EULER CHARACTERISTICS AND THEIR CONGRUENCES FOR MULTI-SIGNED SELMER GROUPS

ANWESH RAY AND R. SUJATHA

Abstract. The notion of the truncated Euler characteristic for Iwasawa modules is a generalization of the usual Euler characteristic to the case when the cohomology 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 $\text{Gal}(\overline{F}/F)$-modules $E_1[p]$ and $E_2[p]$ are irreducible and isomorphic. We compare the Iwasawa invariants of certain primitive 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 $\mathbb{Z}_p^n$-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 [26] and Greenberg [8] initiated the Iwasawa theory of $p$-ordinary elliptic curves $E$ defined over $\mathbb{Q}$. The main object of study is the $p^\infty$-Selmer group over the cyclotomic $\mathbb{Z}_p$-extension, denoted $\text{Sel}(E/\mathbb{Q}^{\text{cyc}})$. Let $\Gamma$ 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 $\text{Sel}(E/\mathbb{Q}^{\text{cyc}})$ is cotorsion as a module over the Iwasawa algebra $\mathbb{Z}_p[[\Gamma]]$. This is now a celebrated theorem of Kato [14].

The corresponding theory for $p$-supersingular elliptic curves was initiated by Perrin-Riou, in [29] and has since gained considerable momentum, see [20][21][19][23][25][22][39][16][18]. If $E$ has supersingular reduction at $p$, then $\text{Sel}(E/\mathbb{Q}^{\text{cyc}})$ 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 [29]. These signed Selmer groups are cotorsion over $\mathbb{Z}_p[[\Gamma]]$.

Suppose $E$ is an elliptic curve defined over a number field $F$. Let $\Sigma_p$ denote the set of primes of $F$ above $p$. In the case when $E$ has good reduction at all primes in $\Sigma_p$, and $F_v \cong \mathbb{Q}_p$ for all $v \in \Sigma_p$ such that $E$ is supersingular at $v$, generalizations of the plus/minus Selmer groups have been studied in [15][28]. The case where $E$ has semistable reduction at the primes in $\Sigma_p$ (i.e. good ordinary, multiplicative or good supersingular) has also been considered, see [23][24]. In this paper, we assume that $E$ has semistable reduction at the primes in $\Sigma_p$. In this mixed-reduction setting, a plethora of Selmer groups depending on the reduction-types at the primes in $\Sigma_p$ can be defined. This collection of Selmer groups is referred to as the multi-signed Selmer groups.
Denote by $\Sigma_{ss}(E) = \{p_1, \ldots, p_d\}$ the set of primes of $F$ above $p$ at which $E$ has good supersingular reduction. Associated to each vector $\xi \in \{+, -\}^d$, there is a multi-signed Selmer group $\text{Sel}^\xi(E/F_{\text{cyc}})$, defined in section 2. There are $2^d$ vectors $\xi$ 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 [11], 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 $\Sigma_0$ 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 $\Sigma_0$-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 B.D. Kim in [17] and Ponsinet [32].

In this paper, the above mentioned results of Greenberg-Vatsal and B.D. Kim are generalized to the mixed reduction setting. It is shown that if the $\mu$-invariant of a certain imprimitive multi-signed Selmer group of $E_1$ is zero, then the $\mu$-invariant of the imprimitive multisigned Selmer group of $E_2$ is also zero. Further, it is shown that if these $\mu$-invariants are both zero, then the imprimitive $\lambda$-invariants match up. The reader may refer to Theorem 4.5 for the precise statement. In fact, we are able to do 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. B.D. Kim, Ponsinet). This is due to the fact that we show that an optimal set of primes $\Sigma_1$ may be chosen so that the imprimitive Iwasawa invariants match with respect to $\Sigma_1$. The set of primes $\Sigma_1$ is optimal in the sense that it is smaller than the full set of primes $\Sigma_0$ considered by Greenberg-Vatsal, B.D. Kim and Ponsinet, defined in the previous paragraph.

The Euler characteristic of the $p$-primary Selmer group an elliptic curve over $\mathbb{Q}$ with $p$-ordinary reduction may be defined when the Mordell Weil group 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. Leveraging our results on $\mu$-invariants and imprimitive $\lambda$-invariants, we prove congruence relations for the truncated Euler characteristics of multi-signed Selmer groups of $p$-congruent elliptic curves. First, this is done over the cyclotomic $\mathbb{Z}_p$-extension of $F$ (cf. Theorem 5.5). 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 $\Sigma_1$. The smaller the set of primes $\Sigma_1$, the more refined the congruence relation between truncated Euler characteristics is. This is why it is of considerable importance that the set of primes $\Sigma_1$ be carefully chosen to be as small as possible. Next,
we extend such results to the multi-signed Selmer groups of certain $\mathbb{Z}_p^m$-extensions and we compare the Akashi series for $p$-congruent elliptic curves over such $\mathbb{Z}_p^m$-extensions (cf. Theorem 6.7). Our results are informed by explicit examples which are listed in section 7.

Acknowledgements: The second author gratefully acknowledges support from NSERC Discovery grant 2019-03987.

2. Preliminaries

Throughout, we fix an odd prime number $p$ and number field $F$. Let $F^{\text{cyc}}$ be the cyclotomic $\mathbb{Z}_p$-extension of $F$. Denote by $\Sigma_p$ the set of primes of $F$ above $p$. Let $E$ be an elliptic curve over $F$ and denote by $\Sigma_{\text{ns}}(E) = \{p_1, \ldots, p_d\}$ the set of primes in $\Sigma_p$ at which $E$ has supersingular reduction. Let $\mathcal{F}_\infty/F$ be a Galois extension of $F$ containing $F^{\text{cyc}}$ such that $\text{Gal}(\mathcal{F}_\infty/F) \simeq \mathbb{Z}_p^m$ for an integer $m \geq 1$. Set $G := \text{Gal}(\mathcal{F}_\infty/F)$, $H := \text{Gal}(\mathcal{F}_\infty/F^{\text{cyc}})$ and let $\Gamma$ be the Galois group $\text{Gal}(F^{\text{cyc}}/F)$, which is identified with $G/H$. Associated to any pro-$p$ group $G$, the Iwasawa algebra $\mathbb{Z}_p[[G]]$ is the inverse limit $\lim_{\rightarrow} \mathbb{Z}_p[G/U]$, where $U$ ranges over all open normal subgroups of $G$. 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 $\text{Gal}(\mathcal{F}_n/F) \simeq (\mathbb{Z}/p^n\mathbb{Z})^m$. We introduce the following hypothesis on the elliptic curve $E$.

**Hypothesis 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 $\text{Gal}(\overline{F}/F)$-module.
3. For every prime $v \in \Sigma_{\text{ns}}(E)$, the completion $F_v$ is isomorphic to $\mathbb{Q}_p$.
4. For $v \in \Sigma_{\text{ns}}(E)$, 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 $v \in \Sigma_{\text{ns}}(E)$.

**Hypothesis 2.** Let $E$ be an elliptic curve over $F$ satisfying Hypothesis 1. We introduce a hypothesis on the tuple $(E, \mathcal{F}_\infty)$.

1. The extension $\mathcal{F}_\infty/F$ is unramified away from a finite set of primes.
2. Let $p_i|p$ be a prime of $F$ at which $E$ has supersingular reduction. Let $n \geq 1$ and let $\eta$ be a prime of $\mathcal{F}_n$ above $p_i$. 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 $n$-th layer in the cyclotomic $\mathbb{Z}_p$-extension of $K$.

