Canad. J. Math. Vol. 75 (1), 2023 pp. 298–321
http://dx.doi.org/10.4153/S0008414X21000699

Euler characteristics and their congruences for multisigned Selmer groups

Anwesh Ray and R. Sujatha

Abstract. The notion of the truncated Euler characteristic for Iwasawa modules is a generalization of the the usual Euler characteristic to the case when the Selmer groups are not finite. Let p be an odd prime, E_1 and E_2 be elliptic curves over a number field F with semistable reduction at all primes $v|p$ such that the $\operatorname{Gal}(\overline{F}/F)$-modules $E_1[p]$ and $E_2[p]$ are irreducible and isomorphic. We compare the Iwasawa invariants of certain imprimitive multisigned Selmer groups of E_1 and E_2. Leveraging these results, congruence relations for the truncated Euler characteristics associated to these Selmer groups over certain $\mathbb{Z}_p^m$-extensions of F are studied. Our results extend earlier congruence relations for elliptic curves over $\mathbb{Q}$ with good ordinary reduction at p.

1 Introduction

The Iwasawa theory of Galois representations, especially those arising from elliptic curves and Hecke eigencuspforms, affords deep insights into the arithmetic of such objects. Let p be a fixed odd prime. Mazur [23] and Greenberg [6] initiated the Iwasawa theory of p-ordinary elliptic curves E defined over $\mathbb{Q}$. The main object of study is the p^∞-Selmer group over the cyclotomic $\mathbb{Z}_p$-extension, denoted by $\operatorname{Sel}(E/\mathbb{Q}^{\text{cyc}})$. Let Γ denote the Galois group of the cyclotomic $\mathbb{Z}_p$-extension over $\mathbb{Q}$. When E has good ordinary reduction at the prime p, it was conjectured by Mazur that the Selmer group $\operatorname{Sel}(E/\mathbb{Q}^{\text{cyc}})$ is cotorsion as a module over the Iwasawa algebra $\mathbb{Z}_p[[\Gamma]]$. This is now a celebrated theorem of Kato [12]. The corresponding theory for p-supersingular elliptic curves was initiated by Perrin-Riou in [26] and has since gained considerable momentum, see [10, 13, 16–19, 22, 28, 34]. If E has supersingular reduction at p, then $\operatorname{Sel}(E/\mathbb{Q}^{\text{cyc}})$ is no longer $\mathbb{Z}_p[[\Gamma]]$-cotorsion. Kobayashi considered plus and minus Selmer groups, which were defined using plus and minus norm groups, that were introduced in [26]. These signed Selmer groups are cotorsion over $\mathbb{Z}_p[[\Gamma]]$.

Suppose E is an elliptic curve defined over a number field F. Let Σ_p denote the set of primes of F above p. In the case when E has good reduction at all primes in Σ_p, and $F_v \simeq \mathbb{Q}_p$ for all $v \in \Sigma_p$ such that E is supersingular at v, generalizations of the plus/minus Selmer groups have been studied in [10, 15, 25]. The case where E has semistable reduction at the primes in Σ_p (i.e., good ordinary, multiplicative or good supersingular) has also been considered, see [20, 21]. In this paper, we assume

Received by the editors November 9, 2020; revised December 16, 2021; accepted December 30, 2021.
Published online on Cambridge Core January 10, 2022.
AMS subject classification: 11R23.
Keywords: Euler characteristics in Iwasawa theory, congruences, multisigned selmer groups, Iwasawa invariants.

that E has semistable reduction at the primes in Σ_p. In this *mixed*-reduction setting, a plethora of Selmer groups depending on the reduction-types at the primes in Σ_p can be defined. This collection of Selmer groups is referred to as the multisigned Selmer groups.

Denote by $\Sigma_{ss}(E) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_d\}$ the set of primes of F above p at which E has good supersingular reduction. Associated to each vector $\ddagger \in \{+,-\}^d$, there is a multisigned Selmer group $\mathrm{Sel}^{\ddagger}(E/F^{\mathrm{cyc}})$, defined in Section 2. There are 2^d vectors $\ddagger$ and hence 2^d Selmer groups to consider.

Two elliptic curves E_1 and E_2 over F are said to be p-congruent if their associated residual representations are isomorphic, i.e., $E_1[p]$ and $E_2[p]$ are isomorphic as Galois modules. It is of particular interest in Iwasawa theory to study the relationship between Iwasawa invariants of the Selmer groups of p-congruent elliptic curves. Such investigations were initiated by Greenberg and Vatsal [8], who considered p-congruent, p-ordinary elliptic curves E_1 and E_2 defined over $\mathbb{Q}$. They showed that the main conjecture is true for E_1 if and only if the main conjecture is true for E_2. To this end, they study the relationship between the algebraic and analytic Iwasawa invariants of E_1 and E_2. Their method involves examining the algebraic structure of certain imprimitive Selmer groups associated to E_1 and E_2 in comparing the Iwasawa-invariants. Let Σ_0 be the set of primes $v \nmid p$ of F at which E_1 or E_2 has bad reduction. Greenberg and Vatsal compare the Σ_0-imprimitive Selmer groups of E_1 and E_2. Their results were generalized to the p-supersingular case for the plus and minus Selmer groups by Kim in [13] and Ponsinet [29].

In this paper, the above mentioned results of Greenberg-Vatsal and Kim are generalized to the mixed reduction setting. Let E_1 and E_2 be two elliptic curves defined over a number field F that are p-congruent for an odd prime p. Assume that both E_1 and E_2 have semistable reduction at all primes of F above p. In other words, E_1 and E_2 both have good reduction or multiplicative reduction at the primes above p. Assume further that the conditions of Hypothesis 2.1 are satisfied. Since E_1 and E_2 are p-congruent, it follows that the sets $\Sigma_{ss}(E_1)$ and $\Sigma_{ss}(E_2)$ are equal (see [25, Proposition 3.9]). Set $\Sigma_{ss} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_d\}$ to denote the set of supersingular primes $v|p$ of E_1 and E_2, and let $\ddagger \in \{+,-\}^d$ be a signed vector. The signed vector prescribes a choice of local condition at each prime in Σ_{ss}. Associated with E_1 and E_2 and $\ddagger$, we consider p-primary Selmer groups $\mathrm{Sel}^{\ddagger}(E_1/F^{\mathrm{cyc}})$ and $\mathrm{Sel}^{\ddagger}(E_2/F^{\mathrm{cyc}})$. We refer to Definition 2.2 for the precise definition. We shall assume throughout for $i = 1, 2$ that the Selmer groups $\mathrm{Sel}^{\ddagger}(E_i/F^{\mathrm{cyc}})$ are cotorsion over the Iwasawa algebra.

Given E_1 and E_2, recall that Σ_0 is the set of all primes $v \nmid p$ at which either E_1 or E_2 has bad reduction. There is a subset Σ_1 of the set of primes Σ_0 which plays a role in the statement of our results (see Definition 4.1). The imprimitive Selmer group $\mathrm{Sel}^{\Sigma_1,\ddagger}(E_i/F^{\mathrm{cyc}})$ is defined by relaxing the Selmer conditions at the primes in Σ_1. The precise definition is given in the discussion preceding Proposition 2.3. Our first result in this paper is Theorem 4.5. We show that if the μ-invariant of $\mathrm{Sel}^{\Sigma_1,\ddagger}(E_1/F^{\mathrm{cyc}})$ is zero, then the μ-invariant of $\mathrm{Sel}^{\Sigma_1,\ddagger}(E_2/F^{\mathrm{cyc}})$ is also zero. Further, if these μ-invariants are both zero, then the imprimitive λ-invariants of $\mathrm{Sel}^{\Sigma_1,\ddagger}(E_1/F^{\mathrm{cyc}})$ and $\mathrm{Sel}^{\Sigma_1,\ddagger}(E_2/F^{\mathrm{cyc}})$ are equal. This result does more than simply generalize the aforementioned results. Over the rational numbers, if Theorem 4.5 is specialized to the case of p-ordinary reduction (resp. p-supersingular reduction), we obtain refinements of the results Greenberg-Vatsal (resp. Kim, Ponsinet). This is due to the fact that the set of primes Σ_1 is optimal in the sense that it is smaller than the full set of primes Σ_0 (considered in previous works).

The Euler characteristic of the p-primary Selmer group an elliptic curve over $\mathbb{Q}$ with p-ordinary reduction may be defined when the Selmer group over $\mathbb{Q}$ is finite. Furthermore, it is of significant interest from the point of view of the p-adic Birch and Swinnerton-Dyer conjecture. The truncated Euler characteristic is a derived version of the usual Euler characteristic, which may be defined in the positive rank setting. Setting $\Gamma := \mathrm{Gal}(F^{\mathrm{cyc}}/F)$, consider the natural map

$$\phi : \mathrm{Sel}^{\ddagger}(E_i/F^{\mathrm{cyc}})^{\Gamma} \to \mathrm{Sel}^{\ddagger}(E_i/F^{\mathrm{cyc}})_{\Gamma},$$

for which $\phi(x)$ is the residue class of x in $\mathrm{Sel}^{\ddagger}(E_i/F^{\mathrm{cyc}})_{\Gamma}$. The truncated Euler characteristic of $\mathrm{Sel}^{\ddagger}(E_i/F^{\mathrm{cyc}})$ can be defined if both the kernel and cokernel of ϕ are finite (see Definition 3.1). If this is the case, we set

$$\chi_t^{\ddagger}(\Gamma, E_i) := \frac{\#\ker\phi}{\#\operatorname{cok}\phi}.$$

The reader is referred to Lemma 3.3 for precise conditions under which the truncated Euler characteristic $\chi_t^{\ddagger}(\Gamma, E_i)$ is well defined (also see Remark 5.0.1).

Leveraging our results on μ-invariants and imprimitive λ-invariants, we prove congruence relations for the truncated Euler characteristics of multisigned Selmer groups of the p-congruent elliptic curves E_1 and E_2. Theorem 5.5 is the main result of the paper, in which $\chi_t^{\ddagger}(\Gamma, E_1)$ is precisely related to $\chi_t^{\ddagger}(\Gamma, E_2)$. We impose Hypothesis (4.2), which states that for $i = 1, 2$, the Selmer groups $\mathrm{Sel}^{\ddagger}(E_i/F^{\mathrm{cyc}})$ are cotorsion over the Iwasawa algebra, and that the truncated Euler characteristics $\chi_t^{\ddagger}(\Gamma, E_i)$ are well defined. At a prime v, $L_v(E_i, s)$ is the local L-function of E_i at v. We set δ_{E_i,Σ_1} to be the product of local-factors at the primes in Σ_1

$$\delta_{E_i,\Sigma_1} := \prod_{v\in\Sigma_1} |L_v(E_i, 1)|_p$$

(see Definition 5.2). Here, $|\cdot|_p$ is the absolute value normalized by $|p|_p^{-1} = p$. It is shown that there is an explicit relationship between $\delta_{E_1,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_1)$ and $\delta_{E_2,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_2)$, and the reader is referred to Theorem 5.5 for the precise statement. The set of primes Σ_1 can be smaller than the set Σ_0, and hence the relation between truncated Euler characteristics is more refined. This is why it is of considerable importance that the set of primes Σ_1 be carefully chosen to be as small as possible. Theorem 6.7 extends Theorem 5.5 to the multisigned Selmer groups of certain $\mathbb{Z}_p^m$-extensions. Furthermore, we compare the Akashi series for p-congruent elliptic curves over such $\mathbb{Z}_p^m$-extensions. Our results are informed by explicit examples which are listed in Section 7.

2 Preliminaries

Throughout, we fix an odd prime number p and number field F. Let F^{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of F. Denote by Σ_p the set of primes of F above p. Let E be an elliptic curve over F and denote by $\Sigma_{\mathrm{ss}}(E) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_d\}$ the set of primes in Σ_p at which E has supersingular reduction. Let $\mathcal{F}_\infty/F$ be a Galois extension of F containing F^{cyc} such that $\mathrm{Gal}(\mathcal{F}_\infty/F) \simeq \mathbb{Z}_p^m$ for an integer $m \geq 1$. Set $\mathrm{G} := \mathrm{Gal}(\mathcal{F}_\infty/F)$, $H := \mathrm{Gal}(\mathcal{F}_\infty/F^{\mathrm{cyc}})$ and let Γ be the Galois group $\mathrm{Gal}(F^{\mathrm{cyc}}/F)$, which is identified with G/H. Associated to any pro-p group $\mathcal{G}$, the Iwasawa algebra $\mathbb{Z}_p[[\mathcal{G}]]$ is the inverse limit $\varprojlim_U \mathbb{Z}_p[\mathcal{G}/U]$, where U ranges over all open normal subgroups of $\mathcal{G}$. Set $\mathcal{F}_0 := F$ and for $n \geq 1$, let $\mathcal{F}_n$ denote the unique subextension $F \subseteq \mathcal{F}_n \subset \mathcal{F}_\infty$ such that $\mathrm{Gal}(\mathcal{F}_n/F) \simeq (\mathbb{Z}/p^n\mathbb{Z})^m$. We introduce the following hypothesis on the elliptic curve E.

Hypothesis 2.1 *Throughout, E is required to satisfy the following hypotheses:*

(1) *E has semistable reduction at all primes $v \in \Sigma_p$ (i.e., either good ordinary, good supersingular or bad multiplicative reduction).*
(2) *The residual representation $E[p]$ is a 2-dimensional $\mathbb{F}_p$-vector space which is irreducible as a $\mathrm{Gal}(\overline{F}/F)$-module.*
(3) *For every prime $v \in \Sigma_{\mathrm{ss}}(E)$, the completion F_v is isomorphic to $\mathbb{Q}_p$.*
(4) *For $v \in \Sigma_{\mathrm{ss}}(E)$, set $a_v(E) := 1 + p - \#\widetilde{E}_v(\mathbb{F}_p)$, where $\widetilde{E}_v$ is the reduction of E at v. Assume that $a_v(E) = 0$ for all $v \in \Sigma_{\mathrm{ss}}(E)$.*

Note that for $v \in \Sigma_{\mathrm{ss}}(E)$, it follows from Hasse's theorem that $|a_v(E)| < 2\sqrt{p}$. Since E has supersingular reduction at v, we find that p divides $\#\widetilde{E}_v(\mathbb{F}_p)$. Therefore, condition (4) above is satisfied for all primes $p \geq 7$.

