg, 'Iwasawa theory for elliptic curves', in: *Arithmetic Theory of Elliptic Curves*, Lecture Notes in Mathematics, 1716 (ed. C. Viola) (Springer, Berlin–Heidelberg, 1999), 51–144.

[6] H. Imai, 'A remark on the rational points of Abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions', *Proc. Japan. Acad. Math. Sci.* **51** (1975), 12–16.

[7] M. Lazard, 'Groupes analytiques p-adiques', *Publ. Inst. Hautes Études Sci.* **26** (1965), 389–603.

[8] B. Mazur, 'Rational points of abelian varieties with values in towers of number fields', *Invent. Math.* **18** (1972), 183–266.

[9] J.-P. Serre, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.* **15** (1972), 259–331.

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106 (Springer, New York, 2009).

[11] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, 83 (Springer, New York, 1982).

AMALA BHAVE, School of Physical Sciences,
Jawaharlal Nehru University, New Delhi, India-110067
e-mail: amalasarma@gmail.com

LACHIT BORA, School of Physical Sciences,
Jawaharlal Nehru University, New Delhi, India-110067
e-mail: boralachit3@gmail.com