The condition 2 ensures that the signed norm groups of $E$ over $\mathcal{F}_{n,\eta}$ may be defined. Thus, the condition is required in defining multi-signed Selmer groups for the extension $\mathcal{F}_\infty/F$, see Definition 2.1. The reader is referred to example 7.2 wherein a $\mathbb{Z}_p^2$-extension $\mathcal{F}_\infty/F$ is considered for which condition 2 is satisfied. For an elliptic curve $E$ and $\mathbb{Z}_p^m$-extension $\mathcal{F}_\infty$ satisfying the above hypotheses, we introduce the multisigned Selmer groups. We introduce local conditions at each of the primes $p_i \in \Sigma_{\text{ns}}(E)$. By Hypothesis 1, the local field $F_{p_i}$ is isomorphic to $\mathbb{Q}_p$. Denote by $\widetilde{E}_{p_i}$ the formal group of $E$ over $F_{p_i}$. For any algebraic extension $L$ of $F_{p_i} \simeq \mathbb{Q}_p$, denote by $\widetilde{E}_{p_i}(L) := \widetilde{E}_{p_i}((m_L))$, where
m_L is the maximal ideal of O_L. Let K be a finite unramified extension of Q_pr and K_cyc the cyclotomic 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 groups:

\[ \hat{E}^+_p(K_n) := \left\{ \begin{array}{l} P \in \hat{E}_p(K_n) \mid \text{tr}_{n/m+1}(P) \in \hat{E}_p(K_m), \text{ for } 0 \leq m < n \text{ and } m \text{ even} \end{array} \right\}, \]

\[ \hat{E}^-_p(K_n) := \left\{ \begin{array}{l} P \in \hat{E}_p(K_n) \mid \text{tr}_{n/m+1}(P) \in \hat{E}_p(K_m), \text{ for } 0 \leq m < n \text{ and } m \text{ odd} \end{array} \right\}, \]

where tr_{n/m+1} : \hat{E}_p(K_n) \to \hat{E}_p(K_{m+1}) denotes the trace map with respect to the formal group law on \( \hat{E}_p \).

Let \( \xi = (\xi_1, \ldots, \xi_d) \in \{+, -, 0\}^d \) be a multi-signed vector, so that each component \( \xi_i \) is either a + or - sign. For each finite prime \( v \notin \Sigma_{ss}(E) \), and each integer \( n \geq 1 \), set

\[ H_v(F_n, E[p^\infty]) := \prod_{\eta|v} \frac{H^1(F_{n, \eta}, E[p^\infty])}{E(F_{n, \eta}) \otimes \mathbb{Q}_p / \mathbb{Z}_p}, \]

where \( \eta \) runs through the primes of \( F_n \) above \( v \). For each prime \( p_i \in \Sigma_{ss}(E) \), set

\[ H^\pm_{p_i}(F_n, E[p^\infty]) := \prod_{\eta|p_i} \frac{H^1(F_{n, \eta}, E[p^\infty])}{\hat{E}^\pm_{p_i}(F_{n, \eta}) \otimes \mathbb{Q}_p / \mathbb{Z}_p}. \]

Let \( \eta \) be a prime of \( F_\infty \) above \( p_i \). By assumption (2), \( F_{n, \eta} \) is isomorphic to \( K_n \) for some finite unramified extension \( K \) over \( \mathbb{Q}_p \). Thus the norm groups \( \hat{E}^\pm_{p_i}(F_{n, \eta}) \) are defined. We now come to the definition of the multisigned Selmer groups.

**Definition 2.1.** Let \( d \) be the cardinality of \( \Sigma_{ss}(E) \) and let \( \xi = (\xi_1, \ldots, \xi_d) \) be a multi-signed vector, so that each component \( \xi_i \) is either a + sign or - sign. Let \( \Sigma \) be a finite primes of \( F \) containing \( \Sigma_p \) and the primes at which \( E \) has bad reduction. Let \( p_1, \ldots, p_d \) be the primes in \( \Sigma_{ss}(E) \). For \( i = 1, \ldots, d \), let \( \hat{H}^\pm_{p_i}(F_n, E[p^\infty]) \) be the group defined above, see (2.2). The multi-signed Selmer group \( \text{Sel}^\xi(E/F_n) \) is the kernel of the map:

\[ \Phi^\xi_{E,F_n} : H^1(F_n, E[p^\infty]) \to \prod_{v \in \Sigma \setminus \Sigma_{ss}(E)} H_v(F_n, E[p^\infty]) \times \prod_{i=1}^d \hat{H}^\xi_{p_i}(F_n, E[p^\infty]). \]

Let \( \text{Sel}^\xi(E/F_\infty) \) be the direct limit \( \lim_{\longrightarrow \, F_n} \text{Sel}^\xi(E/F_n) \) and write \( X^\xi(E/F_\infty) \) for its Pontryagin-dual.

For practical purposes, it is convenient to work with an alternative description of \( \text{Sel}^\xi(E/F_cyc) \).

Let 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 Gal(\( F_v/F_0 \))-modules:

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

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 \( 1_v := \text{Gal}(\mathbb{F}_v/F_v) \) acts via a finite
order quotient. In fact, $D_v$ is specified as follows:

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

where $\phi$ is an unramified 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 [3, p. 150] and [11, section 2].

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

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

where $\eta$ runs through the primes of $F^{\text{cyc}}$ above $p_i$. For $v \in \Sigma \setminus \Sigma_{ss}(E)$, set

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

where $I_\eta$ is the inertia subgroup of $\text{Gal}(F^{\text{cyc}}_\eta/F^{\text{cyc}})$. The Selmer group $\text{Sel}^1(E/F^{\text{cyc}})$ coincides with the kernel of the restriction map

\[
\Phi^1_{E,F^{\text{cyc}}} : H^1(F^{\text{cyc}}, E[p^\infty]) \to \prod_{v \in \Sigma \setminus \Sigma_{\text{ss}}(E)} \mathcal{H}_v(F^{\text{cyc}}, E[p^\infty]) \times \prod_{i=1}^d \mathcal{H}^i_{p_i}(F^{\text{cyc}}, E[p^\infty]).
\]

For further details, see [11, p.32,42] and the discussion in [8, section 5]. Let $\Sigma_0$ be a finite set of primes of $F$ which does not contain any prime $v \in \Sigma_p$. The $\Sigma_0$-imprimitive Selmer group $\text{Sel}^{\Sigma_0,\dagger}(E/F^{\text{cyc}})$ is the kernel of the restriction map

\[
\Phi^{\Sigma_0,\dagger}_{E,F^{\text{cyc}}} : H^1(F^{\text{cyc}}, E[p^\infty]) \to \prod_{v \in \Sigma \setminus (\Sigma_{\text{ss}}(E) \cup \Sigma_0)} \mathcal{H}_v(F^{\text{cyc}}, E[p^\infty]) \times \prod_{i=1}^d \mathcal{H}^i_{p_i}(F^{\text{cyc}}, E[p^\infty]).
\]

The Pontryagin dual of $\text{Sel}^{\Sigma_0,\dagger}(E/F^{\text{cyc}})$ is denoted by $X^{\Sigma_0,\dagger}(E/F^{\text{cyc}})$. The next Proposition follows from [11] Proposition 2.1 and [24] Proposition 4.6.

**Proposition 2.2.** Assume that the Selmer group $\text{Sel}^{\Sigma_0,\dagger}(E/F^{\text{cyc}})$ is cotorsion as a $\mathbb{Z}_p[[\Gamma]]$-module. Then, the maps $\Phi^1_{E,F^{\text{cyc}}}$ and $\Phi^{\Sigma_0,\dagger}_{E,F^{\text{cyc}}}$ are surjective.

Thus we have a short exact sequence relating the $\Sigma_0$-imprimitive Selmer group $\text{Sel}^{\Sigma_0,\dagger}(E/F^{\text{cyc}})$ with the Selmer group $\text{Sel}^1(E/F^{\text{cyc}})$

\[
0 \to \text{Sel}^1(E/F^{\text{cyc}}) \to \text{Sel}^{\Sigma_0,\dagger}(E/F^{\text{cyc}}) \xrightarrow{\Phi^{\Sigma_0,\dagger}_{E,F^{\text{cyc}}}} \prod_{v \in \Sigma_0} \mathcal{H}_v(F^{\text{cyc}}, E[p^\infty]) \to 0.
\]
Choose a topological generator \( \gamma \) of \( \Gamma \) and identify \( \gamma - 1 \) with \( T \) in choosing an isomorphism \( \mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]] \). A polynomial \( f(T) \in \mathbb{Z}_p[T] \) is said to be distinguished if it is a monic polynomial and all non-leading coefficients are divisible by \( p \). By the structure theorem of finitely generated torsion \( \mathbb{Z}_p[[T]] \)-modules, there is a pseudo-isomorphism

\[
\mathcal{X}(E/F)_{\text{cyc}} \cong \bigoplus_{i=1}^{n} \mathbb{Z}_p[[T]]/(f_i(T)) \oplus \bigoplus_{j=1}^{m} \mathbb{Z}_p[[T]]/(p^j).
\]

For \( i = 1, \ldots, n \), the elements \( f_i(T) \) above are distinguished polynomials and the product \( f^\dagger(E) := p^{\sum_i \mu_i} \prod_i f_i(T) \) is called the characteristic polynomial. The signed Iwasawa invariants are defined by \( \lambda^\dagger_E := \deg f^\dagger(T) \) and \( \mu^\dagger_E := \sum_{j=1}^{m} \mu_j \). Denote by \( f_E, \lambda_E, \mu_E \) the characteristic polynomial, \( \lambda \)-invariant and \( \mu \)-invariant of the imprimitive Selmer group \( \mathcal{X}(E/F)_{\text{cyc}} \).