Lemma 2.1 *Let $\mathcal{F}_\infty$ a $\mathbb{Z}_p^m$-extension of F as above. The following conditions are satisfied:*

(1) *The only primes that ramify in $\mathcal{F}_\infty$ are the primes v of F above p.*
(2) *Let $\mathfrak{p}_i|p$ be a prime of F at which E has supersingular reduction. Let $n \geq 1$ and let η be a prime of $\mathcal{F}_n$ above $\mathfrak{p}_i$. Then, $\mathcal{F}_{n,\eta}$ is isomorphic to K_n for some finite unramified extension K of $\mathbb{Q}_p$. Here, K_n is the nth layer in the cyclotomic $\mathbb{Z}_p$-extension of K.*

Proof Note that in any $\mathbb{Z}_p$-extension of F, the only primes that ramify are the primes above p, see [36, Proposition 13.2]. Any $\mathbb{Z}_p^m$-extension is a composite of m independent $\mathbb{Z}_p$-extensions, part (1) follows.

Recall that it is assumed that $\mathcal{F}_\infty$ contains F^{cyc}. We identify $F_{\mathfrak{p}_i}$ with $\mathbb{Q}_p$. By local class field theory, the maximal pro-p extension of $\mathbb{Q}_p$ is the composite of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_p^{\mathrm{cyc}}$ and the unramified $\mathbb{Z}_p$-extension $\mathbb{Q}_p^{\mathrm{nr}}$. Letting $\mathbb{Q}_{p,n} \subset \mathbb{Q}_p^{\mathrm{cyc}}$ be the nth layer, we find that $\mathcal{F}_{n,\eta}$ is the composite of an unramified extension $K/\mathbb{Q}_p$ and $\mathbb{Q}_{p,n}$, and (2) follows. ∎

Part (2) of Lemma 2.1 ensures that the signed norm groups of E over $F_{n,\eta}$ may be defined. This is used in Definition 2.2, where the multisigned Selmer groups associated to E over $\mathcal{F}_\infty$ are defined. We shall now define local conditions at each of the primes $\mathfrak{p}_i \in \Sigma_{\mathrm{ss}}(E)$. By Hypothesis (2.1), the local field $F_{\mathfrak{p}_i}$ is isomorphic to $\mathbb{Q}_p$. Denote by $\widehat{E}_{\mathfrak{p}_i}$ the formal group of E over $F_{\mathfrak{p}_i}$. For any algebraic extension L of $F_{\mathfrak{p}_i} \simeq \mathbb{Q}_p$, denote by $\widehat{E}_{\mathfrak{p}_i}(L) := \widehat{E}_{\mathfrak{p}_i}(\mathfrak{m}_L)$, where $\mathfrak{m}_L$ is the maximal ideal of $\mathcal{O}_L$. Let K be a finite unramified extension of $\mathbb{Q}_p$ and K^{cyc} the cyclotomic $\mathbb{Z}_p$-extension of K. Denote by K_n the unique subextension of K^{cyc}/K of degree p^n. Kobayashi introduced plus and minus norm

https://doi.org/10.4153/S0008414X21000699 Published online by Cambridge University Press

groups:

$$\widehat{E}^{+}_{\mathfrak{p}_i}(K_n) := \left\{P \in \widehat{E}_{\mathfrak{p}_i}(K_n) \mid \mathrm{tr}_{n/m+1}(P) \in \widehat{E}_{\mathfrak{p}_i}(K_m), \text{ for } 0 \le m < n \text{ and } m \text{ even}\right\},$$

$$\widehat{E}^{-}_{\mathfrak{p}_i}(K_n) := \left\{P \in \widehat{E}_{\mathfrak{p}_i}(K_n) \mid \mathrm{tr}_{n/m+1}(P) \in \widehat{E}_{\mathfrak{p}_i}(K_m), \text{ for } 0 \le m < n \text{ and } m \text{ odd}\right\},$$

where $\mathrm{tr}_{n/m+1} : \widehat{E}_{\mathfrak{p}_i}(K_n) \to \widehat{E}_{\mathfrak{p}_i}(K_{m+1})$ denotes the trace map with respect to the formal group law on $\widehat{E}_{\mathfrak{p}_i}$.

Let $\ddagger = (\ddagger_1, \dots, \ddagger_d) \in \{+,-\}^d$ be a multisigned vector, so that each component $\ddagger_i$ is either a + or − sign. For each finite prime $v \notin \Sigma_{ss}(E)$, and each integer $n \ge 1$, set

$$\mathcal{H}_v(\mathcal{F}_n, E[p^\infty]) := \prod_{\eta | v} \frac{H^1(\mathcal{F}_{n,\eta}, E[p^\infty])}{E(\mathcal{F}_{n,\eta}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}, \tag{2.1}$$

where η runs through the primes of $\mathcal{F}_n$ above v. For each prime $\mathfrak{p}_i \in \Sigma_{ss}(E)$, set

$$\mathcal{H}^{\pm}_{\mathfrak{p}_i}(\mathcal{F}_n, E[p^\infty]) := \prod_{\eta | \mathfrak{p}_i} \frac{H^1(\mathcal{F}_{n,\eta}, E[p^\infty])}{\widehat{E}^{\pm}_{\mathfrak{p}_i}(\mathcal{F}_{n,\eta}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}. \tag{2.2}$$

Let η be a prime of $\mathcal{F}_\infty$ above $\mathfrak{p}_i$. By (2) of Lemma 2.1, $\mathcal{F}_{n,\eta}$ is isomorphic to K_n for some finite unramified extension K over $\mathbb{Q}_p$. Thus the norm groups $\widehat{E}^{\pm}_{\mathfrak{p}_i}(\mathcal{F}_{n,\eta})$ are defined. We now come to the definition of the multisigned Selmer groups.

Definition 2.2 Let d be the cardinality of $\Sigma_{ss}(E)$ and let $\ddagger = (\ddagger_1, \dots, \ddagger_d)$ be a multisigned vector, so that each component $\ddagger_i$ is either a + sign or − sign. Let Σ be a finite primes of F containing Σ_p and the primes at which E has bad reduction. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_d$ be the primes in $\Sigma_{ss}(E)$. For $i = 1, \dots, d$, let $\mathcal{H}^{\ddagger_i}_{\mathfrak{p}_i}(\mathcal{F}_n, E[p^\infty])$ be the group defined above, see (2.2). The multisigned Selmer group $\mathrm{Sel}^{\ddagger}(E/\mathcal{F}_n)$ is the kernel of the map:

$$\Phi^{\ddagger}_{E,\mathcal{F}_n} : H^1(\mathcal{F}_n, E[p^\infty]) \to \prod_{v \in \Sigma \setminus \Sigma_{ss}(E)} \mathcal{H}_v(\mathcal{F}_n, E[p^\infty]) \times \prod_{i=1}^{d} \mathcal{H}^{\ddagger_i}_{\mathfrak{p}_i}(\mathcal{F}_n, E[p^\infty]).$$

Let $\mathrm{Sel}^{\ddagger}(E/\mathcal{F}_\infty)$ be the direct limit $\varinjlim_n \mathrm{Sel}^{\ddagger}(E/\mathcal{F}_n)$ and write $\mathrm{X}^{\ddagger}(E/\mathcal{F}_\infty)$ for its Pontryagin-dual.

For practical purposes, it is convenient to work with an alternative description of $\mathrm{Sel}^{\ddagger}(E/F^{\mathrm{cyc}})$. For $v \in \Sigma_p \setminus \Sigma_{ss}(E)$ denote by E_v the curve over the local field F_v. Since E_v has good ordinary or multiplicative reduction, it fits in a short exact sequence of $\mathrm{Gal}(\overline{F_v}/F_v)$-modules:

$$0 \to C_v \to E_v[p^\infty] \to D_v \to 0. \tag{2.3}$$

Here, C_v and D_v are both of corank one over $\mathbb{Z}_p$ with the property that C_v is a divisible subgroup and D_v is the maximal subgroup on which $\mathrm{I}_v := \mathrm{Gal}(\overline{F_v}/F_v^{\mathrm{nr}})$ acts via a finite order quotient. In fact, D_v is specified as follows:

$$D_v = \begin{cases} \widetilde{E}_v[p^\infty] & \text{if } E_v \text{ has good ordinary reduction,} \\ \mathbb{Q}_p/\mathbb{Z}_p(\phi) & \text{if } E_v \text{ has multiplicative reduction,} \end{cases} \tag{2.4}$$

https://doi.org/10.4153/S0008414X21000699 Published online by Cambridge University Press

where ϕ is an unramified quadratic character, which is trivial if and only if E_v has split multiplicative reduction. For further details, the reader is referred to the discussions in [2, p. 150] and [8, section 2].

Note that above each prime v of F, there are finitely many primes $\eta | v$ of F^{cyc}. For $\mathfrak{p}_i \in \Sigma_{\text{ss}}(E)$, set

$$\mathcal{H}^{\pm}_{\mathfrak{p}_i}(F^{\text{cyc}}, E[p^\infty]) := \prod_{\eta | \mathfrak{p}_i} \frac{H^1(F^{\text{cyc}}_\eta, E[p^\infty])}{\widehat{E}^{\pm}(F^{\text{cyc}}_\eta) \otimes \mathbb{Q}_p/\mathbb{Z}_p},$$

where η runs through the primes of F^{cyc} above $\mathfrak{p}_i$. For $v \in \Sigma \backslash \Sigma_{\text{ss}}(E)$, set

(2.5)

$$\mathcal{H}_v(F^{\text{cyc}}, E[p^\infty]) := \begin{cases} \prod_{\eta | v} \operatorname{im}\left(H^1(F^{\text{cyc}}_\eta, E[p^\infty]) \to H^1(\mathrm{I}_\eta, D_v)\right) & \text{if } v \in \Sigma_p \backslash \Sigma_{\text{ss}}(E), \\ \prod_{\eta | v} H^1(F^{\text{cyc}}_\eta, E[p^\infty]) & \text{if } v \in \Sigma \backslash \Sigma_p, \end{cases}$$

where I_η is the inertia subgroup of $\operatorname{Gal}(\overline{F^{\text{cyc}}_\eta}/F^{\text{cyc}}_\eta)$. The Selmer group $\operatorname{Sel}^{\ddagger}(E/F^{\text{cyc}})$ coincides with the kernel of the restriction map

$$\Phi^{\ddagger}_{E,F^{\text{cyc}}} : H^1(F^{\text{cyc}}, E[p^\infty]) \to \prod_{v \in \Sigma \backslash \Sigma_{\text{ss}}(E)} \mathcal{H}_v(F^{\text{cyc}}, E[p^\infty]) \times \prod_{i=1}^{d} \mathcal{H}^{\ddagger_i}_{\mathfrak{p}_i}(F^{\text{cyc}}, E[p^\infty]).$$

For further details, see [8, pp. 32, 42] and the discussion in [6, Section 5]. Let Σ_0 be a finite set of primes of F which does not contain any prime $v \in \Sigma_p$. The Σ_0-imprimitive Selmer group $\operatorname{Sel}^{\Sigma_0,\ddagger}(E/F^{\text{cyc}})$ is the kernel of the restriction map

$$\Phi^{\Sigma_0,\ddagger}_{E,F^{\text{cyc}}} : H^1(F^{\text{cyc}}, E[p^\infty]) \to \prod_{v \in \Sigma \backslash (\Sigma_{\text{ss}}(E) \cup \Sigma_0)} \mathcal{H}_v(F^{\text{cyc}}, E[p^\infty]) \times \prod_{i=1}^{d} \mathcal{H}^{\ddagger_i}_{\mathfrak{p}_i}(F^{\text{cyc}}, E[p^\infty]).$$

The Pontryagin dual of $\operatorname{Sel}^{\Sigma_0,\ddagger}(E/F^{\text{cyc}})$ is denoted by $\mathrm{X}^{\Sigma_0,\ddagger}(E/F^{\text{cyc}})$. The next Proposition follows from [8, Proposition 2.1] and [21, Proposition 4.6].

