*Bull. Aust. Math. Soc.* **101** (2020), 238–246
doi:10.1017/S0004972719000704

# ON THE EULER CHARACTERISTICS OF SIGNED SELMER GROUPS

SUMAN AHMED and MENG FAI LIM ✉

(Received 25 April 2019; accepted 22 May 2019; first published online 9 July 2019)

**Abstract**

Let $p$ be an odd prime number and $E$ an elliptic curve defined over a number field $F$ with good reduction at every prime of $F$ above $p$. We compute the Euler characteristics of the signed Selmer groups of $E$ over the cyclotomic $\mathbb{Z}_p$-extension. The novelty of our result is that we allow the elliptic curve to have mixed reduction types for primes above $p$ and mixed signs in the definition of the signed Selmer groups.

2010 *Mathematics subject classification*: primary 11R23; secondary 11G05, 11S25.

*Keywords and phrases*: Euler characteristics, signed Selmer groups.

## 1. Introduction

Let $p$ be an odd prime. Let $F$ be a number field and $E$ an elliptic curve defined over $F$. If $E$ has good ordinary reduction at every prime of $F$ above $p$, one can define the $p$-primary Selmer group of $E$ over the cyclotomic $\mathbb{Z}_p$-extension $F^{\mathrm{cyc}}$ of $F$. This Selmer group is conjectured to be cotorsion over $\mathbb{Z}_p[[\Gamma]]$ (see [13]), where $\Gamma = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$. Under this conjecture, Perrin-Riou [16] and Schneider [17] computed the $\Gamma$-Euler characteristics of the Selmer groups. The importance of the $\Gamma$-Euler characteristics stems from the fact that their values are related to the $p$-part of the algebraic invariants appearing in the formula of the Birch and Swinnerton-Dyer conjecture, which in turn allows one to study the special values of the Hasse–Weil $L$-function of $E$ via the so-called 'Iwasawa main conjecture' (see [2, 3, 5, 13]).

In this paper, we consider the situation where the elliptic curve $E$ may have good supersingular reduction at some primes above $p$. In this case, one usually works with the so-called signed Selmer groups of $E$ in the sense of [7–10]. Our main result is concerned with computing the Euler characteristics of these signed Selmer groups, which we now describe. Suppose that $E$ has good (not necessarily ordinary) reduction at any prime of $F$ lying above $p$. Denote by $S_p^{\mathrm{ord}}$ (respectively, $S_p^{\mathrm{ss}}$) the set of good ordinary reduction (respectively, good supersingular reduction) primes of $E$ above $p$.

M. F. Lim is supported by the National Natural Science Foundation of China under Grant Nos. 11550110172 and 11771164.

Suppose further that for each $v \in S_p^{\mathrm{ss}}$, one has $F_v = \mathbb{Q}_p$ and $a_v = 1 + p - |\tilde{E}_v(\mathbb{F}_p)| = 0$, where $\tilde{E}_v$ denotes the reduction of $E$ at $v$. Our main result is as follows.

Theorem 1.1. *Suppose that* $\mathrm{Sel}(E/F)$ *is finite and retain the settings described above. Then* $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})$ *is a cotorsion* $\mathbb{Z}_p[[\Gamma]]$*-module and its* $\Gamma$*-Euler characteristic is given by*

$$\frac{|Ш(E/F)(p)|}{|E(F)(p)|^2} \times \prod_v c_v^{(p)} \times \prod_{v \in S_p^{ord}} (d_v^{(p)})^2.$$

*Here $c_v^{(p)}$ is the highest power of $p$ dividing $|E(F_v) : E_0(F_v)|$, where $E_0(F_v)$ is the subgroup of $E(F_v)$ consisting of points with nonsingular reduction modulo $v$, $f_v$ is the residue field of $F_v$ and $d_v^{(p)}$ is the highest power of $p$ dividing $|\tilde{E}_v(f_v)|$.*

We give the definition of the signed Selmer group $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})$ in Section 2. The $\Gamma$-Euler characteristic of $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})$ is the quantity

$$\frac{|H^0(\Gamma, \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}))|}{|H^1(\Gamma, \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}))|}.$$

In the course of proving Theorem 1.1, we will see that the definition of the $\Gamma$-Euler characteristic of $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})$ makes sense. When the elliptic curve has good supersingular reduction at all primes above $p$, the formula was first established by Kim [8]. Our main result extends the result in [8] by allowing the elliptic curve to have mixed reduction types for primes above $p$ and mixed signs in the definition of the signed Selmer groups. The proof of the theorem will be given in Section 2. In fact, we consider a slightly more general situation than that stated above (see Theorem 2.3). As an application, we show that if one of the signed Selmer groups vanishes, so do the others (see Corollary 2.9).