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 [4, section 3] and [41]. 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 Mordell-Weil group is finite. This definition does not extend to the case when the Mordell-Weil group of \( E \) is infinite. The natural substitute is the truncated Euler characteristic.

**Definition 3.1.** Let \( M \) be a discrete \( p \)-primary \( \Gamma \)-module let \( \phi_M \) be the natural map

\[
\phi_M : H^0(\Gamma, M) = M^\Gamma \rightarrow M_\Gamma \cong H^1(\Gamma, M)
\]

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

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

**Lemma 3.2.** Assume that \( M \) is a discrete \( \mathbb{Z}_p[[\Gamma]] \)-module. 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 $M^\Gamma$ is dual to $X^\Gamma$ and the quotient $M_\Gamma$ is dual to $X^\Gamma$. By an application of the structure theorem for finitely generated torsion $\mathbb{Z}_p[\Gamma]$-modules, there is a pseudoisomorphism

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

for some elements $f_i(T) \in \mathbb{Z}_p[[\Gamma]]$. The module $X_\Gamma$ may be identified with $X/TX$ and $X^\Gamma$ is the kernel of the multiplication by $T$ map $\times T : X \to X$. It is easy to see that the groups $X_\Gamma$ and $X^\Gamma$ are finite precisely when $T \nmid f_i(T)$ for $i = 1, \ldots, m$. Therefore, $X_\Gamma$ and $X^\Gamma$ 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 $p^\infty$-torsion submodule of $X$. Let $f_1(T), \ldots, f_n(T)$ 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 $\phi_M$ 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 [41, Lemma 2.11]. □

Let $f_M(T)$ be the characteristic polynomial of the Pontryagin dual of $M$ and write $f_M(T) = T^{r_M}g_M(T)$, where $g_M(0) \neq 0$. Let $| \cdot |_p$ denote the absolute value on $\mathbb{Q}_p$ normalized by $|p|_p = p^{-1}$. When both $\ker(\phi_M)$ and $\cok(\phi_M)$ 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 $\phi_M$ are finite, then

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

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

**Proof.** The assertion follows from [41, Lemma 2.11]. □

Evidently, it follows that $\chi_t(\Gamma, M) = p^N$, where $N \in \mathbb{Z}_{\geq 0}$. Let $\mu_M$ (resp. $\lambda_M$) denote its $\mu$-invariant (resp. $\lambda$-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) $\chi_t(\Gamma, M) = 1$,
(b) $\mu_M = 0$ and $\lambda_M = r_M$.  

7
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 $T \not| g_M(T)$. 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 $g_M(T) = 1$ 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 that $g_M(T)$ is a constant polynomial and hence, $g_M(T) = 1$. By Lemma 3.4

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

\[\square\]

Let $r^E_E$ denote the order of vanishing of $f^E_E(T)$ at $T = 0$, and write

$$f^E_E(T) = p^{r^E_E} g^E_E(T).$$

Note that $g^E_E(0) \neq 0$. According to Lemma 3.4, the truncated Euler characteristic $\chi^E_t(\Gamma, E) := \chi_t(\Gamma, \text{Sel}^E(E/F_{\text{cyc}}))$ is determined by the constant term of $g^E_E(T)$. By Lemma 3.4 if the truncated Euler characteristic is defined, then $\chi^E_t(\Gamma, E) = 1$ if and only if $\mu^E_E = 0$ and $\lambda^E_E = r^E_E$.

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 [34] [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, Tate and Teitelbaum [27] 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 $L(E/\mathbb{Q}, T)$ 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 plus and minus $p$-adic $L$-functions was formulated by Sprung [40]. 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 $L_p(E)$ to denote the $L$-invariant associated to the Galois representation on the $p$-adic Tate module of $E$ (see [11] p. 407). The $p$-adic height pairing (cf. [36] and [37]) is a $p$-adic analog of the usual height pairing. This pairing is
conjectured to be non-degenerate (cf. [37]) and the $p$-adic regulator $R_p(E/\mathbb{Q})$ is defined to be the determinant of this pairing. Let $\kappa$ denote the $p$-adic cyclotomic character. Fix a branch of the $p$-adic logarithm and set $R_\gamma(E/\mathbb{Q})$ 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 non-singular 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 $a_t(E)$ be the $l$-th 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 $r^{an}_E$ denote the order of vanishing of $L(E/\mathbb{Q}, T)$ at $T = 0$.

**Theorem 3.6.** (Perrin-Riou [30], Schneider [37], Jones [13]) Suppose that $E$ has either good ordinary reduction or multiplicative reduction at $p$. Assume that:

1. the truncated Euler-characteristic $\chi_t(\Gamma, E)$ is defined,
2. the $p$-adic regulator $R_p(E/\mathbb{Q})$ is non-zero,
3. $\textup{III}(E/\mathbb{Q})[p^{\infty}]$ 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 the analytic rank $r^{an}_E$ is equal to $r$. If $E$ has split multiplicative reduction at $p$, then the analytic rank $r^{an}_E$ is equal to $r + 1$.

(b) If $E$ has either good ordinary reduction at $p$ or non-split multiplicative reduction at $p$, then

$$\chi_t(\Gamma, E) \sim \epsilon_p(E) \times \frac{R_\gamma(E/\mathbb{Q}) \times \#(\textup{III}(E/\mathbb{Q})[p^{\infty}]) \times \tau(E)}{\#(E(\mathbb{Q})_{\text{tors}})^2}.$$  

Here $\epsilon_p(E)$ is set to be $(1 - \frac{1}{\alpha})^s$, where $\alpha$ 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 $L$-invariant $L_{\gamma}(E)$ plays a role and we have:

$$\chi_t(\Gamma, E) \sim \frac{L_p(E)}{\log_p(\kappa(\gamma))} \times \frac{R_\gamma(E/\mathbb{Q}) \times \#(\textup{III}(E/\mathbb{Q})[p^{\infty}]) \times \tau(E)}{\#(E(\mathbb{Q})_{\text{tors}})^2}.$$  

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 [11]. Denote by $T_p(E) := \varprojlim_n E[p^n]$ the $p$-adic Tate-module equipped with natural Gal($\overline{F}/F$) action and set $V_p(E) := T_p(E) \otimes \mathbb{Q}_p$. At a prime $v \in \Sigma_p \setminus \Sigma_{ss}(E)$, 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 character.

**Hypothesis 3.** Let $E$ be an elliptic curve over $F$ which satisfies Hypothesis \([1]\). Let $\Sigma_{ss}(E) = \{p_1, \ldots, p_d\}$ be the set of primes $v|p$ of $F$ at which $E$ has supersingular reduction. Let $\hat{v} \in \{+, -, \}^d$ be a signed vector. Then $(E, \hat{v})$ satisfies the following conditions:

1. The Selmer group $\text{Sel}^1(E/F^cyc)$ is $\mathbb{Z}_p[[\Gamma]]$-cotorsion.
2. The truncated Euler characteristic $\chi^1_\Gamma(\Gamma, E)$ is defined. In other words, the natural map $\phi^1_\Gamma : \text{Sel}^1(\Gamma, E) \rightarrow \text{Sel}^1(\Gamma, E)^\Gamma$ has finite kernel and cokernel.

Let $E_1$ and $E_2$ be $p$-congruent elliptic curves over $F$. It follows from the proof of \([28, \text{Proposition } 3.9]\) that $\Sigma_{ss}(E_1)$ is equal to $\Sigma_{ss}(E_2)$. Set $\Sigma_{ss} = \{p_1, \ldots, p_d\}$ to denote the set of supersingular primes $v|p$ of $E_1$ and $E_2$, and let $\hat{v} \in \{+, -, \}^d$ be a signed vector. We introduce the following hypothesis on the triple $(E_1, E_2, \hat{v})$.