Proposition 2.3 *Assume that the Selmer group $\operatorname{Sel}^{\Sigma_0,\ddagger}(E/F^{\text{cyc}})$ is cotorsion as a $\mathbb{Z}_p[[\Gamma]]$-module. Then, the maps $\Phi^{\ddagger}_{E,F^{\text{cyc}}}$ and $\Phi^{\Sigma_0,\ddagger}_{E,F^{\text{cyc}}}$ are surjective.*

Thus we have a short exact sequence relating the Σ_0-imprimitive Selmer group $\operatorname{Sel}^{\Sigma_0,\ddagger}(E/F^{\text{cyc}})$ with the Selmer group $\operatorname{Sel}^{\ddagger}(E/F^{\text{cyc}})$

$$0 \to \operatorname{Sel}^{\ddagger}(E/F^{\text{cyc}}) \to \operatorname{Sel}^{\Sigma_0,\ddagger}(E/F^{\text{cyc}}) \xrightarrow{\Phi^{\ddagger,\Sigma_0}_{E,F^{\text{cyc}}}} \prod_{v \in \Sigma_0} \mathcal{H}_v(F^{\text{cyc}}, E[p^\infty]) \to 0.$$

Choose a topological generator γ of Γ and identify $\gamma - 1$ with T in choosing an isomorphism $\mathbb{Z}_p[[\Gamma]] \simeq \mathbb{Z}_p[[T]]$. A polynomial $f(T) \in \mathbb{Z}_p[T]$ is said to be *distinguished* if it is a monic polynomial and all nonleading coefficients are divisible by p. By the structure theorem of finitely generated torsion $\mathbb{Z}_p[[T]]$-modules, there is a pseudo-isomorphism

$$\mathrm{X}^{\ddagger}(E/F^{cyc}) \sim \left(\bigoplus_{i=1}^{n} \mathbb{Z}_p[[T]]/(f_i(T))\right) \oplus \left(\bigoplus_{j=1}^{m} \mathbb{Z}_p[[T]]/(p^{\mu_j})\right).$$

For, $i = 1, \dots, n$, the elements $f_i(T)$ above are distinguished polynomials and the product $f_E^{\ddagger}(T) := p^{\sum_j \mu_j} \prod_i f_i(T)$ is called the *characteristic polynomial*. The signed Iwasawa invariants are defined by $\lambda_E^{\ddagger} := \deg f_E^{\ddagger}(T)$ and $\mu_E^{\ddagger} := \sum_{j=1}^m \mu_j$. Denote by $f_E^{\Sigma_0,\ddagger}(T)$, $\lambda_E^{\Sigma_0,\ddagger}$ and $\mu_E^{\Sigma_0,\ddagger}$ the characteristic polynomial, λ-invariant and μ-invariant of the imprimitive Selmer group $\mathrm{X}^{\Sigma_0,\ddagger}(E/F^{\mathrm{cyc}})$.

3 The truncated Euler characteristic

In this section, we recall the notion of the truncated Euler characteristic, which is a generalization of the usual Euler characteristic. We then discuss explicit formulas for the truncated Euler characteristic, as predicted by the p-adic Birch and Swinnerton-Dyer conjecture. For a more detailed exposition, the reader may refer to [3, Section 3] and [37]. For a discrete p-primary cofinitely generated $\mathbb{Z}_p[[\Gamma]]$-module M for which the cohomology groups $H^i(\Gamma, M)$ have finite order, the Euler characteristic is defined to be the quotient

$$\chi(\Gamma, M) := \frac{\# H^0(\Gamma, M)}{\# H^1(\Gamma, M)}.$$

For an elliptic curve E with potentially good ordinary reduction at all primes above p, the Euler characteristic of the Selmer group is defined, provided the Selmer group of E over the base field is finite. This definition does not extend to the case when the Selmer group of E is infinite. The natural substitute is the *truncated Euler characteristic*.

Definition 3.1 Let M be a discrete p-primary Γ-module let ϕ_M be the natural map

$$\phi_M : H^0(\Gamma, M) = M^{\Gamma} \to M_{\Gamma} \simeq H^1(\Gamma, M)$$

for which $\phi_M(x)$ is the residue class of x in M_Γ. The truncated Euler characteristic $\chi_t(\Gamma, M)$ is defined if both $\ker(\phi_M)$ and $\operatorname{cok}(\phi_M)$ are finite. In this case, $\chi_t(\Gamma, M)$ is defined by

$$\chi_t(\Gamma, M) := \frac{\# \ker(\phi_M)}{\# \operatorname{cok}(\phi_M)}.$$

For a discrete $\mathbb{Z}_p[[\Gamma]]$-module M, set $f_M(T)$ to be the characteristic polynomial of the Pontryagin dual of M and write $f_M(T) = T^{r_M} g_M(T)$, where $g_M(0) \neq 0$. In other words, r_M is the order of vanishing of $f_M(T)$ at $T = 0$.

Lemma 3.2 *Assume that M is cofinitely generated and cotorsion as a $\mathbb{Z}_p[[\Gamma]]$-module. The Euler characteristic $\chi(\Gamma, M)$ is defined if and only if $r_M = 0$.*

Proof Let X be the Pontryagin dual of M. The invariant submodule M^Γ is dual to X_Γ and the quotient M_Γ is dual to X^Γ. By an application of the structure theorem for finitely generated torsion $\mathbb{Z}_p[[\Gamma]]$-modules, there is a pseudoisomorphism

$$X \sim \bigoplus_{i=1}^{m} \mathbb{Z}_p[[T]]/(f_i(T))$$

for some elements $f_i(T) \in \mathbb{Z}_p[[\Gamma]]$. The module X_Γ may be identified with X/TX and X^Γ is the kernel of the multiplication by T map $\times T : X \to X$. It is easy to see that the

https://doi.org/10.4153/S0008414X21000699 Published online by Cambridge University Press

groups X_Γ and X^Γ are finite precisely when $T \nmid f_i(T)$ for $i = 1, \dots, m$. Therefore, X_Γ and X^Γ are finite precisely when $r_M = 0$. ∎

The following lemma is a criterion for the truncated Euler characteristic to be well defined.

Lemma 3.3 *Assume that M is a p-primary, discrete $\mathbb{Z}_p[[\Gamma]]$-module. Let X be the Pontryagin dual of M. Assume that X is a finitely generated torsion $\mathbb{Z}_p[[\Gamma]]$-module. Denote by $X[p^\infty]$ the p^∞-torsion submodule of X. Let $f_1(T), \dots, f_n(T)$ be distinguished polynomials such that $X/X[p^\infty]$ is pseudo-isomorphic to $\bigoplus_{i=1}^n \mathbb{Z}_p[[T]]/(f_i(T))$. Suppose that none of the polynomials $f_i(T)$ is divisible by T^2. Then, the kernel and cokernel of ϕ_M are finite and the truncated Euler characteristic $\chi_t(\Gamma, M)$ is defined. In particular, the truncated Euler characteristic $\chi_t(\Gamma, M)$ is defined when $r_M \leq 1$.*

Proof The assertion of the lemma follows from the proof of [37, Lemma 2.11]. ∎

Let $|\cdot|_p$ denote the absolute value on $\mathbb{Q}_p$ normalized by $|p|_p = p^{-1}$. When both $\ker(\phi_M)$ and $\operatorname{cok}(\phi_M)$ are finite, the truncated Euler characteristic $\chi_t(\Gamma, M)$ is related to the quantity $|g_M(0)|_p$.

Lemma 3.4 *Let M be a discrete $\mathbb{Z}_p[[\Gamma]]$ module which is cofinitely generated and cotorsion. If the kernel and cokernel of ϕ_M are finite, then*

$$\chi_t(\Gamma, M) = |g_M(0)|_p^{-1},$$

and further, $r_M = \operatorname{cork}_{\mathbb{Z}_p} M^\Gamma = \operatorname{cork}_{\mathbb{Z}_p} M_\Gamma$.

Proof The assertion follows from [37, Lemma 2.11]. ∎

Evidently, it follows that $\chi_t(\Gamma, M) = p^N$, where $N \in \mathbb{Z}_{\geq 0}$. Let μ_M (resp. λ_M) denote its μ-invariant (resp. λ-invariant) of $M^\vee$ as a $\mathbb{Z}_p[[\Gamma]]$-module.

Lemma 3.5 *Let M be a cofinitely generated cotorsion $\mathbb{Z}_p[[\Gamma]]$-module such that $\phi_M : M^\Gamma \to M_\Gamma$ has finite kernel and cokernel. Then, the following are equivalent:*

(a) $\chi_t(\Gamma, M) = 1$ *and*
(b) $\mu_M = 0$ *and* $\lambda_M = r_M$.

Proof Suppose that $\chi_t(\Gamma, M) = 1$. Recall that $g_M(T)$ is a polynomial such that $f_M(T) = T^{r_M} g_M(T)$ and $T \nmid g_M(T)$. By Lemma 3.4,

$$|g_M(0)|_p^{-1} = \chi_t(\Gamma, M) = 1.$$

As a result, $f_M(T)$ and $g_M(T)$ are distinguished polynomials. Since $g_M(0)$ is a unit, it follows that $g_M(T)$ is a unit. Since $g_M(T)$ is a distinguished polynomial, it follows that

$$g_M(T) = 1 \text{ and } f_M(T) = T^{r_M}.$$

As a result, $\mu_M = 1$ and $\lambda_M = \deg f_M(T) = r_M$.

Conversely, suppose that $\mu_M = 0$ and $\lambda_M = r_M$. Since $\mu_M = 0$, it follows that $f_M(T)$ and $g_M(T)$ are distinguished polynomials. The degree of $f_M(T)$ is $\lambda_M = r_M$, it follows

https://doi.org/10.4153/S0008414X21000699 Published online by Cambridge University Press

that $g_M(T)$ is a constant polynomial and hence, $g_M(T) = 1$. By Lemma 3.4,

$$\chi_t(\Gamma, M) = |g_M(0)|_p^{-1} = 1. \qquad \blacksquare$$

Let $r_E^\ddagger$ denote the order of vanishing of $f_E^\ddagger(T)$ at $T = 0$, and write

$$f_E^\ddagger(T) = p^{r_E^\ddagger} g_E^\ddagger(T).$$

Note that $g_E^\ddagger(0) \neq 0$. According to Lemma 3.4, the truncated Euler characteristic $\chi_t^\ddagger(\Gamma, E) := \chi_t(\Gamma, \mathrm{Sel}^\ddagger(E/F^{\mathrm{cyc}}))$ is determined by the constant term of $g_E^\ddagger(T)$. By Lemma 3.5, if the truncated Euler characteristic is defined (in the sense of Definition 3.1), then $\chi_t^\ddagger(\Gamma, E) = 1$ if and only if $\mu_E^\ddagger = 0$ and $\lambda_E^\ddagger = r_E^\ddagger$.

We next discuss the p-adic Birch and Swinnerton-Dyer conjecture and its relationship with explicit formulas for truncated Euler characteristics. Note that there are formulations of the p-adic Birch and Swinnerton-Dyer conjecture in very general contexts (see for instance [31, p. 6]). For ease of exposition, we restrict ourselves to the case where the elliptic curves E are defined over $\mathbb{Q}$. For elliptic curves with good ordinary or multiplicative reduction, the p-adic Birch and Swinnerton-Dyer conjecture in its current form was formulated by Mazur et al. [24, p. 38]. This is a p-adic analog of the classical Birch and Swinnerton-Dyer conjecture which predicts the order of vanishing of the Mazur and Swinnerton-Dyer p-adic L-function $\mathcal{L}(E/\mathbb{Q}, T)$ at $T = 0$, and postulates an explicit formula for the leading term (see also [1]). When E has good supersingular reduction at p, a version of the p-adic Birch and Swinnerton-Dyer conjecture for signed p-adic L-functions was formulated by Sprung [35]. The conjecture of *loc. cit.* is equivalent to that of Bernardi and Perrin-Riou [1]. Lemma 3.4 asserts that the truncated Euler-characteristic is related to the leading coefficient of the characteristic element of the Selmer group. The main conjecture and the p-adic Birch and Swinnerton-Dyer conjecture together predict precise formulas for the truncated Euler characteristic.

Assume that E has either good ordinary or multiplicative reduction at p. When E has split multiplicative reduction at p, set $\mathcal{L}_p(E)$ to denote the $\mathcal{L}$-invariant associated to the Galois representation on the p-adic Tate module of E (see [8, p. 407]). The p-adic height pairing (cf. [32] and [33]) is a p-adic analog of the usual height pairing. This pairing is conjectured to be non-degenerate (cf. [33]) and the p-adic regulator $R_p(E/\mathbb{Q})$ is defined to be the determinant of this pairing. Let κ denote the p-adic cyclotomic character. Fix a branch of the p-adic logarithm and set $\mathcal{R}_\gamma(E/\mathbb{Q})$ to denote the normalized height pairing $(\log_p \kappa(\gamma))^{-r} R_p(E/\mathbb{Q})$, where r denotes the rank of the Mordell Weil group $E(\mathbb{Q})$. Let $E_0(\mathbb{Q}_l) \subset E(\mathbb{Q}_l)$ be the subgroup of l-adic points with nonsingular reduction modulo l. Denote by $\tau(E)$ the Tamagawa product $\prod_l c_l$, where c_l is the index of $E_0(\mathbb{Q}_l)$ in $E(\mathbb{Q}_l)$. Let $a_l(E)$ be the lth coefficient of the normalized eigenform associated to E. For p-adic numbers a and b, write $a \sim b$ if $a = ub$ for a p-adic unit u. Let r' be the order of vanishing at $T = 0$ of the characteristic element of the Selmer group $\mathrm{Sel}(E/\mathbb{Q}_{\mathrm{cyc}})$. The following result does *not* assume the main conjecture.