It would be of interest to be able to provide examples illustrating our theorem. It is not difficult to obtain examples of elliptic curves with mixed reduction types at primes above $p$ by arguments similar to those in [5, Proposition 5.4] or [13, Lemma 8.19]. The problem is that we do not know how to verify the finiteness of $\mathrm{Sel}(E/F)$ in these examples. Until a (nice enough) theory of Euler systems has been developed in this mixed reduction context, this does not seem tractable.

After the completion of this work, we were informed by Antonio Lei that he and his coauthor have computed the Euler characteristics of the signed Selmer groups over a $\mathbb{Z}_p^d$-extension (see [11]). However, they work with elliptic curves with good supersingular reduction at all primes above $p$ and with the same sign in their definition of the signed Selmer groups. They also require that the prime $p$ splits completely over $F/\mathbb{Q}$. It would be of interest to see if a similar computation can be performed for the situation considered in Section 2 of our paper. One might even contemplate computing these Euler characteristics over a noncommutative $p$-adic extension.

https://doi.org/10.1017/S0004972719000704 Published online by Cambridge University Press

## 2. Signed Selmer groups

In this section, we will prove Theorem 1.1. As the formula is well documented when $E$ has good ordinary reduction at every prime of $F$ above $p$ (see [2, Theorem 3.3] or [5, Theorem 4.1]), we may and will assume that our elliptic curve $E$ has some primes of supersingular reduction above $p$. In this situation, we shall consider a slightly more general setting following [9]. As always, $p$ will denote a fixed odd prime. Let $F'$ be a number field and $E$ an elliptic curve defined over $F'$. Fix a finite extension $F$ of $F'$. Let $S$ be a finite set of primes of $F'$ which contains the primes above $p$, the bad reduction primes of $E$, the ramified primes of $F/F'$ and the infinite primes. Denote by $F_S$ the maximal algebraic extension of $F$ which is unramified outside $S$. For every (possibly infinite) extension $L$ of $F$ contained in $F_S$, we set $G_S(L) = \mathrm{Gal}(F_S/L)$. We shall write $S_p$ (respectively, $S'_p$) for the set of primes of $S$ lying above $p$ (respectively, not lying above $p$). Denote by $S_p^{\mathrm{ord}}$ (respectively, $S_p^{\mathrm{ss}}$) the set of good ordinary reduction (respectively, good supersingular reduction) primes of $E$ above $p$. We make the following assumptions.

(S1) The elliptic curve $E$ has good reduction at all primes in $S_p$ and $S_p^{\mathrm{ss}} \neq \emptyset$.

(S2) For each $v \in S_p^{\mathrm{ss}}$, one has $F'_v = \mathbb{Q}_p$ and $a_v = 1 + p - |\tilde{E}_v(\mathbb{F}_p)| = 0$, where $\tilde{E}_v$ is the reduction of $E$ at $v$.

(S3) For each $v \in S_p^{\mathrm{ss}}$, $v$ is unramified in $F/F'$.

(S4) For each $w \in S_p^{\mathrm{ss}}(F)$, $[F_w : \mathbb{Q}_p] \not\equiv 0 \pmod 4$. Here $S_p^{\mathrm{ss}}(F)$ is the set of primes of $F$ above $S_p^{\mathrm{ss}}$.

Denote by $F^{\mathrm{cyc}}$ the cyclotomic $\mathbb{Z}_p$-extension of $F$ and $F_n$ the intermediate subfield of $F^{\mathrm{cyc}}$ with $|F_n : F| = p^n$. Note that it follows from (S2) and (S3) that every prime $w \in S_p^{\mathrm{ss}}(F)$ is totally ramified in $F^{\mathrm{cyc}}/F$. In particular, for each such prime $w$, there is a unique prime of $F_n$ lying above $w$, which, by abuse of notation, we still denote by $w$. Following [7–10], we define the groups

$$\begin{aligned} E^+(F_{n,w}) &= \{P \in E(F_{n,w}) \ : \ \mathrm{tr}_{n/m+1}(P) \in E(F_{m,w}), 2 \mid m, -1 \le m \le n-1\}, \\ E^-(F_{n,w}) &= \{P \in E(F_{n,w}) \ : \ \mathrm{tr}_{n/m+1}(P) \in E(F_{m,w}), 2 \nmid m, -1 \le m \le n-1\}, \end{aligned}$$

where $\mathrm{tr}_{n/m+1} : E(F_{n,w}) \longrightarrow E(F_{m+1,w})$ denotes the trace map.