**Hypothesis 4.** Hypothesis \([3]\) holds for both $(E_1, \hat{v})$ and $(E_2, \hat{v})$.

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

$$
H^\pm_v(F^cyc, E_i[p]) := \frac{H^1(F^cyc_{\eta_v}, E_i[p])}{E_i^\pm(F^cyc_{\eta_v})/pE_i^\pm(F^cyc_{\eta_v})}.
$$

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

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

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 $v \not| p$ 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 $F$ and $\Sigma_1(E)$ denote the subset of primes of $F$ such that (i) $v \not| p$, (ii) $v|(\mathcal{N}_E/\overline{\mathcal{N}}_E)$, (iii) if $\mu_p$ 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) $v \not| p$, (ii) $v|(\mathcal{N}_E/\overline{\mathcal{N}}_E)$. 

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

$$\Phi^{\Sigma_1,\dagger}_{E_i} : H^1(F_{\Sigma}/F^{\text{cyc}}, E_i[p]) \to \prod_{\Sigma/\left(\Sigma_{\text{ss}} \cup \Sigma_1\right)} \mathcal{H}_v(F^{\text{cyc}}, E_i[p]) \times \prod_{j=1}^d \mathcal{H}_v^{\dagger_j}(F^{\text{cyc}}, E_i[p]).$$

**Proposition 4.2.** Let $E_1$ and $E_2$ be elliptic curves over $F$ which are $p$-congruent. Let $\xi$ be a signed vector and assume that $(E_1, E_2, \xi)$ satisfies Hypothesis (4). Let $\Sigma_1$ 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 $\text{Sel}^{\Sigma_1,\dagger}(E_1[p]/F^{\text{cyc}}) \simeq \text{Sel}^{\Sigma_1,\dagger}(E_2[p]/F^{\text{cyc}})$.

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

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

This is clear for $v \in \Sigma \setminus \Sigma_{\text{ss}}$. For $v \in \Sigma_{\text{ss}}$, this assertion follows from the arguments in [17, p. 186]. □

**Proposition 4.3.** Let $E$ be an elliptic curve over $F$ satisfying Hypothesis (1) and $\xi$ a signed vector. Let $\Sigma_0$ be a finite set of primes $v \nmid p$ containing $\Sigma_1(E)$. Then, there is an isomorphism $\text{Sel}^{\Sigma_0,\dagger}(E/F^{\text{cyc}})[p] \simeq \text{Sel}^{\Sigma_0,\dagger}(E[p]/F^{\text{cyc}})$.

**Proof.** Let $\Sigma$ be a finite set of primes containing $\Sigma_0$, the primes at which $E$ has bad reduction and $\Sigma_p$. We consider the diagram relating the two Selmer groups:

\[
\begin{array}{cccccc}
0 & \to & \text{Sel}^{\Sigma_0,\dagger}(E[p]/F^{\text{cyc}}) & \longrightarrow & H^1(G_{\Sigma}(F^{\text{cyc}}), E[p]) & \longrightarrow & \text{im } \Phi^{\Sigma_0,\dagger}_E & \longrightarrow & 0 \\
\downarrow f & & \downarrow g & & \downarrow h & & \\
0 & \to & \text{Sel}^{\Sigma_0,\dagger}(E/F^{\text{cyc}})[p] & \longrightarrow & H^1(G_{\Sigma}(F^{\text{cyc}}), E[p^{\infty}])[p] & \longrightarrow & \text{im } \Phi^{\Sigma_0,\dagger}_E[p] & \longrightarrow & 0.
\end{array}
\]

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

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

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

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

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

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

$$h_v : \mathcal{H}_v^{\dagger_v}(F^{\text{cyc}}, E[p]) \to \mathcal{H}_v^{\dagger_v}(F^{\text{cyc}}, E[p^{\infty}]).$$
We show that the maps $h_v$ are injective for $v \in \Sigma \setminus \Sigma_0$. This has been shown in the proof of [11 Proposition 2.8] for $v \in \Sigma_p \setminus \Sigma_{ss}$ and in [17 Proposition 2.10] for $v \in \Sigma_{ss}$. Therefore, it remains to consider primes $v \notin \Sigma_0 \cup \Sigma_p$.

First consider the case when $p \geq 5$. Consider two further cases, first consider the case when $v \nmid (N_E / \mathcal{N}_E)$. In this case, the injectivity of $h_v$ follows from the proof of [17 Lemma 4.1.2]. Next, consider the case when $v \mid (N_E / \mathcal{N}_E)$. Since $v$ is not contained in $\Sigma_0$, it follows that $\mu_p$ is contained in $F_v$ and $E$ has either non-split multiplicative reduction or additive reduction at $v$. In this case, the injectivity of $h_v$ follows from [12 Proposition 5.1]. When $p = 3$, the injectivity of $h_3$ follows from the same reasoning as above. \hfill $\square$

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

**Proof.** We adapt the proof of [9 Proposition 4.14], which is due to Greenberg. Let $\Sigma$ 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:

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

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

By Proposition [2.2] it follows that

$$\text{Sel}^{\text{rel}}_{\Sigma_0}(E/F_{\text{cyc}}) / \text{Sel}^{\Sigma_0}(E/F_{\text{cyc}}) \cong \prod_{i=1}^d H^{1}_{\eta_i}(F_{\text{cyc}}, E[p^\infty]).$$

For $i = 1, \ldots, d$, it follows from standard arguments (see the proof of [17 Proposition 2.11]) that $H^{1}_{\eta_i}(F_{\text{cyc}}, E[p^\infty])$ is isomorphic to $\mathbb{Z}_p[[\Gamma]]$. By [11 Lemma 2.6], it suffices to show that $\text{Sel}^{\text{rel}}(E/F_{\text{cyc}})$ has no proper finite index $\mathbb{Z}_p[[\Gamma]]$-submodules. Since $\text{Sel}^{\text{str}}_{\Sigma_0}(E/F_{\text{cyc}})$ is a quotient of $\text{Sel}^{\Sigma_0}(E/F_{\text{cyc}})$, it is $\mathbb{Z}_p[[\Gamma]]$-torsion.

Recall that $\kappa$ 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 $\Gamma$ is pro-$p$, it follows that $E(F)[p] = 0$, and as a result, $H^0(F_{\text{cyc}}, A_s) = 0$. Since $\Gamma$ is pro-$p$ it follows from standard arguments that $H^0(F, A_s) = 0$ for all $s$. For a subfield $K$ of $F_{\text{cyc}}$, and $v$ a prime of $F$ which does not divide $p$, set $\mathcal{H}_v(K, A_s)$ to be the product $\prod_{\eta \mid v} H^1(K_{\eta}, A_s)/(A_s(K_{\eta}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$, where $\eta$ ranges the finitely many primes of $K$ above $v$. Set $P^{\Sigma_0}(K, A_s)$ to be the product

$$P^{\Sigma_0}(K, A_s) := \prod_{v \in \Sigma \setminus (\Sigma_0 \cup \Sigma_p)} \mathcal{H}_v(K, A_s).$$
and set $P^{\Sigma,\text{str}}(K, A_s)$ to be the product

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

Let $S_{M_s}^{\text{rel}}(K)$ and $S_{M_s}^{\text{str}}(K)$ be the Selmer groups defined as follows

$$S_{M_s}^{\text{rel}}(K) := \ker \left( H^1(F_\Sigma/F_s, A_s) \to P^{\Sigma,\text{rel}}(K, A_s) \right),$$

$$S_{M_s}^{\text{str}}(K) := \ker \left( H^1(F_\Sigma/F_s, A_s) \to P^{\Sigma,\text{str}}(K, A_s) \right).$$

Since $\text{Sel}^{\text{str}}(E/F^{\text{cyc}})$ is $\mathbb{Z}_p[[\Gamma]]$-cotorsion, we have that $S_{A_s}^{\text{str}}(F^{\text{cyc}})^\Gamma$ is finite for all but finitely many values of $s$. Hence, $S_{A_s}^{\text{str}}(F)$ is finite for all but finitely many values of $s$. We set $M = A_s$, and in accordance with the proof of [9, Proposition 4.14], $M^* = A_{-s}$. Denote by $S_M(F)$ the Selmer group defined by the relaxed conditions $S_{A_s}^{\text{rel}}(F)$ and in accordance with the discussion on [9, p. 100], $S_{M^*}(F)$ is the strict Selmer group $S_{A_{-s}}^{\text{str}}(F)$. 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 $H^1(F_\Sigma/F, M) \to P^{\Sigma,\text{rel}}(K, M)$ is surjective (see [9, Proposition 4.13]). It follows from the proof of [9, Proposition 4.14] that $\text{Sel}^{\text{rel}}(E/F^{\text{cyc}})$ has no proper finite index $\mathbb{Z}_p[[\Gamma]]$-submodules. This completes the proof. □

Recall that for $i = 1, 2$, the $\mu$-invariant (resp. $\lambda$-invariant) of the Selmer group $\text{Sel}^{\Sigma_i,\dagger}(E_i/F^{\text{cyc}})$ is denoted $\mu_{E_i}^{\Sigma_i,\dagger}$ (resp. $\lambda_{E_i}^{\Sigma_i,\dagger}$).