Theorem 3.6 (Perrin-Riou [27], Schneider [33], Jones [11]) *Suppose that E has either good ordinary reduction or multiplicative reduction at p. Assume that*

(1) *the p-adic regulator $R_p(E/\mathbb{Q})$ is non-zero and*
(2) *$Ш(E/\mathbb{Q})[p^\infty]$ has finite cardinality.*

Then, the following assertions are true:

(a) *If E has either good ordinary reduction or non-split multiplicative reduction at p, then $r' = r$. If E has split multiplicative reduction at p, then $r' = r + 1$.*

(b) *Assume further that the truncated Euler-characteristic $\chi_t(\Gamma, E)$ is defined (in the sense of Definition 3.1). If E has either good ordinary reduction at p or nonsplit multiplicative reduction at p, then*

$$\chi_t(\Gamma, E) \sim \varepsilon_p(E) \times \frac{\mathcal{R}_\gamma(E/\mathbb{Q}) \times \#(\text{Ш}(E/\mathbb{Q})[p^\infty]) \times \tau(E)}{\#(E(\mathbb{Q})_{\text{tors}})^2}.$$

Here, $\varepsilon_p(E)$ is set to be $(1 - \frac{1}{\alpha})^s$, where α is the unit root of the Hecke polynomial $X^2 - a_p(E)X + p$ and

$$s = \begin{cases} s = 2 & \text{if } E \text{ has good ordinary reduction at } p, \\ s = 1 & \text{if } E \text{ has non-split multiplicative reduction at } p. \end{cases}$$

(c) *If E has split-multiplicative reduction, the $\mathcal{L}$-invariant $\mathcal{L}_p(E)$ plays a role and we have*

$$\chi_t(\Gamma, E) \sim \frac{\mathcal{L}_p(E)}{\log_p(\kappa(\gamma))} \times \frac{\mathcal{R}_\gamma(E/\mathbb{Q}) \times \#(\text{Ш}(E/\mathbb{Q})[p^\infty]) \times \tau(E)}{\#(E(\mathbb{Q})_{\text{tors}})^2}.$$

4 Iwasawa invariants of congruent elliptic curves

In this section, we show that the *imprimitive* Iwasawa-invariants associated to congruent elliptic curves satisfy certain relations. Throughout, E is an elliptic curve over F which satisfies Hypothesis (2.1). Denote by $T_p(E) := \varprojlim_n E[p^n]$ the p-adic Tate-module equipped with natural $\text{Gal}(\overline{F}/F)$ action and set $V_p(E) := T_p(E) \otimes \mathbb{Q}_p$. At a prime $v \in \Sigma_p \backslash \Sigma_{\text{ss}}(E)$, recall that there are corank one $\mathbb{Z}_p$-modules which fit into a short exact sequence

$$0 \to C_v \to E_v[p^\infty] \to D_v \to 0.$$

When E has good ordinary reduction at v, the quotient D_v may be identified with $\widetilde{E}_v[p^\infty]$, where $\widetilde{E}_v$ is the reduction of E at v. On the other hand, when E has multiplicative reduction at v, identify D_v with a twist of $\mathbb{Q}_p/\mathbb{Z}_p$ by an unramified quadratic character.

Hypothesis 4.1 *Let E be an elliptic curve over F which satisfies Hypothesis (2.1). Let $\Sigma_{\text{ss}}(E) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_d\}$ be the set of primes $v|p$ of F at which E has supersingular reduction. Let $\ddagger \in \{+, -\}^d$ be a signed vector. Then $(E, \ddagger)$ satisfies the following conditions:*

(1) *The Selmer group $\text{Sel}^\ddagger(E/F^{\text{cyc}})$ is $\mathbb{Z}_p[[\Gamma]]$-cotorsion.*

(2) *The truncated Euler characteristic $\chi_t^\ddagger(\Gamma, E)$ is defined. In other words, the natural map*

$$\phi_E^\ddagger : \text{Sel}^\ddagger(E/F^{\text{cyc}})^\Gamma \to \text{Sel}^\ddagger(E/F^{\text{cyc}})_\Gamma$$

has finite kernel and cokernel.

https://doi.org/10.4153/S0008414X21000699 Published online by Cambridge University Press

Let E_1 and E_2 be p-congruent elliptic curves over F. It follows from the proof of [25, Proposition 3.9] that $\Sigma_{ss}(E_1)$ is equal to $\Sigma_{ss}(E_2)$. Set $\Sigma_{ss} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_d\}$ to denote the set of supersingular primes $v|p$ of E_1 and E_2, and let $\ddagger \in \{+,-\}^d$ be a signed vector. We introduce the following hypothesis on the triple $(E_1, E_2, \ddagger)$.

Hypothesis 4.2 *Hypothesis (4.1) holds for both $(E_1, \ddagger)$ and $(E_2, \ddagger)$.*

We now define the imprimitive Selmer group associated to the residual Galois representation $E_i[p]$. Let Σ be a set of finite primes of F containing Σ_p and the primes at which E_1 or E_2 has bad reduction. For a prime $v \in \Sigma_p$ let η_v be the unique prime of F^{cyc} above v. Let I_{η_v} be the inertia subgroup of $\mathrm{Gal}(\overline{F^{\mathrm{cyc}}_{\eta_v}}/F^{\mathrm{cyc}}_{\eta_v})$. For a prime $v \in \Sigma_{ss}$, and $i = 1, 2$, define

$$\mathcal{H}_v^{\pm}(F^{\mathrm{cyc}}, E_i[p]) := \frac{H^1(F^{\mathrm{cyc}}_{\eta_v}, E_i[p])}{\widehat{E}_i^{\pm}(F^{\mathrm{cyc}}_{\eta_v})/p\widehat{E}_i^{\pm}(F^{\mathrm{cyc}}_{\eta_v})}.$$

For $v \in \Sigma \backslash \Sigma_{ss}$, set

$$\mathcal{H}_v(F^{\mathrm{cyc}}, E_i[p]) := \begin{cases} \prod_{\eta|v} H^1(F^{\mathrm{cyc}}_\eta, E_i[p]) & \text{if } v \in \Sigma\backslash\Sigma_p, \\ H^1(\mathrm{I}_{\eta_v}, D_v(E_i)[p]) & \text{if } v \in \Sigma_p \backslash \Sigma_{ss}. \end{cases}$$

For an elliptic curve E over F, denote by $\mathcal{N}_E$ the conductor of E and $\overline{\mathcal{N}}_E$ the prime to p part of the Artin conductor of the residual representation $E[p]$. Let $v \nmid p$ be a finite prime of F. Note that v divides $\mathcal{N}_E$ (resp. $\overline{\mathcal{N}}_E$) is and only if it is a bad reduction prime of E (resp. the residual Galois representation $E[p]$ is ramified at v). To ease notation, let $\mathcal{N}_1$ and $\mathcal{N}_2$ denote the conductors of E_1 and E_2, respectively. Denote by $\overline{\mathcal{N}}$ the prime to p part of the Artin conductor of $E_1[p]$. Note that since $E_1[p]$ is isomorphic to $E_2[p]$, $\overline{\mathcal{N}}$ is the conductor of $E_2[p]$.

Definition 4.1 Let E be an elliptic curve over F. If $p \geq 5$, let $\Sigma_1(E)$ denote the subset of primes of F such that (i) $v \nmid p$, (ii) $v|(\mathcal{N}_E/\overline{\mathcal{N}}_E)$, and (iii) if μ_p is contained in F_v, then E has split multiplicative reduction at v. In the case $p = 3$, set $\Sigma_1(E)$ to be the set of primes of F such that (i) $v \nmid p$, (ii) $v|(\mathcal{N}_E/\overline{\mathcal{N}}_E)$.

The Σ_1-imprimitive mod-p Selmer group $\mathrm{Sel}^{\Sigma_1,\ddagger}(E_i[p]/F^{\mathrm{cyc}})$ is defined to be the kernel of the restriction map:

$$\overline{\Phi}^{\Sigma_1,\ddagger}_{E_i} : H^1(F_\Sigma/F^{\mathrm{cyc}}, E_i[p]) \to \prod_{\Sigma/(\Sigma_{ss}\cup\Sigma_1)} \mathcal{H}_v(F^{\mathrm{cyc}}, E_i[p]) \times \prod_{j=1}^{d} \mathcal{H}^{\ddagger_j}_{\mathfrak{p}_j}(F^{\mathrm{cyc}}, E_i[p]).$$

Proposition 4.2 *Let E_1 and E_2 be elliptic curves over F which are p-congruent. Let $\ddagger$ be a signed vector and assume that $(E_1, E_2, \ddagger)$ satisfies Hypothesis (4.2). Let Σ_1 be the set of primes as in Definition 4.1. Then the isomorphism $E_1[p] \simeq E_2[p]$ induces an isomorphism of Selmer groups $\mathrm{Sel}^{\Sigma_1,\ddagger}(E_1[p]/F^{\mathrm{cyc}}) \simeq \mathrm{Sel}^{\Sigma_1,\ddagger}(E_2[p]/F^{\mathrm{cyc}})$.*

Proof Let $\Phi : E_1[p] \xrightarrow{\sim} E_2[p]$ be a choice of isomorphism of Galois modules. Clearly, Φ induces an isomorphism $H^1(F_\Sigma/F^{\mathrm{cyc}}, E_1[p]) \xrightarrow{\sim} H^1(F_\Sigma/F^{\mathrm{cyc}}, E_2[p])$. It suffices to show that for $v \in \Sigma$, the isomorphism $\Phi : E_1[p] \xrightarrow{\sim} E_2[p]$ induces an

https://doi.org/10.4153/S0008414X21000699 Published online by Cambridge University Press

isomorphism

$$\mathcal{H}_v(F^{\mathrm{cyc}}, E_1[p]) \xrightarrow{\sim} \mathcal{H}_v(F^{\mathrm{cyc}}, E_2[p]).$$

This is clear for $v \in \Sigma \backslash \Sigma_{\mathrm{ss}}$. For $v \in \Sigma_{\mathrm{ss}}$, this assertion follows from the arguments in [13, p. 186]. ∎

Proposition 4.3 *Let E be an elliptic curve over F satisfying Hypothesis (2.1) and $\ddagger$ a signed vector. Let Σ_0 be a finite set of primes $v \nmid p$ containing $\Sigma_1(E)$. Then, there is an isomorphism*

$$\mathrm{Sel}^{\Sigma_0,\ddagger}(E/F^{\mathrm{cyc}})[p] \simeq \mathrm{Sel}^{\Sigma_0,\ddagger}(E[p]/F^{\mathrm{cyc}}).$$

Proof Let Σ be a finite set of primes containing Σ_0, the primes at which E has bad reduction and Σ_p. We consider the diagram relating the two Selmer groups:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}^{\Sigma_0,\ddagger}(E[p]/F^{\mathrm{cyc}}) \arrow[r] \arrow[d, "f"] & H^1(\mathrm{G}_\Sigma(F^{\mathrm{cyc}}), E[p]) \arrow[r] \arrow[d, "g"] & \mathrm{im}\, \overline{\Phi}_E^{\Sigma_0,\ddagger} \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & \mathrm{Sel}^{\Sigma_0,\ddagger}(E/F^{\mathrm{cyc}})[p] \arrow[r] & H^1(\mathrm{G}_\Sigma(F^{\mathrm{cyc}}), E[p^\infty])[p] \arrow[r] & \mathrm{im}\, \Phi_E^{\Sigma_0,\ddagger}[p] \arrow[r] & 0.
\end{tikzcd}$$

Since Γ is pro-p and $E[p]$ is an irreducible Galois module, clearly

$$H^0(F, E[p]) = H^0(F^{\mathrm{cyc}}, E[p])^\Gamma = 0.$$

Hence, we deduce that $H^0(F^{\mathrm{cyc}}, E[p^\infty]) = 0$ and have shown that g is an isomorphism.

It only remains to show that h is injective. For $v \in \Sigma/(\Sigma_{\mathrm{ss}}(E) \cup \Sigma_0)$ denote by h_v the natural map

$$h_v : \mathcal{H}_v(F^{\mathrm{cyc}}, E[p]) \to \mathcal{H}_v(F^{\mathrm{cyc}}, E[p^\infty])$$

and for $v \in \Sigma_{\mathrm{ss}}(E)$,

$$h_v : \mathcal{H}_v^{\dagger_v}(F^{\mathrm{cyc}}, E[p]) \to \mathcal{H}_v^{\dagger_v}(F^{\mathrm{cyc}}, E[p^\infty]).$$

We show that the maps h_v are injective for $v \in \Sigma \backslash \Sigma_0$. This has been shown in the proof of [8, Proposition 2.8] for $v \in \Sigma_p \backslash \Sigma_{\mathrm{ss}}$ and in [13, Proposition 2.10] for $v \in \Sigma_{\mathrm{ss}}$. Therefore, it remains to consider primes $v \in \Sigma \backslash (\Sigma_0 \cup \Sigma_p)$.

First consider the case when $p \geq 5$. Recall that $\Sigma_1(E)$ consists of primes of F such that (i) $v \nmid p$, (ii) $v | (\mathcal{N}_E/\overline{\mathcal{N}}_E)$, and (iii) if μ_p is contained in F_v, then E has split multiplicative reduction at v. Since $v \notin \Sigma_0$, one of the above conditions is not satisfied. Since $v \notin \Sigma_p$, (i) is satisfied. Hence, there are two cases to consider:

(1) (ii) is not satisfied and
(2) (ii) is satisfied, but (iii) is not.