From now on, let $I = \{1, \ldots, r\}$, where $r = |S_p^{\mathrm{ss}}(F)|$. We shall index the primes in $S_p^{\mathrm{ss}}(F)$ by $w_1, \ldots, w_r$. For each $\vec{s} = (s_1, \ldots, s_r) \in \{\pm\}^I$, we write

$$\mathcal{H}_n^{\vec{s}} = \bigoplus_{i=1}^{r} \frac{H^1(F_{n,w_i}, E(p))}{E^{s_i}(F_{n,w_i}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}.$$

The signed Selmer group $\mathrm{Sel}^{\vec{s}}(E/F_n)$ is then defined to be

$$\ker\Big(H^1(G_S(F_n), E(p)) \longrightarrow \mathcal{H}_n^{\vec{s}} \times \bigoplus_{w \in S_p^{\mathrm{ord}}(F_n)} \frac{H^1(F_{n,w}, E(p))}{E(F_{n,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \times \bigoplus_{w \in S'_p(F_n)} H^1(F_{n,w}, E(p))\Big),$$

https://doi.org/10.1017/S0004972719000704 Published online by Cambridge University Press

where $S_p^{\mathrm{ord}}(F_n)$ (respectively, $S'_p(F_n)$) denotes the set of primes of $F_n$ above $S_p^{\mathrm{ord}}$ (respectively, $S'_p$). We also recall that the usual $p$-primary Selmer group for $E$ over $F_n$ is defined by

$$\begin{aligned}&\mathrm{Sel}(E/F_n)\\ &\quad = \ker\Big(H^1(G_S(F_n), E(p)) \longrightarrow \bigoplus_{w\in S_p(F_n)} \frac{H^1(F_{n,w}, E(p))}{E(F_{n,w})\otimes \mathbb{Q}_p/\mathbb{Z}_p} \times \bigoplus_{w\in S'_p(F_n)} H^1(F_{n,w}, E(p))\Big).\end{aligned}$$

The two Selmer groups fit into the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}^{\vec{s}}(E/F_n) \arrow[r] \arrow[d, "\alpha"'] & H^1(G_S(F_n), E(p)) \arrow[r, "\psi^{\vec{s}}"] \arrow[d, equal] & \mathcal{H}_n^{\vec{s}} \times \bigoplus_{w\in S_p^{\mathrm{ord}}(F_n)} \frac{H^1(F_{n,w}, E(p))}{E(F_{n,w})\otimes \mathbb{Q}_p/\mathbb{Z}_p} \times \bigoplus_{w\in S'_p(F_n)} H^1(F_{n,w}, E(p)) \arrow[d] \\
0 \arrow[r] & \mathrm{Sel}(E/F_n) \arrow[r] & H^1(G_S(F_n), E(p)) \arrow[r, "\phi"] & \bigoplus_{w\in S_p(F_n)} \frac{H^1(F_{n,w}, E(p))}{E(F_{n,w})\otimes \mathbb{Q}_p/\mathbb{Z}_p} \times \bigoplus_{w\in S'_p(F_n)} H^1(F_{n,w}, E(p))
\end{tikzcd}$$

with exact rows. Denote by $\psi_{ss}^{\vec{s}}$ the map from $\mathrm{Sel}(E/F_n)$ to $\mathcal{H}_n^{\vec{s}}$ that is induced by $\psi^{\vec{s}}$. It is now straightforward to verify the following assertion.