**Theorem 4.5.** Let $E_1$ and $E_2$ be elliptic curves over $F$ which are $p$-congruent. Let $\frac{t}{s}$ be a signed vector and assume that $(E_1, E_2, \frac{t}{s})$ satisfies Hypothesis [4] Let $\Sigma_1$ be the set of primes as in Definition [1.1] Then the following assertions hold:

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

**Proof.** For $i = 1, 2$, let $M_i$ denote the Pontryagin dual of $\text{Sel}^{\Sigma_i,\dagger}(E_i/F^{\text{cyc}})$. It follows from Propositions [1.2 and 1.3 that $M_1/pM_1$ is isomorphic to $M_2/pM_2$. Note that $\mu_{E_i}^{\Sigma_1,\dagger}$ is equal to 0 if and only if $M_i/pM_i$ is finite. Thus, it follows that if $\mu_{E_1}^{\Sigma_1,\dagger}$ is zero, then so is $\mu_{E_2}^{\Sigma_1,\dagger}$.

Next, assume that $\mu_{E_1}^{\Sigma_1,\dagger}$ and $\mu_{E_2}^{\Sigma_1,\dagger}$ are both zero. Proposition [1.3] 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 $\lambda_{E_i}^{\Sigma_1,\dagger}$. Since $M_1/pM_1$ is isomorphic to $M_2/pM_2$, it follows that $\lambda_{E_1}^{\Sigma_1,\dagger}$ is equal to $\lambda_{E_2}^{\Sigma_1,\dagger}$. □

5. Congruences for Euler Characteristics

Consider elliptic curves $E_1$ and $E_2$ that are $p$-congruent and let $\Sigma^{ss} = \{p_1, \ldots, p_d\}$ 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 $\frac{t}{s} \in \{+, -\}^d$ be a signed vector and assume that Hypothesis [4] is satisfied for the triple $(E_1, E_2, \frac{t}{s})$. Associated to $E_1$ and $E_2$ is the set of primes $\Sigma_1$, see Definition [1.1]. In this section, it is shown that there is an explicit relationship between the multi-signed Euler characteristics $\chi_1^{\frac{t}{s}}(\Gamma, E_1)$ and $\chi_1^{\frac{t}{s}}(\Gamma, E_2)$. 

13
Let \( E \) be an elliptic curve satisfying Hypothesis (\( \square \)) and \( \Sigma_0 \) a finite set of primes \( v \nmid p \). Recall that \( r^*_E \) is the order of vanishing of the characteristic polynomial \( f^*_E(T) \) at \( T = 0 \). The following Proposition shows that the quantity \( r^*_E \) is related to the Mordell-Weil rank of \( E \) and the reduction type of \( E \) at the primes \( v \mid p \).

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

(i) the truncated Euler characteristic \( \chi^*_E(\Gamma, E) \) is defined.

(ii) The \( \mathfrak{p} \)-primary part of the Tate-Shafarevich group \( \Sha(E/F) \) is finite.

Let \( r \) be the Mordell-Weil rank of \( E \) and \( \text{sp}_E \) the number of primes \( v \mid p \) at which \( E \) has split multiplicative reduction. Then, we have that \( r \leq r_E^* \leq r + \text{sp}_E \). In particular, if there are no primes \( v \in \Sigma_p \) at which \( E \) has split multiplicative reduction, then \( r_E^* = r \).

**Proof.** Let \( \Sigma \) be a finite set of primes containing \( \Sigma_p \) and the primes at which \( E \) has bad reduction. By Lemma \ref{lem:Selmer-rank}, the multi-signed rank \( r_E^* \) is equal to the \( \mathbb{Z}_p \)-corank of \( \text{Sel}^1(E/F) \). We compare \( \text{Sel}^1(E/F) \) with the usual Selmer group \( \text{Sel}(E/F) \). Let \( \Phi_{E,F} : H^1(F_{\Sigma}/F, E[p^\infty]) \to \prod_{v \in \Sigma} H_v(F, E[p^\infty]) \) be the defining map for the Selmer group \( \text{Sel}(E/F) \). Consider the fundamental diagram

\[
\begin{array}{ccc}
0 & \longrightarrow & \text{Sel}(E/F) \\
\downarrow f & & \downarrow g \\
0 & \longrightarrow & H^1(F_{\Sigma}/F, E[p^\infty]) \\
\downarrow h & & \downarrow h \\
0 & \longrightarrow & \text{Sel}^1(E/F) \Gamma \\
\end{array}
\]

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

\[
(5.1) \quad 0 \to \text{Sel}(E/F) \to \text{Sel}^1(E/F) \to \ker h \to 0.
\]

It suffices to show that the kernel of \( h \) has corank less than or equal to \( \text{sp}_E \). For \( v \in \Sigma \setminus \Sigma_{ss} \), let \( h^*_v \) denote the natural map

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

For \( p_i \in \Sigma_{ss} \), set \( h^*_i \) denotes the map

\[
h^*_i : \mathcal{H}^*_i(F, E[p^\infty]) \to \mathcal{H}^*_i(F^\text{cyc}, E[p^\infty]).
\]

Let \( h^* \) be the product of the maps \( h^*_v \) as \( v \) ranges over \( \Sigma \). Note that the kernel of \( h \) is contained in the kernel of \( h^* \). Let \( \Sigma_{sp}(E) \) be the set of primes \( v \mid p \) at which \( E \) has split multiplicative reduction. We show that \( \ker h^*_v \) is finite if \( v \not\in \Sigma_{sp}(E) \) and of corank one for \( v \in \Sigma_{sp}(E) \). For \( v \in \Sigma \setminus \Sigma_p \), this follows from \cite{5} Lemma 3.4, for \( v \in \Sigma_p \) at which \( E \) has good ordinary reduction, it follows from \cite{5} Proposition 3.5. Next consider the case where \( v \mid p \) 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 $\varphi_v$ is an unramified character. Let $w$ be a prime of $F^{\text{cyc}}$ above $v$ and let $\Gamma_v$ denote $\text{Gal}(F^{\text{cyc}}_w/F_v)$. By Shapiro’s Lemma,
\[
H^0(\Gamma_v, \prod_{\eta|v} H^1(F^{\text{cyc}}_{\eta}, D_v)) \simeq H^0(\Gamma_v, H^1(F^{\text{cyc}}_w, D_v)).
\]

The kernel of $h'_v$ is contained in the kernel of the restriction map
\[
H^1(F_v, D_v) \to H^1(F^{\text{cyc}}_w, D_v)
\]
and by the inflation restriction sequence, the kernel of $h'_v$ is contained in $H^1(\Gamma_v, H^0(F^{\text{cyc}}_w, D_v))$. When $E$ has non-split multiplicative reduction at $v$, the character $\varphi_v$ is non-trivial and thus $H^0(F_v, D_v) = 0$. Since $\Gamma_v$ is pro-$p$, it follows that $H^0(F^{\text{cyc}}_w, D_v) = 0$ when $\varphi_v \neq 1$. On the other hand, when $\varphi_v = 1$, the Galois action on $H^0(F^{\text{cyc}}_w, D_v) \simeq \mathbb{Q}_p/\mathbb{Z}_p$ is trivial. As a result, the corank of $H^1(\Gamma_v, H^0(F^{\text{cyc}}_w, D_v))$ 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 [24, Theorem 5.3].