First consider the case when (ii) is not satisfied, i.e., $v \nmid (\mathcal{N}_E/\overline{\mathcal{N}}_E)$. In this case, the injectivity of h_v follows from the proof of [5, Lemma 4.1.2] . Next, consider the case when (ii) is satisfied, but (iii) is not. Since (ii) is satisfied, $v \mid \mathcal{N}_E$, hence, E has bad reduction at v. Since (iii) is not satisfied, it follows that μ_p is contained in F_v and E has either non-split multiplicative reduction or additive reduction at v. In this case,

https://doi.org/10.4153/S0008414X21000699 Published online by Cambridge University Press

the injectivity of h_v follows from [9, Proposition 5.1]. When $p = 3$, the injectivity of h_v follows from the same reasoning as above. ∎

Proposition 4.4 *Let E be an elliptic curve over a number field F and Σ_0 any finite set of primes $v \nmid p$. Assume that:* (i) $E(F)[p] = 0$, (ii) $\mathrm{Sel}^{\Sigma_0,\ddagger}(E/F^{\mathrm{cyc}})$ *is cotorsion as a $\mathbb{Z}_p[[\Gamma]]$-module. Then the Selmer group $\mathrm{Sel}^{\Sigma_0,\ddagger}(E/F^{\mathrm{cyc}})$ contains no proper finite index $\mathbb{Z}_p[[\Gamma]]$-submodules.*

Proof We adapt the proof of [7, Proposition 4.14], which is due to Greenberg. Let Σ be a finite set of primes containing $\Sigma_0 \cup \Sigma_p$ and the primes of E at which E has bad reduction. Consider the $\Sigma_0 \cup \Sigma_p$-strict and relaxed Selmer groups:

$$\mathrm{Sel}^{\mathrm{rel}}(E/F^{\mathrm{cyc}}) := \ker\left\{H^1(F_\Sigma/F^{\mathrm{cyc}}, E[p^\infty]) \to \prod_{v\in\Sigma\setminus(\Sigma_0\cup\Sigma_p)} \mathcal{H}_v(F^{\mathrm{cyc}}, E[p^\infty])\right\},$$

$$\mathrm{Sel}^{\mathrm{str}}(E/F^{\mathrm{cyc}}) := \ker\left\{\mathrm{Sel}^{\mathrm{rel}}(E/F^{\mathrm{cyc}}) \to \prod_{v\in\Sigma_0\cup\Sigma_p}\prod_{\eta|v} H^1(F^{\mathrm{cyc}}_\eta, E[p^\infty])\right\}.$$

By Proposition 2.3, it follows that

$$\mathrm{Sel}^{\mathrm{rel}}(E/F^{\mathrm{cyc}})/\,\mathrm{Sel}^{\Sigma_0,\ddagger}(E/F^{\mathrm{cyc}}) \simeq \prod_{i=1}^{d} \mathcal{H}^{\ddagger_i}_{\mathfrak{p}_i}(F^{\mathrm{cyc}}, E[p^\infty]).$$

For $i = 1,\dots,d$, it follows from standard arguments (see the proof of [13, Proposition 2.11]) that $\mathcal{H}^{\ddagger_i}_{\mathfrak{p}_i}(F^{\mathrm{cyc}}, E[p^\infty])^\vee$ is isomorphic to $\mathbb{Z}_p[[\Gamma]]$. By [8, Lemma 2.6] , it suffices to show that $\mathrm{Sel}^{\mathrm{rel}}(E/F^{\mathrm{cyc}})$ has no proper finite index $\mathbb{Z}_p[[\Gamma]]$-submodules. Since $\mathrm{Sel}^{\mathrm{str}}(E/F^{\mathrm{cyc}})^\vee$ is a quotient of $\mathrm{Sel}^{\Sigma_0,\ddagger}(E/F^{\mathrm{cyc}})^\vee$, it is $\mathbb{Z}_p[[\Gamma]]$-torsion.

Recall that κ denotes the p-adic cyclotomic character. For $s \in \mathbb{Z}$, let A_s denote the twisted Galois module $E[p^\infty] \otimes \kappa^s$. Since $E(F)[p] = 0$ and Γ is pro-p, it follows that $E(F^{\mathrm{cyc}})[p] = 0$, and as a result, $H^0(F^{\mathrm{cyc}}, A_s) = 0$. Since Γ is pro-p it follows from standard arguments that $H^0(F, A_s) = 0$ for all s. For a subfield K of F^{cyc}, and v a prime of F which does not divide p, set $\mathcal{H}_v(K, A_s)$ to be the product $\prod_{\eta|v} H^1(K_\eta, A_s)/(A_s(K_\eta)\otimes\mathbb{Q}_p/\mathbb{Z}_p)$, where η ranges the finitely many primes of K above v. Set $P^{\Sigma,\mathrm{rel}}(K, A_s)$ to be the product

$$P^{\Sigma,\mathrm{rel}}(K, A_s) := \prod_{v\in\Sigma\setminus(\Sigma_0\cup\Sigma_p)} \mathcal{H}_v(K, A_s)$$

and set $P^{\Sigma,\mathrm{str}}(K, A_s)$ to be the product

$$P^{\Sigma,\mathrm{str}}(K, A_s) := \prod_{v\in\Sigma\setminus(\Sigma_0\cup\Sigma_p)} \mathcal{H}_v(K, A_s) \times \prod_{v\in\Sigma_0\cup\Sigma_p} H^1(K, A_s).$$

Let $S^{\mathrm{rel}}_{A_s}(K)$ and $S^{\mathrm{str}}_{A_s}(K)$ be the Selmer groups defined as follows

$$S^{\mathrm{rel}}_{A_s}(K) := \ker\left(H^1(F_\Sigma/F, A_s) \to P^{\Sigma,\mathrm{rel}}(K, A_s)\right),$$

$$S^{\mathrm{str}}_{A_s}(K) := \ker\left(H^1(F_\Sigma/F, A_s) \to P^{\Sigma,\mathrm{str}}(K, A_s)\right).$$

Since $\mathrm{Sel}^{\mathrm{str}}(E/F^{\mathrm{cyc}})$ is $\mathbb{Z}_p[[\Gamma]]$-cotorsion, we have that $S^{\mathrm{str}}_{A_s}(F^{\mathrm{cyc}})^{\Gamma}$ is finite for all but finitely many values of s. Hence, $S^{\mathrm{str}}_{A_s}(F)$ is finite for all but finitely many values of s. We set $M = A_s$, and in accordance with the proof of [7, Proposition 4.14], $M^* = A_{-s}$. Denote by $S_M(F)$ the Selmer group defined by the relaxed conditions $S^{\mathrm{rel}}_{A_s}(F)$ and in accordance with the discussion on [7, p. 100], $S_{M^*}(F)$ is the strict Selmer group $S^{\mathrm{str}}_{A_{-s}}(F)$. Let s be such that $S_{M^*}(F)$ is finite. Since $S_{M^*}(F)$ is finite and $M^*(F) = 0$, it follows that the map $H^1(F_\Sigma/F, M) \to P^{\Sigma,\mathrm{rel}}(K, M)$ is surjective (see [7, Proposition 4.13]). It follows from the proof of [7, Proposition 4.14] that $\mathrm{Sel}^{\mathrm{rel}}(E/F^{\mathrm{cyc}})$ has no proper finite index $\mathbb{Z}_p[[\Gamma]]$-submodules. This completes the proof. ∎

Recall that for $i = 1, 2$, the μ-invariant (resp. λ-invariant) of the Selmer group $\mathrm{Sel}^{\Sigma_1,\ddagger}(E_i/F^{\mathrm{cyc}})$ is denoted by $\mu^{\Sigma_1,\ddagger}_{E_i}$ (resp. $\lambda^{\Sigma_1,\ddagger}_{E_i}$).

Theorem 4.5 *Let E_1 and E_2 be elliptic curves over F which are p-congruent. Let $\ddagger$ be a signed vector and assume that $(E_1, E_2, \ddagger)$ satisfies Hypothesis (4.2). Let Σ_1 be the set of primes as in Definition 4.1. Then the following assertions hold:*

(1) *The μ-invariant $\mu^{\Sigma_1,\ddagger}_{E_1}$ is equal to zero if and only if $\mu^{\Sigma_1,\ddagger}_{E_2}$ is equal to zero.*
(2) *If $\mu^{\Sigma_1,\ddagger}_{E_1} = 0$ (or equivalently $\mu^{\Sigma_1,\ddagger}_{E_2} = 0$), then the Σ_1-imprimitive λ-invariants $\lambda^{\Sigma_1,\ddagger}_{E_1}$ and $\lambda^{\Sigma_1,\ddagger}_{E_2}$ are equal.*

Proof For $i = 1, 2$, let M_i denote the Pontryagin dual of $\mathrm{Sel}^{\Sigma_1,\ddagger}(E_i/F^{\mathrm{cyc}})$. It follows from Propositions 4.2 and 4.3 that M_1/pM_1 is isomorphic to M_2/pM_2. Note that $\mu^{\Sigma_1,\ddagger}_{E_i}$ is equal to 0 if and only if M_i/pM_i is finite. Thus, it follows that if $\mu^{\Sigma_1,\ddagger}_{E_1}$ is zero, then so is $\mu^{\Sigma_1,\ddagger}_{E_2}$.

Next, assume that $\mu^{\ddagger}_{E_1}$ and $\mu^{\ddagger}_{E_2}$ are both zero. Proposition 4.4 asserts that M_i contains no finite $\mathbb{Z}_p[[\Gamma]]$-submodules, and thus, M_i is a free $\mathbb{Z}_p$-module of rank equal to $\lambda^{\Sigma_1,\ddagger}_{E_i}$. Since M_1/pM_1 is isomorphic to M_2/pM_2, it follows that $\lambda^{\Sigma_1,\ddagger}_{E_1}$ is equal to $\lambda^{\Sigma_1,\ddagger}_{E_2}$. ∎

5 Congruences for Euler characteristics

Consider elliptic curves E_1 and E_2 that are p-congruent and let $\Sigma^{\mathrm{ss}} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_d\}$ be the set of supersingular primes v of E_1 such that $v|p$. As noted earlier, these are also the supersingular primes v of E_2 such that $v|p$. Let $\ddagger \in \{+,-\}^d$ be a signed vector and assume that Hypothesis (4.2) is satisfied for the triple $(E_1, E_2, \ddagger)$. Associated to E_1 and E_2 is the set of primes Σ_1, see Definition 4.1. In this section, it is shown that there is an explicit relationship between the multisigned Euler characteristics $\chi^{\ddagger}_t(\Gamma, E_1)$ and $\chi^{\ddagger}_t(\Gamma, E_2)$.

Let E be an elliptic curve satisfying Hypothesis (2.1) and Σ_0 a finite set of primes $v \nmid p$. Recall that $r^{\ddagger}_E$ is the order of vanishing of the characteristic polynomial $f^{\ddagger}_E(T)$ at $T = 0$. The following Proposition shows that the quantity $r^{\ddagger}_E$ is related to the Mordell Weil rank of E and the reduction type of E at the primes $v|p$. The proof of the following result is based on an adaptation of the control theorem from the ordinary setting, see [23].

https://doi.org/10.4153/S0008414X21000699 Published online by Cambridge University Press

Proposition 5.1 *Let E be as above and assume that the following two conditions are satisfied:*

(i) *the truncated Euler characteristic $\chi_t^{\ddagger}(\Gamma, E)$ is defined (in the sense of Definition 3.1).*
(ii) *The p-primary part of the Tate-Shafarevich group $\text{Ш}(E/F)$ is finite.*

Let r be the Mordell-Weil rank of E and sp_E the number of primes $v|p$ at which E has split multiplicative reduction. Then, we have that $r \le r_E^{\ddagger} \le r + \mathrm{sp}_E$. In particular, if there are no primes $v \in \Sigma_p$ at which E has split multiplicative reduction, then $r_E^{\ddagger}$ is equal to r.

Proof Let Σ be a finite set of primes containing Σ_p and the primes at which E has bad reduction. By Lemma 3.4, the multisigned rank $r_E^{\ddagger}$ is equal to the $\mathbb{Z}_p$-corank of $\mathrm{Sel}^{\ddagger}(E/F^{\mathrm{cyc}})^{\Gamma}$. We compare $\mathrm{Sel}^{\ddagger}(E/F^{\mathrm{cyc}})^{\Gamma}$ with the usual Selmer group $\mathrm{Sel}(E/F)$. Let $\Phi_{E,F} : H^1(F_\Sigma/F, E[p^\infty]) \to \prod_{v\in\Sigma} \mathcal{H}_v(F, E[p^\infty])$ be the defining map for the Selmer group $\mathrm{Sel}(E/F)$. Consider the fundamental diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}(E/F) \arrow[r] \arrow[d, "f"] & H^1(F_\Sigma/F, E[p^\infty]) \arrow[r] \arrow[d, "g"] & \mathrm{im}\,\Phi_{E,F} \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & \mathrm{Sel}^{\ddagger}(E/F^{\mathrm{cyc}})^{\Gamma} \arrow[r] & H^1(F_\Sigma/F^{\mathrm{cyc}}, E[p^\infty])^{\Gamma} \arrow[r] & \mathrm{im}\,\Phi^{\ddagger}_{E,F^{\mathrm{cyc}}} \arrow[r] & 0,
\end{tikzcd}$$

where the vertical maps are induced by restriction. Since $E(F)[p] = 0$ and Γ is pro-p, it follows that $H^0(F^{\mathrm{cyc}}, E[p^\infty]) = 0$. It follows from the inflation-restriction sequence that g is an isomorphism. Thus, we have the following short exact sequence:

$$0 \to \mathrm{Sel}(E/F) \to \mathrm{Sel}^{\ddagger}(E/F^{\mathrm{cyc}})^{\Gamma} \to \ker h \to 0. \tag{5.1}$$

It suffices to show that the kernel of h has corank less than or equal to sp_E. For $v \in \Sigma\backslash\Sigma_{\mathrm{ss}}$, let h'_v denote the natural map

$$h'_v : \mathcal{H}_v(F, E[p^\infty]) \to \mathcal{H}_v(F^{\mathrm{cyc}}, E[p^\infty]).$$

For $\mathfrak{p}_i \in \Sigma_{\mathrm{ss}}$, set $h'_{\mathfrak{p}_i}$ denotes the map

$$h'_{\mathfrak{p}_i} : \mathcal{H}^{\ddagger_i}_{\mathfrak{p}_i}(F, E[p^\infty]) \to \mathcal{H}^{\ddagger_i}_{\mathfrak{p}_i}(F^{\mathrm{cyc}}, E[p^\infty]).$$

Let h' be the product of the maps h'_v as v ranges over Σ. Note that the kernel of h is contained in the kernel of h'. Let $\Sigma_{\mathrm{sp}}(E)$ be the set of primes $v|p$ at which E has split multiplicative reduction. We show that $\ker h'_v$ is finite if $v \notin \Sigma_{\mathrm{sp}}(E)$ and of corank one for $v \in \Sigma_{\mathrm{sp}}(E)$. For $v \in \Sigma\backslash\Sigma_p$, this follows from [4, Lemma 3.4] , for $v \in \Sigma_p$ at which E has good ordinary reduction, it follows from [4, Proposition 3.5]. Next consider the case where $v|p$ and E has multiplicative reduction at v.