LEMMA 2.1. *We have the identification*

$$\mathrm{Sel}^{\vec{s}}(E/F_n) = \ker(\mathrm{Sel}(E/F_n) \xrightarrow{\psi_{ss}^{\vec{s}}} \mathcal{H}_n^{\vec{s}}).$$

Write

$$\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}) = \varinjlim_n \mathrm{Sel}^{\vec{s}}(E/F_n) \quad \text{and} \quad \mathcal{H}_\infty^{\vec{s}} = \varinjlim_n \mathcal{H}_n^{\vec{s}}.$$

It is not difficult to verify that $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})$ is cofinitely generated over $\mathbb{Z}_p[[\Gamma]]$. In fact, one expects the following conjecture, which is a natural extension of Mazur [13] and Kobayashi [10].

CONJECTURE 2.2. $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})$ *is a cotorsion* $\mathbb{Z}_p[[\Gamma]]$*-module, where* $\Gamma = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$.

When $S_p^{\mathrm{ss}}$ is empty, the above conjecture is precisely Mazur's conjecture [13], which is known in the case when $E$ is defined over $\mathbb{Q}$ and $F$ is an abelian extension of $\mathbb{Q}$ (see [6]). When $E$ is an elliptic curve over $\mathbb{Q}$ with good supersingular singular reduction at $p$, this conjecture was formulated by Kobayashi [10] (see [1] for some recent progress on this conjecture). We shall prove the following result from which Theorem 1.1 follows by taking $F = F'$.

THEOREM 2.3. *Assume that (S1)–(S4) hold and* $\mathrm{Sel}(E/F)$ *is finite. Then* $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})$ *is a cotorsion* $\mathbb{Z}_p[[\Gamma]]$*-module and its* $\Gamma$*-Euler characteristic is given by*

$$\frac{|Ш(E/F)(p)|}{|E(F)(p)|^2} \times \prod_w c_w^{(p)} \times \prod_{w\in S_p^{\mathrm{ord}}(F)} (d_w^{(p)})^2.$$

https://doi.org/10.1017/S0004972719000704 Published online by Cambridge University Press

The remainder of this section will be devoted to the proof of Theorem 2.3. We first record two preparatory lemmas which are required for our calculation.

LEMMA 2.4. *Assume that (S1)–(S3) hold. Then* $E(F)(p) = 0$ *and* $E(F^{\mathrm{cyc}})(p) = 0$.

PROOF. For $w \in S_p^{\mathrm{ss}}(F)$, a similar argument to that in [10, Proposition 8.7] yields $E(F_w)(p) = 0$. Since we are assuming that $S_p^{\mathrm{ss}} \neq \emptyset$, this in turn implies that $E(F)(p) = 0$. But, as $F^{\mathrm{cyc}}/F$ is a pro-$p$ extension, it follows from [15, Corollary 1.6.13] that $E(F^{\mathrm{cyc}})(p) = 0$. □

LEMMA 2.5. *Assume that (S1)–(S3) hold and* $\mathrm{Sel}(E/F)$ *is finite. Then*

$$H^2(G_S(F^{\mathrm{cyc}}), E(p)) = 0, \quad H^1(\Gamma, H^1(G_S(F^{\mathrm{cyc}}), E(p))) = 0$$

*and*

$$H^1(G_S(F), E(p)) \cong H^1(G_S(F^{\mathrm{cyc}}), E(p))^{\Gamma}.$$

PROOF. Since $\Gamma$ has $p$-cohomological dimension one, the spectral sequence

$$H^i(\Gamma, H^j(G_S(F^{\mathrm{cyc}}), E(p))) \Longrightarrow H^{i+j}(G_S(F), E(p))$$

yields short exact sequences

$$0 \longrightarrow H^1(\Gamma, E(F^{\mathrm{cyc}})(p))) \longrightarrow H^1(G_S(F), E(p)) \longrightarrow H^1(G_S(F^{\mathrm{cyc}}), E(p))^{\Gamma} \longrightarrow 0$$

and

$$0 \to H^1(\Gamma, H^1(G_S(F^{\mathrm{cyc}}), E(p))) \to H^2(G_S(F), E(p)) \to H^2(G_S(F^{\mathrm{cyc}}), E(p))^{\Gamma} \to 0.$$

The final isomorphism of the lemma follows from the first short exact sequence and Lemma 2.4. On the other hand, as $\mathrm{Sel}(E/F)$ is finite, it follows from [2, Proposition 1.9] that $H^2(G_S(F), E(p)) = 0$. Putting this into the second short exact sequence yields $H^1(\Gamma, H^1(G_S(F^{\mathrm{cyc}}), E(p))) = 0$ and $H^2(G_S(F^{\mathrm{cyc}}), E(p))^{\Gamma} = 0$, where the latter in turn implies that $H^2(G_S(F^{\mathrm{cyc}}), E(p)) = 0$. This proves the lemma. □