Putting all this together, we have that $\text{corank}_{\mathbb{Z}_p} \ker h \leq \text{sp}_E$, and thus, from the short exact sequence (5.1), we have
\[
r^+_E \leq \text{corank}_{\mathbb{Z}_p} \text{Sel}(E/F) + \text{sp}_E = r + \text{corank}_{\mathbb{Z}_p} \text{III}(E/F)[p^\infty] + \text{sp}_E.
\]
Since it is assumed that $\text{III}(E/F)[p^\infty]$ is finite, the result follows. □

We now study congruences for truncated Euler characteristics. For $v \in \Sigma_0$, set $h^{(v)}_E(T)$ to be the characteristic polynomial of the Pontryagin dual of $\mathcal{H}_v(F^{\text{cyc}}, E[p^\infty])$. Since $\text{Sel}^\dagger(E/F^{\text{cyc}})$ is $\mathbb{Z}_p[[\Gamma]]$-cotorsion, it follows from Proposition 2.2 that there is a short exact sequence:
\[
0 \to \text{Sel}^\dagger(E/F^{\text{cyc}}) \to \text{Sel}^\dagger(\Sigma_0)(E/F^{\text{cyc}}) \to \prod_{v \in \Sigma_0} \mathcal{H}_v(F^{\text{cyc}}, E[p^\infty]) \to 0.
\]
As a result, we arrive at the following relation:
\[
(5.2) \quad f_E^{\Sigma_0, \dagger}(T) = f_E(T) \prod_{l \in \Sigma_0} h^{(v)}_E(T).
\]
Recall that $V_p(E)$ is the $p$-adic vector space $T_p(E) \otimes \mathbb{Q}_p$, equipped with $\text{Gal}(\bar{F}/F)$-action. Let $P_v(E, T)$ denote the characteristic polynomial
\[
(5.3) \quad P_v(E, T) := \det \left((\text{Id} - \text{Frob}_v \chi)|_{V_p(E)^{\dagger}}\right),
\]
where $I_v$ is the inertia group at $v$. For $s \in \mathbb{C}$, set $L_s(E, s)$ to denote $P_v(E, Nv^{-s})^{-1}$, where $Nv$ denotes the norm $N_{L/Q}v$. Recall that $\gamma$ is a topological generator of $\Gamma$. Let $\rho : \Gamma \to \mu_{p^\infty}$ be a finite order character and let $\sigma_v$ denote the Frobenius at $v$. Let $P_v(E, T)$ be the element in $\mathbb{Z}_p[[\Gamma]]$ defined by the relation $P_v(E, \rho(\gamma) - 1) = P_v(E, \rho(\sigma_v)Nv^{-1})$. 

15
According to [11, Proposition 2.4], the polynomial $\mathcal{P}_v(E, T)$ generates the Pontryagin dual of $\mathcal{H}_v(F^{\text{cyc}}, E[p^\infty])$ and thus coincides with $h^{(v)}(T)$ up to a unit in $\mathbb{Z}_p[[\Gamma]]$.

**Definition 5.2.** Set $\Phi_{E, \Sigma_0}$ 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

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

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

$$g_E^{\Sigma_0, \pm}(T) = g_E^1(T) \prod_{t \in \Sigma_0} h_E^{(v)}(T).$$

One has the following result.

**Lemma 5.3.** Let $E$ be an elliptic curve satisfying Hypothesis (1) and let $\vec{\lambda}$ be a signed vector, for a finite set $\Sigma_0$ consisting of primes $v \nmid p$. Then we have the following equality:

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

**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

$$|g_E^{\Sigma_0, \pm}(0)|_p^{-1} = |g_E^1(0)|_p^{-1} \prod_{t \in \Sigma_0} |L_v(E, 1)|_p = |g_E^1(0)|_p^{-1} \times \Phi_{E, \Sigma_0}.$$ 

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

Denote the $\mu$-invariants of $\text{Sel}^E(F^{\text{cyc}})$ and $\text{Sel}^{\Sigma_0, \pm}(E/F^{\text{cyc}})$ by $\mu_E^{\pm}$ and $\mu_E^{\Sigma_0, \pm}$ respectively. Denote the $\lambda$-invariants by $\lambda_E^{\pm}$ and $\lambda_E^{\Sigma_0, \pm}$ respectively. It is easy to show that for $v \in \Sigma_0$, the $\mu$-invariant of $h^{(v)}(T)$ is equal to zero, and hence $\mu_E^{\Sigma_0, \pm}$ is equal to $\mu_E^{\pm}$.

**Lemma 5.4.** Let $E$ be an elliptic curve satisfying Hypothesis (1) and let $\vec{\lambda}$ be a signed vector. For a finite set $\Sigma_0$ consisting of primes $v \nmid p$, we have that

$$\Phi_{E, \Sigma_0} \times \chi_t(\Gamma, E) = 1 \iff \mu_E^{\pm} = 0 \text{ and } \lambda_E^{\Sigma_0, \pm} = r_E^{\pm}.$$ 

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

$$f_E^{\Sigma_0, \pm}(T) = f_E^1(T) \times \prod_{v \in \Sigma_0} h_E^{(v)}(T)$$

(see (5.2)). According to [11, Proposition 2.4], the polynomial $\mathcal{P}_v(E, T)$ generates the Pontryagin dual of $\mathcal{H}_v(F^{\text{cyc}}, E[p^\infty])$ and thus coincides with $h^{(v)}(T)$ up to a unit in $\mathbb{Z}_p[[\Gamma]]$. It

16
is easy to see that \( P_v(E, T) \) 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 \( \mu_{E}^\dagger = \mu_{E, \Sigma_0}^\dagger = 0 \).

Conversely, suppose that \( \mu_{E}^\dagger = 0 \) and that \( \lambda_{E, \Sigma_0}^\dagger = r_{E}^\dagger \). The degree of \( f_{E, \Sigma_0}(T) \) is equal to \( \lambda_{E, \Sigma_0}^\dagger = r_{E}^\dagger \). Since \( f_{E, \Sigma_0}(T) \) is expressed as \( T^{r_{E}^\dagger} g_{E, \Sigma_0}(T) \), the degree of \( g_{E, \Sigma_0}(T) \) is equal to zero. It has been shown that \( \mu_{E, \Sigma_0}^\dagger = \mu_{E}^\dagger = 0 \). It follows that \( g_{E, \Sigma_0}(T) \) is a unit in \( \mathbb{Z}_p \). Lemma \ref{lem:5.4} asserts that \( \Phi_{E, \Sigma_0} \times \chi_t(\Gamma, E) \) 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 \( \Sigma_1 \). The smaller the set of primes \( \Sigma_1 \), the more refined the congruence relation between truncated Euler characteristics is. This is why it is of considerable importance that the set of primes \( \Sigma_1 \) be carefully chosen to be as small as possible. We note that in the statement of [33, 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 \( \Sigma_0 \) was the full set of primes \( v \parallel p \) at which \( E_1 \) or \( E_2 \) has bad reduction. The set of primes \( \Sigma_1 \) is smaller and hence, when \( F = \mathbb{Q} \) the result below refines the result [33 Theorem 3.3].

**Theorem 5.5.** Let \( E_1 \) and \( E_2 \) be elliptic curves which satisfy Hypothesis [4] mentioned in the introduction. Then, the following assertions hold.

1. Suppose \( r_{E_1}^\dagger \) is equal to \( r_{E_2}^\dagger \). Then, \( \Phi_{E_1, \Sigma_1} \times \chi_t(\Gamma, E_1) \) is equal to 1 if and only if \( \Phi_{E_2, \Sigma_1} \times \chi_t(\Gamma, E_2) \) is equal to 1.

2. If \( r_{E_1}^\dagger < r_{E_2}^\dagger \), then \( \Phi_{E_1, \Sigma_1} \times \chi_t(\Gamma, E_1) \) is divisible by \( p \).

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

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

Consider the case when \( r_{E_1}^\dagger = r_{E_2}^\dagger \). It is natural to ask if \( \chi_t(\Gamma, E_1) = 1 \) implies that \( \chi_t(\Gamma, E_2) = 1 \)? This statement is false, as is shown in [33 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 $\Phi_{E_1, \Sigma_1}$, i.e.