The Galois representation of the local Galois group G_{F_v} on $E[p]$ is of the form $\begin{pmatrix} \varphi_v\kappa & * \\ & \varphi_v^{-1}\end{pmatrix}$, where φ_v is an unramified character. Let w be a prime of F^{cyc} above v and let Γ_v denote $\mathrm{Gal}(F_w^{\mathrm{cyc}}/F_v)$. By Shapiro's Lemma,

$$H^0\left(\Gamma, \prod_{\eta|v} H^1(F_\eta^{\mathrm{cyc}}, D_v)\right) \simeq H^0(\Gamma_v, H^1(F_w^{\mathrm{cyc}}, D_v)).$$

https://doi.org/10.4153/S0008414X21000699 Published online by Cambridge University Press

The kernel of h'_v is contained in the kernel of the restriction map

$$H^1(F_v, D_v) \to H^1(F_w^{\mathrm{cyc}}, D_v)$$

and by the inflation restriction sequence, the kernel of h'_v is contained in $H^1(\Gamma_v, H^0(F_w^{\mathrm{cyc}}, D_v))$. When E has nonsplit multiplicative reduction at v, the character φ_v is nontrivial and thus $H^0(F_v, D_v) = 0$. Since Γ_v is pro-p, it follows that $H^0(F_w^{\mathrm{cyc}}, D_v) = 0$ when $\varphi_v \neq 1$. On the other hand, when $\varphi_v = 1$, the Galois action on $H^0(F_w^{\mathrm{cyc}}, D_v) \simeq \mathbb{Q}_p/\mathbb{Z}_p$ is trivial. As a result, the corank of $H^1(\Gamma_v, H^0(F_w^{\mathrm{cyc}}, D_v))$ is one when E has split multiplicative reduction at v.

Finally, consider the case when $v|p$ and E has supersingular reduction at v. In this case, h'_v is injective, as shown in the proof of [21, Theorem 5.3].

Putting all this together, we have that $\mathrm{corank}_{\mathbb{Z}_p} \ker h \leq \mathrm{sp}_E$, and thus, from the short exact sequence (5.1), we have

$$r_E^{\ddagger} \leq \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}(E/F) + \mathrm{sp}_E = r + \mathrm{corank}_{\mathbb{Z}_p} Ш(E/F)[p^{\infty}] + \mathrm{sp}_E .$$

Since it is assumed that $Ш(E/F)[p^{\infty}]$ is finite, the result follows. ∎

Remark 5.0.1 It is generally expected that for any signed vector $\ddagger$, the order of vanishing $r_E^{\ddagger}$ should equal the rank of $E(F)$ when E has good reduction at the primes above p. This can be verified through computation when $F = \mathbb{Q}$. The above result shows that if certain additional conditions are met, then this statement is indeed true. In particular, in the case when $\mathrm{rank}\, E(F) = 1$ (and $Ш(E/F)[p^{\infty}]$ is finite), one should expect that $r_E^{\ddagger} = 1$ as well. Assuming this, it follows from Lemma 3.3 that the truncated Euler characteristic is defined in this setting. Of course, in the rank zero setting, the truncated Euler characteristic matches the classical Euler characteristic which is defined if $Ш(E/F)[p^{\infty}]$ is finite. We believe that the conditions of Lemma 3.3 should always be satisfied for multisigned Selmer groups, however, this expectation has not been written down explicitly in any references that we are aware of.

We now study congruences for truncated Euler characteristics. For $v \in \Sigma_0$, set $h_E^{(v)}(T)$ to be the characteristic polynomial of the Pontryagin dual of $\mathcal{H}_v(F^{\mathrm{cyc}}, E[p^{\infty}])$. Since $\mathrm{Sel}^{\ddagger}(E/F^{\mathrm{cyc}})$ is $\mathbb{Z}_p[[\Gamma]]$-cotorsion, it follows from Proposition 2.3 that there is a short exact sequence:

$$0 \to \mathrm{Sel}^{\ddagger}(E/F^{\mathrm{cyc}}) \to \mathrm{Sel}^{\ddagger,\Sigma_0}(E/F^{\mathrm{cyc}}) \to \prod_{v\in\Sigma_0} \mathcal{H}_v(F^{\mathrm{cyc}}, E[p^{\infty}]) \to 0.$$

As a result, we arrive at the following relation:

$$f_E^{\Sigma_0,\ddagger}(T) = f_E^{\ddagger}(T) \prod_{l\in\Sigma_0} h_E^{(v)}(T). \tag{5.2}$$

Recall that $V_p(E)$ is the p-adic vector space $T_p(E) \otimes \mathbb{Q}_p$, equipped with $\mathrm{Gal}(\overline{F}/F)$-action. Let $P_v(E,T)$ denote the characteristic polynomial

$$P_v(E,T) := \det\left((\mathrm{Id} - \mathrm{Frob}_v\, X)_{|V_p(E)^{\mathrm{I}_v}}\right), \tag{5.3}$$

where I_v is the inertia group at v. For $s \in \mathbb{C}$, set $L_v(E,s)$ to denote $P_v(E, Nv^{-s})^{-1}$, where Nv denotes the norm $N_{L/\mathbb{Q}}v$. Recall that γ is a topological generator of Γ. Let $\rho : \Gamma \to \mu_{p^{\infty}}$ be a finite order character and let σ_v denote the Frobenius at v.

Let $\mathcal{P}_v(E,T)$ be the element in $\mathbb{Z}_p[[\Gamma]]$ defined by the relation $\mathcal{P}_v(E,\rho(\gamma)-1) = P_v(E,\rho(\sigma_v)Nv^{-1})$. According to [8, Proposition 2.4], the polynomial $\mathcal{P}_v(E,T)$ generates the Pontryagin dual of $\mathcal{H}_v(F^{\mathrm{cyc}}, E[p^\infty])$ and thus coincides with $h^{(v)}(T)$ up to a unit in $\mathbb{Z}_p[[\Gamma]]$.

Definition 5.2 Set δ_{E,Σ_0} to be the product $\prod_{v\in\Sigma_0}|L_v(E,1)|_p$. Here, $|L_v(E,1)|_p$ is set to be equal to 0 if $L_v(E,1)^{-1}=0$.

Write

$$f_E^{\Sigma_0,\ddagger}(T) = T^{r_E^\ddagger} g_E^{\Sigma_0,\ddagger}(T),$$

and set $|g_{E,\Sigma_0}(0)|_p^{-1}$ to be zero if $g_{E,\Sigma_0}(0)$ equals zero. It follows from the relation (5.2) that

$$g_E^{\Sigma_0,\ddagger}(T) = g_E^{\ddagger}(T)\prod_{l\in\Sigma_0} h_E^{(v)}(T). \tag{5.4}$$

One has the following result.

Lemma 5.3 *Let E be an elliptic curve satisfying Hypothesis (2.1) and let ‡ be a signed vector, for a finite set Σ_0 consisting of primes $v\nmid p$. Then we have the following equality:*

$$\delta_{E,\Sigma_0}\times\chi_t^\ddagger(\Gamma,E) = |g_E^{\Sigma_0,\ddagger}(0)|_p^{-1}.$$

Proof Note that $\mathcal{P}_v(E,0)$ equals $P_v(E,l^{-1}) = L_v(E,1)^{-1}$. Therefore, it follows that $h^{(v)}(0)$ coincides with $|L_v(E,1)|_p$ up to a unit in $\mathbb{Z}_p$. From the relation (5.4), we have that

$$|g_E^{\Sigma_0,\ddagger}(0)|_p^{-1} = |g_E^{\ddagger}(0)|_p^{-1}\prod_{l\in\Sigma_0}|L_v(E,1)|_p = |g_E^\ddagger(0)|_p^{-1}\times\delta_{E,\Sigma_0}.$$

Lemma 3.4 asserts that $\chi_t^\ddagger(\Gamma,E)$ is equal to $|g_E^\ddagger(0)|_p^{-1}$, and this completes the proof. ∎

Denote the μ-invariants of $\mathrm{Sel}^\ddagger(E/F^{\mathrm{cyc}})$ and $\mathrm{Sel}^{\Sigma_0,\ddagger}(E/F^{\mathrm{cyc}})$ by $\mu_E^\ddagger$ and $\mu_E^{\Sigma_0,\ddagger}$, respectively. Denote the λ-invariants by $\lambda_E^\ddagger$ and $\lambda_E^{\Sigma_0,\ddagger}$ respectively. It is easy to show that for $v\in\Sigma_0$, the μ-invariant of $h_E^{(v)}(T)$ is equal to zero, and hence $\mu_E^{\Sigma_0,\ddagger}$ is equal to $\mu_E^\ddagger$.

Lemma 5.4 *Let E be an elliptic curve satisfying Hypothesis (2.1) and let ‡ be a signed vector. For a finite set Σ_0 consisting of primes $v\nmid p$, we have that*

$$\delta_{E,\Sigma_0}\times\chi_t^\ddagger(\Gamma,E) = 1 \Leftrightarrow \mu_E^\ddagger = 0 \text{ and } \lambda_E^{\Sigma_0,\ddagger} = r_E^\ddagger.$$

Proof First assume that $\delta_{E,\Sigma_0}\times\chi_t^\ddagger(\Gamma,E)=1$, it is then shown that $\mu_E^\ddagger=0$ and $\lambda_E^{\Sigma_0,\ddagger}=r_E^\ddagger$. Recall that $f_E^{\Sigma_0,\ddagger}(T)$ is the characteristic polynomial for the Selmer group $\mathrm{Sel}^{\Sigma_0,\ddagger}(E/F^{\mathrm{cyc}})$ and is written as $T^{r_E^\ddagger}g_E^{\Sigma_0,\ddagger}(T)$. It follows from Lemma 5.3 that $g_E^{\Sigma_0,\ddagger}(0)$ is a unit in $\mathbb{Z}_p$, and thus $g_E^{\Sigma_0,\ddagger}(T)$ is a unit in $\mathbb{Z}_p[[\Gamma]]$. It follows from this that $\mu_{E,\Sigma_0}^\ddagger=0$ and $\lambda_{E,\Sigma_0}^\ddagger = r_E^\ddagger$. The following relation is satisfied:

$$f_{E,\Sigma_0}^\ddagger(T) = f_E^\ddagger(T)\times\prod_{v\in\Sigma_0}h_E^{(v)}(T)$$

https://doi.org/10.4153/S0008414X21000699 Published online by Cambridge University Press

(see (5.2)). According to [8, Proposition 2.4], the polynomial $\mathcal{P}_v(E,T)$ generates the Pontryagin dual of $\mathcal{H}_v(F^{\mathrm{cyc}}, E[p^\infty])$ and thus coincides with $h^{(v)}(T)$ up to a unit in $\mathbb{Z}_p[[\Gamma]]$. It is easy to see that $\mathcal{P}_v(E,T)$ is equal to a monic polynomial, up to a unit in $\mathbb{Z}_p$. As a result, p does not divide $h^{(v)}(T)$. It follows that $\mu_E^{\ddagger} = \mu_{E,\Sigma_0}^{\ddagger} = 0$.

Conversely, suppose that $\mu_E^{\ddagger} = 0$ and that $\lambda_{E,\Sigma_0}^{\ddagger} = r_E^{\ddagger}$. The degree of $f_{E,\Sigma_0}^{\ddagger}(T)$ is equal to $\lambda_{E,\Sigma_0}^{\ddagger} = r_E^{\ddagger}$. Since $f_{E,\Sigma_0}^{\ddagger}(T)$ is expressed as $T^{r_E^{\ddagger}} g_{E,\Sigma_0}(T)$, the degree of $g_{E,\Sigma_0}(T)$ is equal to zero. It has been shown that $\mu_{E,\Sigma_0}^{\ddagger} = \mu_E^{\ddagger} = 0$. It follows that $g_{E,\Sigma_0}(T)$ is a unit in $\mathbb{Z}_p$. Lemma 5.3 asserts that $\delta_{E,\Sigma_0} \times \chi_t^{\ddagger}(\Gamma, E)$ is equal to $|g_{E,\Sigma_0}(0)|_p^{-1}$ and therefore equal to 1. ■

Next, we come to the main theorem of the section. It is shown that the truncated Euler characteristic of E_1 is related to that of E_2 after one accounts for the auxiliary set of primes Σ_1. The smaller the set of primes Σ_1, the more refined the congruence relation between truncated Euler characteristics is. This is why it is of considerable importance that the set of primes Σ_1 be carefully chosen to be as small as possible. We note that in the statement of [30, Theorem 3.3], the elliptic curves E_1 and E_2 were defined over $\mathbb{Q}$ with good ordinary reduction at p. Furthermore, the set of auxiliary primes Σ_0 was the full set of primes $v \nmid p$ at which E_1 or E_2 has bad reduction. The set of primes Σ_1 is smaller and hence, when $F = \mathbb{Q}$ the result below refines the result [30, Theorem 3.3].