Let $w \in S_p^{\mathrm{ss}}(F)$. The next lemma is concerned with analysing the local map

$$g_w : \frac{H^1(F_w, E(p))}{E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \longrightarrow \left( \frac{H^1(F_w^{\mathrm{cyc}}, E(p))}{E^{\pm}(F_w^{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^{\Gamma}.$$

LEMMA 2.6. *If (S1)–(S4) hold, then the map* $g_w$ *is an isomorphism for every* $w \in S_p^{\mathrm{ss}}(F)$.

PROOF. We essentially follow the idea in the proof of [7, Proposition 4.28]. Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \arrow[r] \arrow[d, "a_w"'] & H^1(F_w, E(p)) \arrow[r] \arrow[d, "b_w"'] & \dfrac{H^1(F_w, E(p))}{E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \arrow[r] \arrow[d, "g_w"'] & 0 \\
0 \arrow[r] & (E^{\pm}(F_w^{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma} \arrow[r] & H^1(F_w^{\mathrm{cyc}}, E(p))^{\Gamma} \arrow[r] & \left( \dfrac{H^1(F_w^{\mathrm{cyc}}, E(p))}{E^{\pm}(F_w^{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)^{\Gamma} &
\end{tikzcd}$$

https://doi.org/10.1017/S0004972719000704 Published online by Cambridge University Press

with exact rows. As seen from the proof of Lemma 2.4, $E(F_w)(p) = 0$, which in turn implies that $E(F_w^{\mathrm{cyc}})(p) = 0$. Hence, $b_w$ is an isomorphism. Consequently, $a_w$ is injective. By (S4) and [9, Corollary 3.25], $(E^{\pm}(F_w^{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma}$ is a cofree $\mathbb{Z}_p$-module with $\mathbb{Z}_p$-corank $[F_w : \mathbb{Q}_p]$. But, by Mattuck's theorem [12], $E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ is also a cofree $\mathbb{Z}_p$-module with $\mathbb{Z}_p$-corank $[F_w : \mathbb{Q}_p]$. Hence, $a_w$ must be an isomorphism, which in turn implies that $g_w$ is injective.

Since $E(F_w)(p) = 0$, it follows from local Tate duality that $H^2(F_w, E[p]) = 0$, which in turn implies that $H^1(F_w, E(p))$ is $p$-divisible. Combining this with a standard local Euler characteristic calculation (see [3, Section 3, Proposition 1]), we see that $H^1(F_w, E(p))$ is a cofree $\mathbb{Z}_p$-module with $\mathbb{Z}_p$-corank $[F_w : \mathbb{Q}_p]$ . On the other hand, from [9, Proposition 3.32], $(H^1(F_w^{\mathrm{cyc}}, E(p))/E^{\pm}(F_w^{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\Gamma}$ is a cofree $\mathbb{Z}_p$-module with $\mathbb{Z}_p$-corank $[F_w : \mathbb{Q}_p]$. Thus, $g_w$ is an injection between two $p$-divisible groups of the same $\mathbb{Z}_p$-corank and hence it must be an isomorphism. This proves the lemma. □

Now consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}(E/F) \arrow[r] \arrow[d, "a"] & H^1(G_S(F), E(p)) \arrow[r, "\rho"] \arrow[d, "h"] & \displaystyle\bigoplus_{w|p} \frac{H^1(F_w, E(p))}{E(F_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p} \times \bigoplus_{w \in S_p'(F)} H^1(F_w, E(p)) \arrow[d, "g=\oplus_w g_w"] \\
0 \arrow[r] & \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})^{\Gamma} \arrow[r] & H^1(G_S(F^{\mathrm{cyc}}), E(p))^{\Gamma} \arrow[r, "\phi_\infty"] & \displaystyle\Big(\mathcal{H}_\infty^{\vec{s}} \times \mathcal{H}_\infty^{\mathrm{ord}} \times \bigoplus_{w \in S_p'(F^{\mathrm{cyc}})} H^1(F_w^{\mathrm{cyc}}, E(p))\Big)^{\Gamma}
\end{tikzcd}$$

with exact rows, where

$$\mathcal{H}_\infty^{\mathrm{ord}} = \varinjlim_n \bigoplus_{w \in S_p^{\mathrm{ord}}(F_n)} \frac{H^1(F_{n,w}, E(p))}{E(F_{n,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}.$$

We shall make use of the notation in the above diagram without further mention.