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

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 multi-signed Selmer groups have not been defined for more general $p$-adic Lie extensions. In the good ordinary reduction setting, the reader is referred to [41] for a discussion on truncated Euler characteristics over general $p$-adic Lie extensions. In [33] 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 $F\mathcal{F}_\infty$ be a Galois extension of $F$ containing $F^\text{cyc}$ such that $\text{Gal}(F\mathcal{F}_\infty/F) \simeq \mathbb{Z}_p^m$ for an integer $m \geq 1$. Set $G := \text{Gal}(F\mathcal{F}_\infty/F), H := \text{Gal}(F\mathcal{F}_\infty/F^\text{cyc})$ and identify $\Gamma$ with $\text{Gal}(F^\text{cyc}/F) \simeq G/H$. Let $E$ be an elliptic curve and $\xi$ be a signed vector, assume that $(E, \xi)$ satisfies Hypothesis (3) and assume that Hypothesis (2) is satisfied for the pair $(E, F\mathcal{F}_\infty)$. Another natural hypothesis is that the Selmer groups be in $\mathfrak{M}_H(G)$. The precise definition is given below.

**Definition 6.1.** Let $M$ be a cofinitely generated cotorsion $\mathbb{Z}_p[[G]]$-module and let $M(p)$ be the $p$-primary submodule of $M$. The category $\mathfrak{M}_H(G)$ 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 5.** Assume that the Selmer group $\text{Sel}^\xi(E/F\mathcal{F}_\infty)$ is in $\mathfrak{M}_H(G)$.

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

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

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

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

1. Both $\ker(\psi_M)$ and $\cok(\psi_M)$ are finite,
2. $H^i(G, M)$ is finite for $i \geq 2$.

The truncated $G$-Euler characteristic is then defined by

$$\chi_t(\Gamma, M) := \frac{\# \ker(\psi_M)}{\# \cok(\psi_M)} \times \prod_{i \geq 2} \# (H^i(G, M))^{-1}.$$ 

Next, we recall the notion of the Akashi series. For a cofinitely generated $\Gamma$-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 $\text{Ak}_H(D)$ is taken to be the following alternating product:

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

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

Proposition 6.4. [41, Proposition 2.10] Let $D$ be a discrete $p$-primary $G$-module such that the Pontryagin dual $D^\vee$ is in $\mathfrak{M}_H(G)$. Then, the Akashi series $\text{Ak}_H(D)$ is defined. Furthermore, suppose that $D$ has finite truncated $G$-Euler characteristic. Let $\beta T^k$ be the leading term of $\text{Ak}_H(D)$. Then, the following assertions hold:

1. The order of vanishing $k$ is given by
   $$k = \sum_{i \geq 0} (-1)^i \text{corank}_{Z_p} H^i(H, D)^\Gamma$$

2. The truncated $G$-Euler characteristic is given by
   $$\chi_t(G, D) = |\beta|^{-1}.$$

The truncated $G$-Euler characteristic of $\text{Sel}^1(E/F_\infty)$ is denoted $\chi_t^1(G, E)$. When the truncated $G$-Euler characteristic is defined, it is related to the Akashi series of $\text{Sel}^1(E/F_\infty)$, which we denote by $\text{Ak}_H^1(E)$. The following Theorem due to Lei and Lim describes the link between Akashi series $\text{Ak}_H^1(E)$ and the characteristic polynomial $f_E^1(T)$ of the Selmer group $\text{Sel}^1(E/F^{\text{cyc}})$.

Theorem 6.5. [24, Theorem 1.1] Let $E$ be an elliptic curve over a number field $F$, and let $\varepsilon$ be a signed vector. Let $F_\infty$ be a $\mathbb{Z}_p^m$-extension of $F$ which contains $F^{\text{cyc}}$. Assume that:

1. Hypotheses (1), (2), (3) and (5) are satisfied.
2. The Selmer group $\text{Sel}^1(E/F^{\text{cyc}})$ is $\mathbb{Z}_p[\Gamma]$-cotorsion.

Then, the Akashi series $\text{Ak}_H^1(E)$ is well-defined and is given by

$$\text{Ak}_H^1(E) = T^{\gamma_E} \cdot f_E^1(T),$$

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

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

1. Hypotheses (1), (2), (3) and (5) are satisfied.
2. The truncated $G$-Euler characteristic $\chi_t^1(G, E)$ is well defined.

Then, the truncated $G$-Euler characteristic $\chi_t^1(G, E)$ is equal to the truncated $\Gamma$-Euler characteristic $\chi_t(\Gamma, E)$. 

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 $\frac{r}{s}$ be a signed vector. Assume that

1. Hypotheses (2), (4) and (5) are satisfied.
2. The truncated $G$-Euler characteristic $\chi^\frac{r}{s}_i(G, E)$ is well defined.

Then, the following assertions hold.

1. Suppose that $r^\frac{1}{E_1} = r^\frac{1}{E_2}$. Then, we have that the truncated $G$-Euler characteristics are defined, then $\Phi^\frac{r}{E_1}_{E_1, \Sigma_1} \times \chi_i(G, E_1)$ is equal to 1 if and only if $\Phi^\frac{r}{E_2}_{E_2, \Sigma_1} \times \chi_i(G, E_2)$ is equal to 1. Furthermore, $\Phi^\frac{r}{E_1}_{E_1, \Sigma_1} \times \Delta^\Sigma_1 E_2$ is equal to $T^r E_1 \{ \Sigma(G, E) \}$ if and only if $\Phi^\frac{r}{E_2}_{E_2, \Sigma_1} \times \Delta^\Sigma_1 E_2$ is equal to $T^r E_1 \{ \Sigma(G, E) \}$.
2. Suppose that $r^\frac{1}{E_1} < r^\frac{1}{E_2}$. Then, $p$ divides $\Phi^\frac{r}{E_1}_{E_1, \Sigma_1} \times \chi_i(G, E_1)$.

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 [33, 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 $E_2 = 462a1$. 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 $\chi^\frac{r}{s}_i(G, E_i)$ is well defined for $i = 1, 2$. Hypothesis (1) is satisfied for the elliptic curves $E_1$ and $E_2$. Let $\frac{r}{s} \in \{+, -\}$ be a choice of sign. Assume that for $i = 1, 2$, the Selmer group $\text{Sel}^\frac{r}{s}(E_i/\mathbb{Q}_{\text{Gal}})$ is $\mathbb{Z}_p[[\Gamma]]$-cotorsion. Therefore, Hypothesis (4) is satisfied. We show that $\Phi^\frac{r}{E_1}_{E_1, \Sigma_1} \times \chi^\frac{r}{s}_i(G, E_1) = 1$ if $i = 1, 2$. This demonstrates Theorem 5.5 which asserts that

$$\Phi^\frac{r}{E_1}_{E_1, \Sigma_1} \times \chi^\frac{r}{s}_i(G, E_1) = 1 \text{ if and only if } \Phi^\frac{r}{E_2}_{E_2, \Sigma_1} \times \chi^\frac{r}{s}_i(G, E_2) = 1.$$
otherwise. These values are calculated from the following:

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

None of the above values are not divisible by 5 and hence, \( \Phi_{E_1, \Sigma_1} \) and \( \Phi_{E_2, \Sigma_1} \) 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

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

see [16, Theorem 1.2]. For both elliptic curves, \#III(\( E_i/\mathbb{Q} \))[5] and \( E_i(\mathbb{Q}) \) has no 5-torsion. It follows that \#Sel(\( E/\mathbb{Q} \)) ~ 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 \( pp^* \), where \( p = (2 + i) \) and \( p^* = (2 - i) \).

Both curves \( E_1 \) and \( E_2 \) are supersingular at the primes \( p \) and \( p^* \). The Mordell Weil ranks of \( E_1 \) (resp. \( E_2 \)) over \( F \) are 0 (resp. 1). Let \( \pi = (\pi_1, \pi_2) \) be a signed vector. It follows that the order of vanishing of the signed Selmer group at \( T = 0 \) is given by \( r^+_{E_1} = 0 \) and \( r^+_{E_2} = 1 \). Since \( r^+_{E_2} \leq 1 \), it follows from Lemma 3.3 that the truncated Euler characteristic \( \chi_{\pi}(\Gamma, E_2) \) is well defined. On the other hand, since \( r^+_{E_1} = 0 \), the truncated Euler characteristic \( \chi_{\pi}(\Gamma, E_1) \) is well defined and coincides with the usual Euler characteristic \( \chi(\Gamma, E_1) \).