Theorem 5.5 *Let E_1 and E_2 be elliptic curves which satisfy Hypothesis* (4.2) *mentioned in the introduction. Then, the following assertions hold.*

(1) *Suppose $r_{E_1}^{\ddagger}$ is equal to $r_{E_2}^{\ddagger}$. Then, $\delta_{E_1,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_1)$ is equal to* 1 *if and only if $\delta_{E_2,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_2)$ is equal to* 1.
(2) *If $r_{E_1}^{\ddagger} < r_{E_2}^{\ddagger}$, then $\delta_{E_1,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_1)$ is divisible by p.*
(3) *If $\delta_{E_1,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_1)$ is divisible by p and $\delta_{E_2,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_2) = 1$, then, $r_{E_1}^{\ddagger} < r_{E_2}^{\ddagger}$.*

Proof We first assume consider the case when $r_{E_1}^{\ddagger}$ is equal to $r_{E_2}^{\ddagger}$. It follows from Lemma 5.4 that $\delta_{E_i,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_i) = 1$ if and only if $\mu_{E_i}^{\ddagger} = 0$ and $\lambda_{E_i}^{\Sigma_1,\ddagger} = r_{E_i}^{\ddagger}$. Suppose that $\delta_{E_1,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_1) = 1$, then it follows that $\mu_{E_1}^{\ddagger} = 0$ and $\lambda_{E_1}^{\Sigma_1,\ddagger} = r_{E_1}^{\ddagger}$. It follows from Corollary 4.5 that $\mu_{E_2}^{\ddagger} = 0$ and $\lambda_{E_2}^{\Sigma_1,\ddagger} = r_{E_2}^{\ddagger}$. Thus, by Lemma 5.4, we have that $\delta_{E_2,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_2) = 1$. This proves part (1).

Next, it is assumed that $r_{E_1}^{\ddagger} < r_{E_2}^{\ddagger}$ and it shown that p divides $\delta_{E_1,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_1)$. Suppose by way of contradiction that p does not divide $\delta_{E_1,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_1)$. This means that $\delta_{E_1,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_1)$ is equal to 1. Lemma 5.4 asserts that $\mu_{E_1}^{\ddagger} = 0$ and $\lambda_{E_1}^{\Sigma_1,\ddagger} = r_{E_1}^{\ddagger}$. It follows from Corollary 4.5 that $\mu_{E_2}^{\ddagger} = 0$ and $\lambda_{E_2}^{\Sigma_1,\ddagger} = r_{E_1}^{\ddagger}$. Recall that $\lambda_{E_2}^{\Sigma_1,\ddagger}$ is the degree of the characteristic polynomial $f_{E_2}^{\ddagger}(T)$. Since $r_{E_2}^{\ddagger}$ is the order of vanishing of $f_{E_2}^{\ddagger}(T)$ at $T = 0$, it follows that $\lambda_{E_2}^{\Sigma_1,\ddagger} \geq r_{E_2}^{\ddagger}$. This is a contradiction, as it is assumed that $r_{E_1}^{\ddagger} < r_{E_2}^{\ddagger}$. Hence, p divides $\delta_{E_1,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_1)$. This proves part (2).

Next, we prove part (3). Since $\delta_{E_2,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_2) = 1$, we deduce from Lemma 5.4 that $\mu_{E_2}^{\ddagger} = 0$ and $\lambda_{E_2}^{\Sigma_1,\ddagger} = r_{E_2}^{\ddagger}$. It follows from Corollary 4.5 that $\mu_{E_1}^{\ddagger} = 0$ and $\lambda_{E_1}^{\Sigma_1,\ddagger} = r_{E_2}^{\ddagger}$. Since p divides $\delta_{E_1,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_1)$, it follows from Lemma 5.4 that $r_{E_1}^{\ddagger} < \lambda_{E_1}^{\Sigma_1,\ddagger}$. Therefore, we have shown that $r_{E_1}^{\ddagger} < r_{E_2}^{\ddagger}$. ■

Consider the case when $r^{\ddagger}_{E_1} = r^{\ddagger}_{E_2}$. It is natural to ask if $\chi^{\ddagger}_t(\Gamma, E_1) = 1$ implies that $\chi^{\ddagger}_t(\Gamma, E_2) = 1$? This statement is false, as is shown in [30, Example 5.2], where it is shown that there are 5-congruent elliptic curves E_1 and E_2 over $\mathbb{Q}$ which both have Mordell-Weil rank 1 and good ordinary reduction at 5, such that $\chi_t(\Gamma, E_1) = 1$ and $\chi_t(\Gamma, E_2) = 5^2$. Therefore it is necessary to account the factors δ_{E_i,Σ_1}, i.e.,

$$\delta_{E_1,\Sigma_1} \times \chi_t(\Gamma, E_1) = 1 \Leftrightarrow \delta_{E_2,\Sigma_1} \times \chi_t(\Gamma, E_2) = 1.$$

6 Results over $\mathbb{Z}_p^m$-extensions

We show that our results on truncated Euler characteristics generalize to $\mathbb{Z}_p^m$-extensions. The multisigned Selmer groups have not been defined for more general p-adic Lie extensions. In the good ordinary reduction setting, the reader is referred to [37] for a discussion on truncated Euler characteristics over general p-adic Lie extensions. In [30, Section 4], congruence relations are proved for truncated Euler characteristics over p-adic Lie extensions for elliptic curves with good ordinary reduction at p.

Let $\mathcal{F}_\infty/F$ be a Galois extension of F containing F^{cyc} such that $\text{Gal}(\mathcal{F}_\infty/F) \simeq \mathbb{Z}_p^m$ for an integer $m \geq 1$. Set $\mathrm{G} := \text{Gal}(\mathcal{F}_\infty/F)$, $H := \text{Gal}(\mathcal{F}_\infty/F^{\text{cyc}})$ and identify Γ with $\text{Gal}(F^{\text{cyc}}/F) \simeq \mathrm{G}/\mathrm{H}$. Let E be an elliptic curve and $\ddagger$ be a signed vector, assume that $(E, \ddagger)$ satisfies Hypothesis (4.1). Another natural hypothesis is that the Selmer groups be in $\mathfrak{M}_H(\mathrm{G})$. The precise definition is given below.

Definition 6.1 Let M be a cofinitely generated cotorsion $\mathbb{Z}_p[[\mathrm{G}]]$-module and let $M(p)$ be the p-primary submodule of M. The category $\mathfrak{M}_H(\mathrm{G})$ consists of all such modules M such that $M/M(p)$ is a finitely generated $\mathbb{Z}_p[[H]]$-module.

We introduce the following hypothesis.

Hypothesis 6.1 *Assume that the Selmer group* $\text{Sel}^{\ddagger}(E/\mathcal{F}_\infty)$ *is in* $\mathfrak{M}_H(\mathrm{G})$.

We recall the notion of the truncated G-Euler characteristic of $\text{Sel}^{\ddagger}(E/\mathcal{F}_\infty)$.

Definition 6.2 Let M be a discrete p-primary G-module, define

$$\psi_D : H^0(\Gamma, M^H) \to H^1(\mathrm{G}, M)$$

as the composite of the natural map $\phi_{D^H} : H^0(\Gamma, M^H) \to H^1(\Gamma, M^H)$ with the inflation map $H^1(\Gamma, M^H) \to H^1(\mathrm{G}, M)$. The G-Euler characteristic of the module M is defined if the following two conditions are satisfied:

(1) both $\ker(\psi_M)$ and $\text{cok}(\psi_M)$ are finite and
(2) $H^i(\mathrm{G}, M)$ is finite for $i \geq 2$.

The truncated G-Euler characteristic is then defined by

$$\chi_t(\mathrm{G}, M) := \frac{\# \ker(\psi_M)}{\# \text{cok}(\psi_M)} \times \prod_{i=2}^{m} \# \left(H^i(\mathrm{G}, M)\right)^{(-1)^i}.$$

Next, we recall the notion of the Akashi series. For a cofinitely generated Γ-module M, let $\text{char}_\Gamma(M)$ be the characteristic polynomial of its Pontryagin dual $M^\vee$. This is the unique polynomial generating the characteristic ideal which can be expressed as the product of a power of p and a distinguished polynomial.

Definition 6.3 Let D be a discrete p-primary G-module. The Akashi series of D is defined if $H^i(H, D)$ is cotorsion and cofinitely generated for all $i \geq 0$. In this case, the Akashi series $\mathrm{Ak}_H(D)$ is taken to be the following alternating product:

$$\mathrm{Ak}_H(D) := \prod_{i=0}^{m-1} \left(\mathrm{char}_\Gamma H^i(H, D)\right)^{(-1)^i}.$$

Note that the Akashi series coincides with the characteristic polynomial when $\mathcal{F}_\infty = F^{\mathrm{cyc}}$. The following Proposition describes the relationship between the Akashi series and truncated G-Euler characteristic.

Proposition 6.4 [37, Proposition 2.10] *Let D be a discrete p-primary* G*-module such that the Pontryagin dual $D^\vee$ is in $\mathfrak{M}_H(\mathrm{G})$. Then, the Akashi series $\mathrm{Ak}_H(D)$ is defined. Furthermore, suppose that the truncated* G*-Euler characteristic of D is defined in the sense of Definition 6.2. Let βT^k be the leading term of $\mathrm{Ak}_H(D)$. Then, the following assertions hold:*

(1) *the order of vanishing k is given by*

$$k = \sum_{i \geq 0} (-1)^i \,\mathrm{corank}_{\mathbb{Z}_p} H^i(H, D)^\Gamma,$$

(2) *the truncated* G*-Euler characteristic is given by*

$$\chi_t(\mathrm{G}, D) = |\beta|_p^{-1}.$$

The truncated G-Euler characteristic of $\mathrm{Sel}^\ddagger(E/\mathcal{F}_\infty)$ is denoted by $\chi_t^\ddagger(\mathrm{G}, E)$. When the truncated G-Euler characteristic is defined, it is related to the Akashi series of $\mathrm{Sel}^\ddagger(E/\mathcal{F}_\infty)$, which we denote by $\mathrm{Ak}_H^\ddagger(E)$. The following theorem due to Lei and Lim describes the link between Akashi series $\mathrm{Ak}_H^\ddagger(E)$ and the characteristic polynomial $f_E^\ddagger(T)$ of the Selmer group $\mathrm{Sel}^\ddagger(E/F^{\mathrm{cyc}})$.

Theorem 6.5 [21, Theorem 1.1] *Let E be an elliptic curve over a number field F, and let $\ddagger$ be a signed vector. Let $\mathcal{F}_\infty$ be a $\mathbb{Z}_p^m$-extension of F which contains F^{cyc}. Assume that:*

(1) *Hypotheses* (2.1) *and* (6.1) *are satisfied.*
(2) *The Selmer group* $\mathrm{Sel}^\ddagger(E/F^{\mathrm{cyc}})$ *is* $\mathbb{Z}_p[[\Gamma]]$*-cotorsion.*

Then, the Akashi series $\mathrm{Ak}_H^\ddagger(E)$ is well-defined and is given by

$$\mathrm{Ak}_H^\ddagger(E) = T^{\gamma_E} \cdot f_E^\ddagger(T),$$

where γ_E is the number of primes of F^{cyc} above p with nontrivial decomposition group in $\mathcal{F}_\infty/F^{\mathrm{cyc}}$ and at which E has split multiplicative reduction.

Corollary 6.6 *Let E be an elliptic curve over a number field F, and let $\ddagger$ be a signed vector. Let $\mathcal{F}_\infty$ be a $\mathbb{Z}_p^m$-extension of F which contains F^{cyc}. Assume that*

(1) *Hypotheses* (2.1), (4.1), *and* (6.1) *are satisfied.*
(2) *The truncated* G*-Euler characteristic* $\chi_t^\ddagger(\mathrm{G}, E)$ *is well defined.*

Then, the truncated G*-Euler characteristic* $\chi_t^\ddagger(\mathrm{G}, E)$ *is equal to the truncated* Γ*-Euler characteristic* $\chi_t^\ddagger(\Gamma, E)$.

Proof The result is a direct consequence of Theorem 6.5, Proposition 6.4, and Lemma 3.4. ■

Theorem 6.7 *Let E_1 and E_2 be p-congruent elliptic curves over a number field F. Let $\ddagger$ be a signed vector. Assume that*

(1) *Hypotheses (4.2) and (6.1) are satisfied.*
(2) *The truncated* G*-Euler characteristic $\chi_t^{\ddagger}(\mathrm{G}, E)$ is well defined.*

Then, the following assertions hold.

(1) *Suppose that $r^{\ddagger}_{E_1} = r^{\ddagger}_{E_2}$. Then, we have that the truncated* G*-Euler characteristics are defined, then $\delta_{E_1,\Sigma_1} \times \chi_t^{\ddagger}(\mathrm{G}, E_1)$ is equal to* 1 *if and only if $\delta_{E_2,\Sigma_1} \times \chi_t^{\ddagger}(\mathrm{G}, E_2)$ is equal to* 1*. Furthermore, $\delta_{E_1,\Sigma_1} \times \mathrm{Ak}_H^{\ddagger}(E_1)$ is equal to $T^{r_{E_1}+\gamma_{E_1}}$ if and only if $\delta_{E_2,\Sigma_1} \times \mathrm{Ak}_H^{\ddagger}(E_2)$ is equal to $T^{r_{E_1}+\gamma_{E_2}}$.*
(2) *Suppose that $r^{\ddagger}_{E_1} < r^{\ddagger}_{E_2}$. Then, p divides $\delta_{E_1,\Sigma_1} \times \chi_t^{\ddagger}(\mathrm{G}, E_1)$.*

Proof The result is a direct consequence of Theorem 5.5, Proposition 6.4, and Corollary 6.6. ∎

7 Examples

We discuss two concrete examples which illustrate our results for $p = 5$. Our computations are aided by Sage. The reader is referred to [30, Section 5] for examples when both elliptic curves are defined over $\mathbb{Q}$ and have good ordinary reduction at $p = 5$.