Lemma 2.7. *Assume that (S1)–(S4) hold and that* $\mathrm{Sel}(E/F)$ *is finite. Then* $\rho$ *is surjective and* $H^1(\Gamma, \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})) = 0$.

Proof. Since $\mathrm{Sel}(E/F)$ is finite, it follows from [2, Proposition 1.9] that $\operatorname{coker}\rho$ is finite of order $|E(F)(p)|$. By Lemma 2.4, this implies that $\rho$ is surjective, which proves the first assertion of the lemma.

Combining [2, Lemma 3.4 and Proposition 3.5] with Lemma 2.6, we see that $g$ is surjective. Therefore, $\phi_\infty$ is also surjective. Now consider the exact sequence

$$0 \longrightarrow \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}) \longrightarrow H^1(G_S(F^{\mathrm{cyc}}), E(p)) \xrightarrow{\ \phi\ } B,$$

where $B = \mathcal{H}_\infty^{\vec{s}} \times \mathcal{H}_\infty^{\mathrm{ord}} \times \bigoplus_{w \nmid p} H^1(F_w^{\mathrm{cyc}}, E(p))$. Write $A = \mathrm{im}(\phi)$ and $C = \mathrm{coker}\,(\phi)$. Taking the $\Gamma$-invariant of the short exact sequence

$$0 \longrightarrow \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}) \longrightarrow H^1(G_S(F^{\mathrm{cyc}})E(p)) \longrightarrow A \longrightarrow 0,$$

https://doi.org/10.1017/S0004972719000704 Published online by Cambridge University Press

and using Lemma 2.5 yields the exact sequence

$$0 \to \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})^{\Gamma} \to H^1(G_S(F^{\mathrm{cyc}}), E(p))^{\Gamma} \xrightarrow{\tau} A^{\Gamma} \longrightarrow H^1(\Gamma, \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})) \to 0$$

with $H^1(\Gamma, A) = 0$. Then, from the $\Gamma$-invariant of the short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

we obtain a short exact sequence

$$0 \longrightarrow A^{\Gamma} \longrightarrow B^{\Gamma} \longrightarrow C^{\Gamma} \longrightarrow 0.$$

Since $\phi_\infty$ is given by the composition $H^1(G_S(F^{\mathrm{cyc}}), E(p)) \longrightarrow A^{\Gamma} \longrightarrow B^{\Gamma}$ and is surjective, the injection $A^{\Gamma} \longrightarrow B^{\Gamma}$ is also surjective and hence an isomorphism. Under this identification, $\tau = \phi_\infty$ and its surjectivity in turn implies that $H^1(\Gamma, \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})) = 0$. This completes proof of the lemma. □

We record a by-product of our argument, which is not required for the final proof. It may also be possible to derive this result by the methods of [8, Proposition 3.10]. However, we include the following alternative proof, which might be of interest in its own right. We should emphasise that our proof relies on the finiteness of $\mathrm{Sel}(E/F)$.

Proposition 2.8. *Assume that (S1)–(S4) hold and that* $\mathrm{Sel}(E/F)$ *is finite. Then we have the short exact sequence*

$$0 \to \mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}) \to H^1(G_S(F^{\mathrm{cyc}}), E(p)) \xrightarrow{\phi} \mathcal{H}^{\vec{s}}_{\infty} \times \mathcal{H}^{\mathrm{ord}}_{\infty} \times \bigoplus_{w \in S'_p(F^{\mathrm{cyc}})} H^1(F^{\mathrm{cyc}}_w, E(p)) \to 0.$$

Proof. We retain the notation of Lemma 2.7. In the proof of Lemma 2.7, we obtained a short exact sequence

$$0 \longrightarrow A^{\Gamma} \longrightarrow B^{\Gamma} \longrightarrow C^{\Gamma} \longrightarrow 0$$

and showed that $A^{\Gamma} \cong B^{\Gamma}$. Thus, $C^{\Gamma} = 0$, which in turn implies that $C = 0$. But recall that $C = \operatorname{coker}\phi$ and so this proves the proposition. □

We can finally prove Theorem 2.3.