Since \( r^+_{E_1} < r^+_{E_2} \), Theorem 3.5 asserts that 5 divides \( \Phi_{E_1, \Sigma_1} \times \chi(\Gamma, E_1) \). We demonstrate this via direct calculation by showing that \( \Phi_{E_1, \Sigma_1} \) is divisible by 5.

We shall assume that the Selmer groups \( \text{Sel}^\dagger(\mathcal{E}_i/F^{\text{cyc}}) \) are cotorsion. The optimal set of primes \( \Sigma_1 \) 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 \( \Phi_{E_1, \Sigma_1} \) is divisible by 5.

Let \( F_1 \) and \( F_2 \) be the maximal pro-\( p \) abelian extension of \( F \) unramified outside \( p \), resp. \( p^* \). Both \( F_1 \) and \( F_2 \) are \( \mathbb{Z}_p \)-extensions of \( F \). Let \( F_\infty \) be the composite of \( F_1 \) and \( F_2 \). We discuss results for truncated Euler characteristics over \( F_\infty \). Assume that for \( i = 1, 2 \), the Selmer group \( \text{Sel}^\dagger(\mathcal{E}_i/F_\infty) \) is in \( \mathfrak{M}(H) \). Recall that \( G = \text{Gal}(F_\infty/F) \) and \( H = \text{Gal}(F_\infty/F^{\text{cyc}}) \). The conditions of Hypothesis 2 are satisfied for \( F_\infty \). Corollary 6.6 asserts that \( \chi_i(G, E_i) \) is equal to \( \chi_i(G, E_i) \) 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). Comptes rendus de l’Académie des sciences. Série I, Mathématique 317.3 (1993): 227-232.

[2] D. Bernardi, C. Goldstein and N. Stephens. Notes $p$-adiques sur les courbes elliptiques. Journal für die reine und angewandte Mathematik 1984.351 (1984): 129-170.

[3] J. Coates and R. Greenberg. Kummer theory for abelian varieties over local fields, Invent. math. 124.1 (1996): 129-174.

[4] J.H. Coates et al., Links between cyclotomic and $GL_2$ Iwasawa theory, Doc. Math 2003 (2003): 187-215.

[5] J.H. Coates and R. Sujatha, Galois cohomology of elliptic curves, Narosa, 2000.

[6] D. Disegni. On the $p$-adic Birch and Swinnerton-Dyer conjecture for elliptic curves over number fields. Kyoto Journal of Mathematics 60.2 (2020): 473-510.

[7] M. Emerton, R. Pollack, and T. Weston, Variation of Iwasawa invariants in Hida families, Invent. math. 163.3 (2006): 523-580.

[8] R. Greenberg. Iwasawa theory for $p$-adic representations. Algebraic Number Theory—in Honor of K. Iwasawa. Mathematical Society of Japan, 1989.

[9] R. Greenberg. Iwasawa theory for elliptic curves. Arithmetic theory of elliptic curves. Springer, Berlin, Heidelberg, 1999. 51-144.

[10] Greenberg, Ralph, and Glenn Stevens. $p$-adic $L$-functions and $p$-adic periods of modular forms. Inventiones mathematicae 111.1 (1993): 407-447.

[11] R. Greenberg and V. Vatsal, On the Iwasawa invariants of elliptic curves, Invent. math. 142.1 (2000): 17-63.

[12] Hachimori, Yoshitaka, and Kazuo Matsuno. "An analogue of Kida’s formula for the Selmer groups of elliptic curves." Journal of Algebraic Geometry 8.3 (1999): 581-601.

[13] J.W. Jones. Iwasawa $L$-functions for multiplicative abelian varieties. Duke MathematicalJournal 59.2 (1989): 399-420.

[14] K. Kato. $p$-adic Hodge theory and values of zeta functions of modular forms. Astérisque 295 (2004): 117-290.

[15] B.D. Kim. Signed-Selmer Groups over the $\mathbb{Z}_p^2$-extension of an Imaginary Quadratic Field. Canadian Journal of Mathematics 66.4 (2014): 826-843.

[16] B.D.Kim. The plus/minus Selmer groups for supersingular primes. Journal of the Australian Mathematical Society 95.2 (2013): 189-200.

[17] B. D. Kim. The Iwasawa invariants of the plus/minus Selmer groups. Asian Journal of Mathematics 13.2 (2009): 181-190.

[18] T. Kitajima and R. Otsuki. On the plus and the minus Selmer groups for elliptic curves at supersingular primes. Tokyo Journal of Mathematics 41.1 (2018): 273-303.

[19] S. Kobayashi. Iwasawa theory for elliptic curves at supersingular primes. Invent. math. 152.1 (2003): 1-36.

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

[21] Kurihara, Masato. On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I. Inventiones mathematicae 149.1 (2002): 195-224.

[22] A. Lei, D. Loeffler, and S. L. Zerbes. Wach modules and Iwasawa theory for modular forms Asian J. Math., 2010.

[23] Lei, Antonio, and Meng Fai Lim. Mordell-Weil ranks and Tate-Shafarevich groups of elliptic curves with mixed-reduction type over cyclotomic extensions. arXiv preprint [arXiv:1911.10643] (2019).

[24] A. Lei, and M.F. Lim. Akashi series of signed Selmer groups of elliptic curves with semistable reduction at primes above $p$. arXiv preprint [arXiv:2001.09304] (2020).

[25] Iovita, Adrian, and Robert Pollack. Iwasawa theory of elliptic curves at supersingular primes over $\mathbb{Z}_p$-extensions of number fields. Journal für die reine und angewandte Mathematik 2006.598 (2006): 71-103.

[26] B. Mazur. Rational points of abelian varieties with values in towers of number fields. Invent. math. 18.3-4 (1972): 183-266.
[27] B. Mazur, J. Tate, and J. Teitelbaum, On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, Invent. math. 84.1 (1986): 1-48.
[28] F.A.E. Nuccio and R. Sujatha. Residual supersingular Iwasawa theory and signed Iwasawa invariants. arXiv preprint arXiv:1911.10649 (2019).
[29] B. Perrin-Riou. Théorie d’Iwasawa p-adique locale et globale. Invent. math. 99.1 (1990): 247-292.
[30] B. Perrin-Riou, Théorie d’Iwasawa et hauteurs p-adiques, Invent. math. 109.1 (1992): 137-185.
[31] R. Pollack. On the p-adic L-function of a modular form at a supersingular prime. Duke Mathematical Journal 118.3 (2003): 523-558.
[32] Ponsinet, Gautier. "On the structure of signed Selmer groups." Mathematische Zeitschrift 294.3 (2020): 1635-1658.
[33] A. Ray and R. Sujatha. Euler Characteristics and their Congruences in the Positive Rank Setting. Canadian Math. Bull. (2019): 1-19.
[34] K. Rubin. The main conjectures of Iwasawa theory for imaginary quadratic fields. Invent. math. 103.1 (1991): 25-68.
[35] J.H. Silverman. The arithmetic of elliptic curves, Vol. 106. Springer Science and Business Media, 2009.
[36] P. Schneider. p-adic height pairings I, Invent. math. 69.3 (1982): 401-409.
[37] P. Schneider. p-adic height pairings. II, Invent. math. 79.2 (1985): 329-374.
[38] S.Shekhar and R. Sujatha, Euler characteristic and congruences of elliptic curves, Münster J. Math. 7.1 (2014): 327-343.
[39] F. Sprung. Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures. Journal of Number Theory 132.7 (2012): 1483-1506.
[40] F. Sprung. A formulation of p-adic versions of the Birch and Swinnerton-Dyer conjectures in the supersingular case. Research in Number Theory 1.1 (2015): 17.
[41] S.L. Zerbes. Generalised Euler characteristics of Selmer groups, Proceedings of the London Mathematical Society 98.3 (2008): 775-796.

Department of Mathematics, University of British Columbia, Vancouver BC, V6T 1Z2, Canada.
Email address: anweshray@math.ubc.ca

Department of Mathematics, University of British Columbia, Vancouver BC, V6T 1Z2, Canada.
Email address: sujatha@math.ubc.ca