7.1 Example 1

Consider elliptic curves $E_1 = 66a1$ and $E_2 = 462d1$. The elliptic curves E_1 and E_2 are 5-congruent and supersingular at 5. Both elliptic curves E_1 and E_2 have Mordell-Weil rank zero, hence the Euler characteristic $\chi(\Gamma, E_i)$ is well defined for $i = 1, 2$. Hypothesis (2.1) is satisfied for the elliptic curves E_1 and E_2. Let $\ddagger \in \{+, -\}$ be a choice of sign. Assume that for $i = 1, 2$, the Selmer group $\mathrm{Sel}^{\ddagger}(E_i/\mathbb{Q}^{\mathrm{cyc}})$ is $\mathbb{Z}_p[[\Gamma]]$-cotorsion. Therefore, Hypothesis (4.2) is satisfied. We show that $\delta_{E_i,\Sigma_1} = 1$ and $\chi_t^{\ddagger}(\Gamma, E_i) = 1$ for $i = 1, 2$. This demonstrates Theorem 5.5 which asserts that

$$\delta_{E_1,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_1) = 1 \text{ if and only if } \delta_{E_2,\Sigma_1} \times \chi_t^{\ddagger}(\Gamma, E_2) = 1.$$

The conductor N_1 of E_1 (resp. N_2 of E_2) is $66 = 2 \times 3 \times 11$ (resp. $462 = 2 \times 3 \times 7 \times 11$). The set Σ_0 consists of the primes $v \neq 5$ at which E_1 or E_2 has bad reduction. We have that $\Sigma_0 = \{2, 3, 7, 11\}$. We calculate the optimal set of primes $\Sigma_1 \subseteq \Sigma_0$. Let $\overline{N}$ denote the prime to 5 Artin conductor of the residual representation. Recall that Σ_1 is the set of primes $\Sigma(E_1) \cup \Sigma(E_2)$, where $\Sigma(E_i)$ consists of the primes $v \neq 5$ such that $v|(N_i/\overline{N})$, and if μ_5 is contained in $\mathbb{Q}_v$, then E has split multiplicative reduction at v. Note that $\mathbb{Q}_{11}$ contains μ_5 and both elliptic curves E_1 and E_2 have nonsplit multiplicative reduction at 11. Hence, $\Sigma_1 \subseteq \{2, 3, 7\}$ is strictly smaller than $\Sigma_0 = \{2, 3, 7, 11\}$. Recall that δ_{E,Σ_1} is the product $\prod_{v\in\Sigma_1} |L_v(E, 1)|_5$. From the discussion in [30, p. 7] , $L_v(E_i, 1)^{-1}$ is equal to $v^{-1}(l + \beta_v(E_i) - a_l(E))$, where $\beta_v(E_i)$ is 1 when E_i has good reduction at v and is 0 otherwise. These values are calculated from the following:

$$2 + \beta_2(E_1) - a_2(E_1) = 3, 3 + \beta_3(E_1) - a_3(E_1) = 2, 7 + \beta_7(E_1) - a_7(E_1) = 6,$$
$$2 + \beta_2(E_2) - a_2(E_2) = 3, 3 + \beta_3(E_2) - a_3(E_2) = 3, 7 + \beta_7(E_2) - a_7(E_2) = 8.$$

https://doi.org/10.4153/S0008414X21000699 Published online by Cambridge University Press

None of the above values are not divisible by 5 and hence, δ_{E_1,Σ_1} and δ_{E_2,Σ_1} are both 1. The Euler characteristics $\chi^{\pm}(\Gamma, E_i)$ may be calculated explicitly. The Euler characteristic $\chi(\Gamma, E_i)$ is given up to 5-adic unit by

$$\chi^{\pm}(\Gamma, E_i) \sim \#\operatorname{Sel}(E/\mathbb{Q}) \times \prod c_v(E_i),$$

see [14, Theorem 1.2]. For both elliptic curves, $\#Ш(E_i/\mathbb{Q})[5]$ and $E_i(\mathbb{Q})$ has no 5-torsion. It follows that $\#\operatorname{Sel}(E/\mathbb{Q}) \sim 1$. Furthermore, the Tamagawa products $\prod c_v(E_1) = 6$ and $\prod c_v(E_1) = 16$. It thus follows that both Euler characteristics $\chi^{\pm}(\Gamma, E_i) = 1$ for $i = 1, 2$. We have thus demonstrated the relationship between Euler characteristics via explicit computation.

7.2 Example 2

We work out an example over the field $F := \mathbb{Q}(i)$. Let E_1 (resp. E_2) be the curves $38a1$ (resp. $114b1$), base-changed to F. The elliptic curves E_1 and E_2 are 5-congruent. The prime $p = 5$ splits into $\mathfrak{p}\mathfrak{p}^*$, where $\mathfrak{p} = (2+i)$ and $\mathfrak{p}^* = (2-i)$. Both curves E_1 and E_2 are supersingular at the primes $\mathfrak{p}$ and $\mathfrak{p}^*$. The Mordell-Weil ranks of E_1 (resp. E_2) over F are 0 (resp. 1). Let $\ddagger = (\ddagger_1, \ddagger_2)$ be a signed vector. It thus makes sense to assume that the order of vanishing of the signed Selmer group at $T = 0$ is given by $r_{E_1}^{\ddagger} = 0$ and $r_{E_2}^{\ddagger} = 1$. Since $r_{E_2}^{\ddagger} \leq 1$, it follows from Lemma 3.3 that the truncated Euler characteristic $\chi_t^{\ddagger}(\Gamma, E_2)$ is well defined. On the other hand, since $r_{E_1}^{\ddagger} = 0$, the truncated Euler characteristic $\chi_t^{\ddagger}(\Gamma, E_1)$ is well defined and coincides with the usual Euler characteristic $\chi(\Gamma, E_1)$. Since $r_{E_1}^{\ddagger} < r_{E_2}^{\ddagger}$, Theorem 5.5 asserts that 5 divides $\delta_{E_1,\Sigma_1} \times \chi(\Gamma, E_1)$. We demonstrate this via direct calculation by showing that δ_{E_1,Σ_1} is divisible by 5.

We shall assume that the Selmer groups $\operatorname{Sel}^{\ddagger}(E_i/F^{\mathrm{cyc}})$ are cotorsion. The optimal set of primes Σ_1 is contained in $\{(i+1), 3, 19\}$, the set of primes $v \nmid 5$ at which either E_1 or E_2 has bad reduction. Both curves E_1 and E_2 have split multiplicative reduction at 19, and hence $19 \in \Sigma_1$. The prime 19 is inert in F and its norm is $19^2 = 361$. The curve E_1 has split multiplicative reduction at 19, hence $a_{19}(E_1) = 1$. Recall that $L_{19}(E_1, 1)^{-1}$ is equal to $P_{19}(E_1, 19^{-2})$, see the discussion following (5.3). The characteristic polynomial $P_{19}(E_1, T)$ is equal to $1 - a_{19}(E_1)T$. Therefore, $L_{19}(E_1, 1)^{-1} = \frac{19^2 - a_{19}(E_1)}{19^2} = \frac{360}{361}$. This implies that $|L_{19}(E_1, 1)|_5 = 5$. Since $19 \in \Sigma_1$, it follows that δ_{E_1,Σ_1} is divisible by 5.

Let F_1 and F_2 be the maximal pro-p abelian extension of F unramified outside $\mathfrak{p}$, resp. $\mathfrak{p}^*$. Both F_1 and F_2 are $\mathbb{Z}_p$-extensions of F. Let $\mathcal{F}_\infty$ be the composite of F_1 and F_2. We discuss results for truncated Euler characteristics over $\mathcal{F}_\infty$. Assume that for $i = 1, 2$, the Selmer group $\operatorname{Sel}^{\ddagger}(E_i/\mathcal{F}_\infty)$ is in $\mathfrak{M}_H(\mathrm{G})$. Recall that $\mathrm{G} = \operatorname{Gal}(\mathcal{F}_\infty/F)$ and $H = \operatorname{Gal}(\mathcal{F}_\infty/F^{\mathrm{cyc}})$. Corollary 6.6 asserts that $\chi_t^{\ddagger}(\mathrm{G}, E_i)$ is equal to $\chi_t^{\ddagger}(\mathrm{G}, E_i)$ for $i = 1, 2$.

References

[1] D. Bernardi and B. Perrin-Riou, Variante p-adique de la conjecture de Birch et Swinnerton-Dyer (le cas supersingulier). C. R. Acad. Sci. Série 1. Math. **317**(1993), no. 3, 227–232.

[2] J. Coates and R. Greenberg, *Kummer theory for abelian varieties over local fields*. Invent. Math. **124**(1996), no. 1, 129–174.

[3] J. H. Coates, P. Schneider, and R. Sujatha, *Links between cyclotomic and GL_2 Iwasawa theory*. Doc. Math. **2003**(2003), 187–215.

[4] J. H. Coates and R. Sujatha, *Galois cohomology of elliptic curves*. In: Lecture Notes at the Tata Institute of Fundamental Research No. 88, Narosa Publishing House, New Delhi, (2000).

[5] M. Emerton, R. Pollack, and T. Weston, *Variation of Iwasawa invariants in Hida families*. Invent. Math. **163**(2006), 3, 523–580.

[6] R. Greenberg, *Iwasawa theory for p-adic representations*. In: Algebraic number theory—in Honor of K. Iwasawa. Mathematical Society of Japan, Tokyo, 1989.

[7] R. Greenberg, *Iwasawa theory for elliptic curves*. In: Arithmetic theory of elliptic curves, Springer, Berlin, Heidelberg, 1999, pp. 51–144.

[8] R. Greenberg and V. Vatsal, *On the Iwasawa invariants of elliptic curves*. Invent. Math. **142**(2000), no. 1, 17–63.

[9] Y. Hachimori and K. Matsuno. *An analogue of Kida's formula for the Selmer groups of elliptic curves*. J. Algebr. Geom. **8**(1999), no. 3, 581–601.

[10] A. Iovita and R. Pollack, *Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields*. J. Reine Angew. Math. **2006**(2006), no. 598, 71–103.

[11] J. W. Jones. *Iwasawa L-functions for multiplicative abelian varieties*. Duke Math. J. **59**(1989), no. 2, 399–420.

[12] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*. Astérisque **295**(2004), 117–290.

[13] B. D. Kim, *The Iwasawa invariants of the plus/minus Selmer groups*. Asian J. Math. **13**(2009), no. 2, 181–190.

[14] B. D. Kim, *The plus/minus Selmer groups for supersingular primes*. J. Aust. Math. Soc. **95**(2013), no. 2, 189–200.

[15] B. D. Kim, *Signed-selmer groups over the $\mathbb{Z}_p^2$-extension of an imaginary quadratic field*. Canad. J. Math. **66**(2014), no. 4, 826–843.

[16] T. Kitajima and R. Otsuki, *On the plus and the minus Selmer groups for elliptic curves at supersingular primes*. Tokyo J. Math. **41**(2018), no. 1, 273–303.

[17] S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*. Invent. Math. **152**(2003), no. 1, 1–36.

[18] M. Kurihara, *The Iwasawa theory of elliptic curves that have supersingular reduction. Algebraic number theory and related topics (Kyoto, 2000)*. Surikaisekikenkyusho Kokyuroku **1154**(2000), 33–43.

[19] M. Kurihara, *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I*. Invent. Math. **149**(2002), no. 1, 195–224.

[20] A. Lei and M. F. Lim, *Mordell-Weil ranks and Tate-Shafarevich groups of elliptic curves with mixed-reduction type over cyclotomic extensions*. Int. J. Number Theory. Preprint, (2021). arXiv:1911.10643

[21] A. Lei and M. F. Lim, *Akashi series of signed Selmer groups of elliptic curves with semistable reduction at primes above p*. Preprint, 2021. arXiv:2001.09304

[22] A. Lei, D. Loeffler, and S. L. Zerbes, *Wach modules and Iwasawa theory for modular forms*. Asian J. Math. **14**(2010), no. 4, 475–528.

[23] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*. Invent. Math. **18**(1972), nos. 3–4, 183–266.

[24] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*. Invent. Math. **84**(1986), no. 1, 1–48.

[25] F. A. E. Nuccio and R. Sujatha, *Residual supersingular Iwasawa theory and signed Iwasawa invariants*. In Press, Rendiconti del Seminario Matematico della Universita di Padova (2021). arXiv:1911.10649

[26] B. Perrin-Riou, *Théorie d'Iwasawap-adique locale et globale*. Invent. Math. **99**(1990), no. 1, 247–292.

[27] B. Perrin-Riou, *Théorie d'Iwasawa et hauteurs p-adiques*. Invent. Math. **109**(1992), no. 1, 137–185.

[28] R. Pollack, *On the p-adic L-function of a modular form at a supersingular prime*. Duke Math. J. **118**(2003), no. 3, 523–558.

[29] G. Ponsinet, *On the structure of signed Selmer groups*. Math. Zeitschrift **294**(2020), no. 3, 1635–1658.

[30] A. Ray and R. Sujatha, *Euler Characteristics and their Congruences in the Positive Rank Setting*. Canad. Math. Bull. **64**(2021), no. 1, 228–245.

[31] K. Rubin, *The main conjectures of Iwasawa theory for imaginary quadratic fields*. Invent. Math. **103**(1991), no. 1, 25–68.

[32] P. Schneider, *p-adic height pairings I*. Invent. Math. **69**(1982), no. 3, 401–409.
[33] P. Schneider, *p-adic height pairings. II*. Invent. Math. **79**(1985), no. 2, 329–374.
[34] F. Sprung, *Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures*. J. Number Theory **132**(2012), no. 7, 1483–1506.
[35] F. Sprung, *A formulation of p-adic versions of the Birch and Swinnerton-Dyer conjectures in the supersingular case*. Res. Number Theory **1**(2015), no. 1, 17.
[36] L. C. Washington, *Introduction to cyclotomic fields*. Vol. 83. Springer Science & Business Media, Berlin, 1997.
[37] S. L. Zerbes, *Generalised Euler characteristics of Selmer groups*. Proc. Lond. Math. Soc. **98**(2008), no. 3, 775–796.

Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada
e-mail: anweshray@math.ubc.ca sujatha@math.ubc.ca