Proof of Theorem 2.3. To prove the first assertion of the theorem, it suffices to show that $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})^{\Gamma}$ is finite. By Lemma 2.5, $h$ is an isomorphism. Therefore, by the snake lemma, we are reduced to showing that $\ker g$ is finite. In fact, for $w \in S_p^{\mathrm{ord}}(F)$, $\ker g_w$ is finite with order $(d_w^{(p)})^2$ (see [2, Proposition 3.5] or [5, Lemma 4.4]). If $w \in S_p^{\mathrm{ss}}(F)$, then $g_w$ is an isomorphism by Lemma 2.6. Finally, for $w \nmid p$, $\ker g_w$ is finite with order $c_w^{(p)}$ (see [2, Lemma 3.4] or [5, Lemma 4.4]). Hence, $\ker g$ is finite, as required.

It remains to compute the $\Gamma$-Euler characteristic of $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})$. By Lemma 2.5, $\rho$ is surjective. Taking the final isomorphism in the assertion of Lemma 2.5 into account, it then follows from the above diagram that

$$|\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})^{\Gamma}| = |\mathrm{Sel}(E/F)|\,|\ker g|.$$

https://doi.org/10.1017/S0004972719000704 Published online by Cambridge University Press

By Lemma 2.7, the left-hand side is just the $\Gamma$-Euler characteristic of $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})$. Since $\mathrm{Sel}(E/F)$ is finite, $|\mathrm{Sel}(E/F)| = |Ш(E/F)(p)|$. Also, as seen above, $|\ker g|$ is given by $\prod_w c_w^{(p)} \times \prod_{w\in S_p^{\mathrm{ord}}(F)} (d_w^{(p)})^2$. Combining these calculations, we obtain the required formula, noting that $|E(F)(p)| = 1$ by Lemma 2.4. □

We record an interesting corollary of (the proof of) Theorem 2.3.

Corollary 2.9. *Assume that (S1)–(S4) hold. Suppose that there exists* $\vec{t} \in \{\pm\}^I$ *such that* $\mathrm{Sel}^{\vec{t}}(E/F^{\mathrm{cyc}}) = 0$. *Then* $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}) = 0$ *for every* $\vec{s} \in \{\pm\}^I$.

Proof. Suppose that $\mathrm{Sel}^{\vec{t}}(E/F^{\mathrm{cyc}}) = 0$ for some $\vec{t} \in \{\pm\}^I$. Then, from the diagram before Lemma 2.7, we see that $\mathrm{Sel}(E/F) = 0$. In particular, $\mathrm{Sel}(E/F)$ is finite. Therefore, by the argument in the proof of Theorem 2.3,

$$|\mathrm{Sel}^{\vec{t}}(E/F^{\mathrm{cyc}})^{\Gamma}| = |\mathrm{Sel}(E/F)|\,|\ker g| = |\ker g|.$$

Since $\mathrm{Sel}^{\vec{t}}(E/F^{\mathrm{cyc}}) = 0$, it follows that $\ker g = 0$. From the proof of Theorem 2.3, we also see that $\ker g$ has the same common value for every $\vec{s} \in \{\pm\}^I$ and hence is trivial. Consequently,

$$|\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})^{\Gamma}| = 0,$$

which in turn implies that $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}})^{\Gamma} = 0$. The latter is of course equivalent to $\mathrm{Sel}^{\vec{s}}(E/F^{\mathrm{cyc}}) = 0$, as required. □

## 3. Concluding remarks

In Theorem 2.3, we assume that for each $w \in S_p^{\mathrm{ss}}(F)$, $[F_w : \mathbb{Q}_p] \neq 0 \pmod 4$ (this is assumption (S4)). If all the signs appearing in the signed Selmer group are −, one does not require this assumption (S4). However, if at least one of the signs is a +, we are not able to prove that the local map $g_w$ is injective without this assumption. In fact, tracing the proof of Lemma 2.6, it would seem that $g_w$ has a kernel which is a cofree $\mathbb{Z}_p$-module with corank 2 (when $[F_w : \mathbb{Q}_p] = 0 \pmod 4$). This seems reminiscent of the so-called 'exceptional zeros' phenomenon in the case of a split multiplicative prime (see [4, 14]). We do not have a good explanation at present.

## Acknowledgements

The authors are very grateful to Antonio Lei for his interest in the paper and for sharing the preprint [11]. In particular, we would like to thank him for suggesting a more direct proof of Corollary 2.9. We would also like to thank the anonymous referee for providing various helpful comments that have improved the exposition of the paper. The research of this article took place when S. Ahmed was a postdoctoral fellow at Central China Normal University and he would like to acknowledge the hospitality and conducive working conditions provided there.

https://doi.org/10.1017/S0004972719000704 Published online by Cambridge University Press

## References

[1] K. Büyükboduk and A. Lei, ‘Integral Iwasawa theory of Galois representations for non-ordinary primes’, *Math. Z.* **286** (2017), 361–398.

[2] J. Coates and R. Sujatha, *Galois Cohomology of Elliptic Curves*, 2nd edn, Tata Institute of Fundamental Research Lectures on Mathematics, 88 (Narosa, New Delhi–Mumbai, 2010).

[3] R. Greenberg, ‘Iwasawa theory for $p$-adic representations’, in: *Algebraic Number Theory—in Honor of K. Iwasawa*, Advanced Studies in Pure Mathematics, 17 (eds. J. Coates, R. Greenberg, B. Mazur and I. Satake) (Kinokuniya–Mathematical Society of Japan, Tokyo, 1989), 97–137.

[4] R. Greenberg, ‘Trivial zeros of $p$-adic $L$-functions’, in: *p-adic Monodromy and the Birch and Swinnerton-Dyer Conjecture (Boston, MA, 1991)*, Contemporary Mathematics, 165 (American Mathematical Society, Providence, RI, 1994), 149–174.

[5] R. Greenberg, ‘Iwasawa theory for elliptic curves’, in: *Arithmetic Theory of Elliptic Curves (Cetraro, 1997)*, Lecture Notes in Mathematics, 1716 (ed. C. Viola) (Springer, Berlin, 1999), 51–144.

[6] K. Kato, ‘$p$-adic Hodge theory and values of zeta functions of modular forms’, in: *Cohomologies p-adiques et applications arithmétiques. III*, Astérisque, 295 (Société Mathématique de France, Paris, 2004), 117–290.

[7] B. D. Kim, ‘The parity conjecture for elliptic curves at supersingular reduction primes’, *Compos. Math.* **143** (2007), 47–72.

[8] B. D. Kim, ‘The plus/minus Selmer groups for supersingular primes’, *J. Aust. Math. Soc.* **95**(2) (2013), 189–200.

[9] T. Kitajima and R. Otsuki, ‘On the plus and the minus Selmer groups for elliptic curves at supersingular primes’, *Tokyo J. Math.* **41**(1) (2018), 273–303.

[10] S. Kobayashi, ‘Iwasawa theory for elliptic curves at supersingular primes’, *Invent. Math.* **152**(1) (2003), 1–36.

[11] A. Lei and R. Sujatha, ‘On Selmer groups in the supersingular reduction case’, Preprint.

[12] A. Mattuck, ‘Abelian varieties over $p$-adic ground fields’, *Ann. of Math. (2)* **62** (1955), 92–119.

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

[14] B. Mazur, J. Tate and J. Teitelbaum, ‘On $p$-adic analogues of the conjectures of Birch and Swinnerton-Dyer’, *Invent. Math.* **84** (1986), 1–48.

[15] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, 2nd edn, Grundlehren der Mathematischen Wissenschaften, 323 (Springer, Berlin, 2008).

[16] B. Perrin-Riou, ‘Arithmétique des courbes elliptiques et theórie d’Iwasawa’, *Mém. Soc. Math. Fr.* **17** (1984), 1–129.

[17] P. Schneider, ‘Iwasawa $L$-functions of varieties over algebraic number fields. A first approach’, *Invent. Math.* **71** (1983), 251–293.

SUMAN AHMED, School of Mathematics and Statistics,
Central China Normal University,
Wuhan, 430079, PR China
e-mail: npur.suman@gmail.com

MENG FAI LIM, School of Mathematics and Statistics and
Hubei Key Laboratory of Mathematical Sciences,
Central China Normal University, Wuhan, 430079, PR China
e-mail: limmf@mail.ccnu.edu.cn

https://doi.org/10.1017/S0004972719000704 Published online by Cambridge University Press